Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 2310 – 2319
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.6052

Securing Health Data in the Digital Age: Challenges, Regulatory Frameworks, and Strategic Solutions in Saudi Arabia

Houda Alhoussari[1]

Abstract

The rapid digital transformation in Saudi Arabia, driven by the ambitious Vision 2030 initiative, positions health data as a cornerstone of innovation in the healthcare sector. Health data, classified as sensitive and strategic, is critical for improving patient care, advancing medical research, and fostering predictive analytics. However, this digitization also exposes health data to escalating cyber threats, such as ransomware, phishing, and attacks on IoMT devices. These risks compromise data confidentiality, integrity, and availability, eroding trust and causing significant economic impacts.This study adopts an analytical and comparative approach to evaluate the challenges and solutions associated with health data cybersecurity in Saudi Arabia. It examines the strengths and weaknesses of national frameworks, including the Personal Data Protection Law (PDPL) and the Essential Cybersecurity Controls (ECC), while benchmarking them against international standards such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). By addressing technical, organizational, and human challenges, the research proposes strategic recommendations, emphasizing technological measures, regulatory enhancements, and capacity-building initiatives.The findings aim to contribute to the development of a secure and innovative digital healthcare ecosystem in Saudi Arabia, aligning with the goals of Vision 2030 and ensuring the protection of sensitive health data.

Keywords: *Health Data, cybersecurity, Vision 2030, GDPR, HIPAA, Saudi Arabia, Personal Data Protection Law (PDPL), IoMT.*

Introduction

In the era of rapid digital transformation, health data has emerged as a cornerstone of innovation and progress in the healthcare sector. In Saudi Arabia, the Vision 2030 initiative aims to modernize the healthcare system by integrating advanced digital technologies, such as the Internet of Medical Things (IoMT) and electronic health records, to improve the quality of care, enhance research capabilities, and optimize health crisis management. However, these advancements also expose sensitive health data to unprecedented cyber threats, including ransomware attacks, phishing schemes, and vulnerabilities in connected medical devices. (Camara & Peris-Lopez, 2015)

The classification of health data as sensitive under the Personal Data Protection Law (PDPL) underscores its critical value and the necessity for robust security measures (Khattak & Abukhait., 2024). Yet, the increasing interconnectivity of healthcare systems, coupled with challenges such as outdated technologies, human errors, and organizational limitations, presents significant risks to the confidentiality, integrity, and availability of health data. These issues highlight the need for comprehensive strategies to ensure data protection while supporting innovation (Douville, 2023).

This article adopts an analytical and comparative approach to examine the cybersecurity landscape of health data in Saudi Arabia. It evaluates the effectiveness of national frameworks, such as the PDPL and the Essential Cybersecurity Controls (ECC), and compares them with international standards, including the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). By addressing technical, organizational, and human challenges, the study aims to provide strategic recommendations that align with Vision 2030's objectives.

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

Ultimately, this research seeks to contribute to the development of a secure, innovative, and trustworthy healthcare ecosystem that balances the protection of sensitive health data with the pursuit of technological advancement.

Literature Review

The Concept of Health Data

Health data can be categorized into several types, each requiring tailored levels of protection based on its sensitivity and associated risks.

"Personal Data" (Art. 1, Para. 1, PDPL) is defined as any information that can directly or indirectly identify a person, such as name, address, identification number, or demographic details. It also includes specific medical data (Ahmad et al., 2025). According to Article 1, Paragraph 13 of Saudi Arabia's Personal Data Protection Law (PDPL), medical data refers to any information related to an individual's physical, mental, or psychological health, as well as healthcare services provided (preventive, curative, or rehabilitative). Examples include electronic medical records, clinical test results, and medical history.

"Sensitive Data" includes highly private information, such as genetic and biometric data, or details about mental health and specific conditions (e.g., disabilities, reproductive treatments). Such data is often targeted by malicious attacks and can be exploited for discrimination or blackmail. This highlights the critical need for robust security measures. (Maisnier-Boche, 2019)

Another category is "Collective and Aggregated Data", which is anonymized or grouped for research or management purposes (e.g., epidemiological statistics, datasets for medical artificial intelligence). Despite being anonymized, these data can sometimes be re-identified, jeopardizing research projects or public policies if leaked.

Finally, "Financial Health Data", such as insurance payment information or consultation fees, is also vulnerable to theft and fraud, requiring strong protective mechanisms.

The level of protection required depends on the sensitivity of the data and the potential consequences of a breach.

Strategic Importance of Health Data

Health data plays a crucial role in the medical sector, not only as a core element in delivering care but also as a driver of innovation and a tool for managing health crises. It enables accurate diagnoses through detailed analysis of medical history and clinical results, paving the way for personalized treatments tailored to patients' specific needs, particularly in precision medicine (Otaibi, 2019).

Furthermore, the use of connected medical devices provides real-time patient monitoring, ensuring optimal care management (BIBI et al., 2023). Health data also supports medical research and accelerates the development of innovative treatments. For example, big data played a critical role in expediting vaccine and drug development during the COVID-19 pandemic (Bernelin, 2020).

The strategic importance of health data makes it highly vulnerable to threats. According to IBM's 2023 report, the average cost of a health data breach is approximately USD 10.93 million per incident.

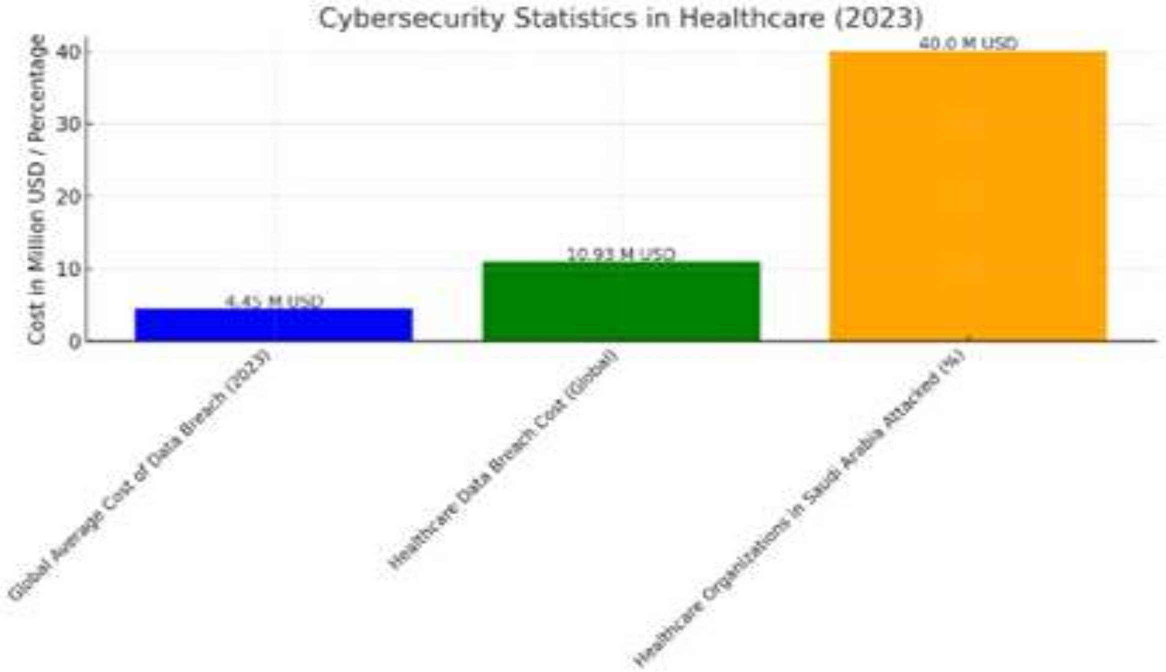

Figure 1. Averges Cost of a Data Breach 2023

Major Threats to Health Data

Health data faces three main types of cyber threats:

- Ransomware: Ransomware is a type of malicious software (malware) that encrypts a victim's data or computer systems, blocking access. Cybercriminals demand a ransom in exchange for a decryption key to restore access. If the ransom is not paid within a set timeframe, attackers often threaten to permanently delete the data or make it public. This threat significantly disrupts healthcare services. For example, the global WannaCry attack in 2017 paralyzed thousands of hospitals, including facilities in the UK (Aminot, 2020). Similarly, French hospitals were targeted by cyberattacks in 2021 and 2022 (Mahendru, 2024).

- Phishing Attacks: Cybercriminals exploit human error by sending fraudulent emails designed to steal login credentials. According to Proofpoint (2023), 65% of cyberattacks in the healthcare sector begin with phishing campaigns (Hussain, 2020).

- Attacks on the Internet of Medical Things (IoMT): These threats target connected devices, such as smart pacemakers or health monitors, which can be hacked to manipulate their functionality or access confidential data (Osama, 2023).

These major cyber threats have severe implications for patient privacy, exposing sensitive information to exploitation. Stolen data can be used to fraudulently access healthcare services or commit financial fraud. Moreover, cybersecurity gaps in health data management impose significant economic costs, both short- and long-term, affecting patients and healthcare institutions alike.

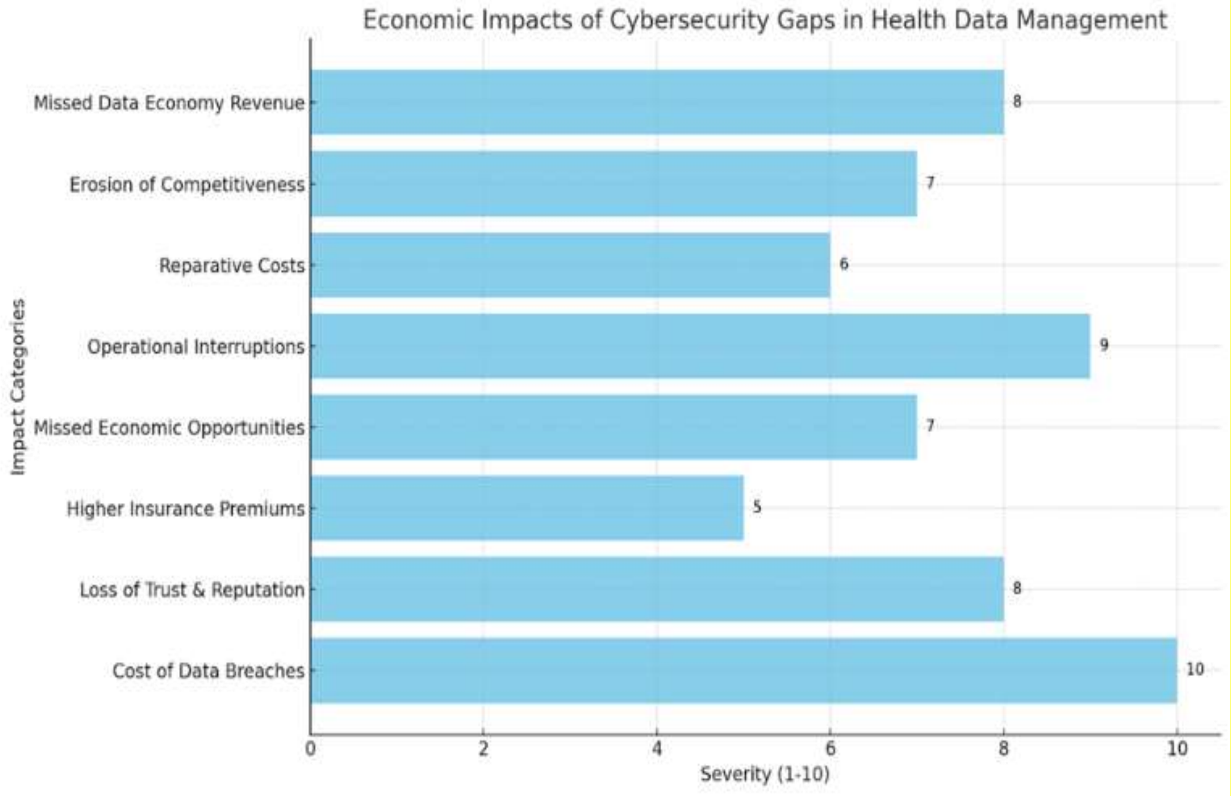

Figure 2. Economic Impacts of Cybersecurity Gaps in Health Data Management. (Source: Data provided by IBM, Commercial Allianz, WEF, Deloitte, and OECD).

This chart illustrates the economic impacts of cybersecurity gaps in health data management, ranked by severity on a scale of 1 to 10.

Legal Framwork

The protection of health data is primarily governed by the Personal Data Protection Law (PDPL) and the Essential Cybersecurity Controls (ECC)**.**

Personal Data Protection Law

The Personal Data Protection Law (PDPL)**,** enacted in 2021, serves as the primary framework for managing and protecting personal data in Saudi Arabia. It includes specific provisions for sensitive data, particularly health data. One of the strengths of this law lies in its clear definition of health data as personal, sensitive, and medical information, requiring enhanced protection measures (Articles 1 and 13, PDPL). It also grants individuals the right to be informed about the collection, use, and retention of their personal data, with the ability to withdraw their consent for data processing at any time (Articles 4 and 5, PDPL).

Given the sensitive nature of health data, the PDPL places special emphasis on its protection (Lucas, 2017). The law mandates strict requirements for the collection, processing, and retention of such data, ensuring its security and limiting its use to legitimate purposes, such as medical care, scientific research, or managing health crises (Articles 2 and 3, PDPL). The law also underscores the responsibility of medical institutions to secure health data and report any breaches.

Although Saudi Arabia's PDPL represents significant progress in protecting personal data, including that generated by IoMT devices, certain practical challenges remain. First, the uniform implementation of its provisions is a major challenge, particularly across different healthcare institutions, where technical and organizational resources vary widely. Second, the low level of awareness among healthcare professionals regarding the law's requirements and best practices in cybersecurity poses a critical vulnerability.

These shortcomings undermine the overall effectiveness of the legal framework and highlight the need for additional measures to strengthen compliance and awareness across the healthcare sector (Vaugelade, 2019).

La Essential Cybersecurity Controls

The ECC, developed by Saudi Arabia's National Cybersecurity Authority (NCA), are a key initiative to protect critical systems, including those in the healthcare sector, based on the CIA triad (Confidentiality, Integrity, Availability). These controls aim to ensure the confidentiality of health data by enforcing measures such as encrypting data in transit and at rest, thereby preventing unauthorized access. Integrity 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 strengthened through network segmentation strategies and regular software updates, ensuring continuous and secure access to data, even during a cyberattack (Essential Cybersecurity Controls, 2024).

However, the implementation of the ECC faces challenges, particularly in smaller medical facilities constrained by limited budgets and a lack of technical expertise. Additionally, the absence of mandatory audits and centralized oversight reduces their effectiveness, leaving some institutions vulnerable to growing threats such as ransomware and attacks targeting IoMT devices (Lindstad & Rosager-Ludvigsen, 2023).

Research and Methodology

Research Design

This study adopts a mixed-methods approach, combining qualitative and quantitative analysis. The primary focus is on analyzing regulatory frameworks, technical standards, and organizational practices related to health data cybersecurity in Saudi Arabia.

Data Collection

Data was gathered from multiple sources, including:

Primary Data: Surveys conducted with patients aged 18 to 55 to assess awareness of cybersecurity practices.

Secondary Data: Academic publications, reports from regulatory bodies (e.g., SDAIA, NCA), and international guidelines (e.g., GDPR, HIPAA).

Comparative Analysis

A comparative legal analysis was conducted to identify similarities and differences between the PDPL, GDPR, and HIPAA, focusing on their provisions for sensitive data protection and cybersecurity measures.

Analytical Framework

The study employs a multidisciplinary framework, integrating technical, organizational, and legal perspectives. This framework evaluates the impact of cybersecurity measures on data protection, innovation, and patient trust in the healthcare sector.

Analyse and Discussion

A careful and analytical review of the PDPL, General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA) has enabled us to identify their points of convergence and divergence.

Points of Convergence

The three regulatory frameworks – PDPL, GDPR, and HIPAA – converge on fundamental principles for protecting personal and sensitive data, including medical information. They require explicit consent from individuals before any data processing, thereby ensuring transparency and trust. In the event of a data breach, these regulations mandate prompt notification to individuals and authorities to mitigate the impacts. Finally, they emphasize accountability by requiring organizations to implement robust internal policies to ensure the security and integrity of the data (Sarabdeen et al., 2024).

Points of Divergence

The differences between the three frameworks are structured around four key points:

Financial Penalties

The GDPR imposes very strict financial penalties, which can reach up to €20 million or 4% of a company's global annual revenue, serving as a strong deterrent (Art. 83 GDPR).

The PDPL, while also enforcing penalties, has not yet reached a similar scale, with fines capped at 5 million SAR, potentially reducing its deterrent effect (Art. 35 PDPL).

The HIPAA also provides for fines, but these are primarily based on the severity of the violation and can amount to up to $1.5 million USD per year for a single violation (Art. § 160.404).

Data Portability

The GDPR places significant emphasis on data portability, allowing individuals to easily transfer their personal information between different providers (Art. 20 GDPR).

In comparison, the HIPAA and PDPL do not prioritize this aspect to the same extent.

Compliance Audits

The HIPAA requires regular audits to assess the compliance of medical entities, a practice less emphasized in the GDPR and PDPL. In Saudi Arabia, the PDPL does not explicitly mandate systematic audits but includes general requirements for oversight and compliance (Art. 20 PDPL). However, the Essential Cybersecurity Controls (ECC) explicitly recommend regular audits as a means to ensure the security of critical infrastructures, including in the healthcare sector. The National Cybersecurity Authority (NCA) regularly organizes campaigns to encourage organizations to conduct compliance assessments, particularly for entities handling sensitive data. These campaigns include technical audits of system configurations and organizational processes.

Securing IoMT Devices

The HIPAA pays special attention to connected devices handling Electronic Protected Health Information (ePHI) in the medical field, requiring specific measures for their security (45 CFR § 164.308 to § 164.316 HIPAA).

The GDPR generally covers connected devices but does not include specific regulations for medical devices.

The PDPL does not yet provide detailed guidelines for IoMT devices, although they are indirectly covered under the broader framework for sensitive data protection.

As a result, the PDPL reflects a balance between international standards and the cultural and legal specificities of Saudi Arabia, particularly regarding sensitive data.

Despite the efforts made, audits in Saudi Arabia primarily focus on large critical infrastructures, while small and medium-sized healthcare entities, often constrained by limited resources, struggle to implement them systematically. This disparity weakens the overall security of data in the sector.

Implementation Challenges

Challenges related to cybersecurity in the healthcare sector can multiply, encompassing technical, organizational, and human aspects. When these challenges are not adequately addressed, they significantly increase the vulnerability of systems.

Technical challenges

Vulnerabilities of IoMT Devices

These technologies have critical vulnerabilities, making them highly susceptible to cyberattacks. Often deployed without robust security protocols, IoMT devices are exposed to external intrusions, primarily due to the lack of regular updates. A weakness identified in a study by Kaspersky (2020) reveals that over 70% of these devices are not properly updated.

The vulnerability stems from the lack of built-in security during design (Security by Design), where encryption is not always applied before transmitting data (Lindstad & Rosager-Ludvigsen, 2023).

Moreover, the extended lifecycle of these devices often makes them incompatible with new technologies and modern cybersecurity solutions.

These vulnerabilities allow cybercriminals to exploit the devices to manipulate their functionality or alter data, directly endangering patient health and safety (Osma et al., 2023).

Outdated Software

Many healthcare institutions rely on outdated IT systems, often incompatible with modern cybersecurity solutions. These software systems, due to the lack of regular updates, remain vulnerable to well-known exploits (IBM Security Report (2023) on cyber threats in the healthcare sector).

Organizational Challenges

Lack of Coordination and Absence of Regular Audits

Coordination among healthcare institutions is often insufficient to ensure uniform data protection.

The absence of regular audits prevents the identification and remediation of existing vulnerabilities. According to a Deloitte survey, over 60% of medical institutions in the Middle East do not conduct periodic cybersecurity assessments. (Deloitte Centre for Health Solutions, 2018)

Limited Budgets

Budgets allocated to cybersecurity in the healthcare sector are often insufficient, particularly in smaller institutions. This limits the adoption of modern technologies and staff training.

Human Challenges

Human error is a major vulnerability in healthcare cybersecurity. Risky practices, such as using weak passwords or sharing information insecurely, increase the likelihood of system compromise (Alsharif & Mishra, 2021). For example, a cyberattack in 2022 on a hospital network in Saudi Arabia revealed that default passwords were still being used in several critical systems, jeopardizing the security of sensitive data (IBM Security Report, 2023).

The results of a survey conducted among patients aged 18 to 55 support this observation. A significant portion of respondents reported a lack of information about cybersecurity best practices and the measures implemented by institutions to protect their health data.

This lack of awareness is not limited to medical staff but also includes end-users of connected systems, such as IoMT devices, thereby increasing the risks of cyberattacks.

Implementing Robust Cybersecurity Strategies

While the protection of health data relies on complementary measures—technical, organizational, and regulatory—in Saudi Arabia, it is built on a combination of these three technical measures, supported by national initiatives such as the National E-Health Program and the guidelines of the Saudi Data and Artificial Intelligence Authority (SDAIA).

On the technical level, tools such as Advanced Encryption Standard (AES), Transport Layer Security (TLS), multi-factor authentication (MFA), intrusion detection systems (SIEM), network segmentation, and the use of specialized firewalls for connected devices are essential for securing health data.

Network segmentation and regular patching help mitigate the risks associated with these technologies. The National E-Health Program plays a key role in centralizing and digitizing health data while establishing secure infrastructures to ensure their protection (Essential Cybersecurity Controls, 2024).

On the organizational level, raising awareness among healthcare professionals about cyber threats and developing clear policies for access management and incident response are top priorities.

Regular audits, encouraged by the National Cybersecurity Authority, ensure system compliance with security standards. The Saudi Data and Artificial Intelligence Authority (SDAIA), as the regulatory authority for data, enforces standards for the use, retention, and confidentiality of data, particularly under the Personal Data Protection Law .

Finally, on the regulatory level, Saudi Arabia strictly enforces the PDPL, which protects sensitive data, and the ECC to secure critical infrastructures.

Alignment with international standards, such as the GDPR and HIPAA, ensures global compliance while accounting for local cultural and legal specificities. Through its guidelines, the SDAIA establishes frameworks to ensure the ethical and secure use of health data, particularly in initiatives leveraging artificial intelligence.

These integrated efforts enable Saudi Arabia to build a secure digital ecosystem that balances innovation with the protection of sensitive data.

Recommendations

To strengthen health data security, it is crucial to:

Strengthen Legal Frameworks: Mandate the obligatory notification of data breaches, impose stricter penalties for sensitive data violations, and align Saudi standards with international regulations (GDPR, HIPAA) for cross-border data transfers.

Adopt Technological Innovations: Integrate artificial intelligence to detect threats and blockchain to secure data exchanges (Alhoussari, 2025).

Develop Human Capabilities: Raise awareness and provide regular training for healthcare professionals, involve patients in targeted education campaigns, and promote local expertise in this field.

Enhance Governance and Collaboration: Establish a centralized authority to oversee cybersecurity and promote international partnerships to share knowledge and best practices.

These actions, working in synergy, will enhance health data security while fostering innovation.

Conclusion

The digital transformation driven by Vision 2030 places health data at the core of innovation and healthcare delivery in Saudi Arabia. However, this data, increasingly vulnerable to cyber threats, requires robust protective measures.

An analysis of Saudi regulatory frameworks, such as the PDPL and ECC, highlights significant progress but also reveals practical challenges to address, particularly in raising awareness and ensuring compliance with standards.

To achieve optimal security, it is essential to adopt an integrated approach that combines technical, organizational, and legal measures while leveraging emerging technologies. By effectively securing sensitive data, Saudi Arabia can not only protect patient privacy but also build trust and advance its ambitions in digital healthcare.

Acknowledgment

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

Alhoussari H., (2025), "Blockchain and Healthcare Data", in Blockchain & Privacy book, Bruylant, pp. 105-123.

Alhoussari H., (2024), Les vertus et les vices de l'utilisation de la Blockchain dans le domaine de santé, Journal of Justice and Law, V.11, 2024/3 ,pp. 84-110.

Alhoussari H., (January 2025), "Integrating ESG Criteria in Corporate Strategies: Determinants and Implications for Performance", Journal of Ecohumanism, Vol. 3, N° 8, pp. 2968-2979, DOI:10.62754/joe.v3i8.5791.

AMINOT J.-L, Wanna C. (April-2020), « Une frayeur à l'échelle planétaire », Responsabilité & Environnement, N° 98 , pp. 53-56.

Aumans Avocats, « Objets Connectés de santé : enjeux juridiques », (25/03/2024) https://aumans-avocats.com/objets-connectes-de-sante-enjeux-juridiques/

Ahmad, I., Jamali, D. R., & Khattak, M. N. (2025). Can organizations get away with greenwashing? CSR attributions and counterproductive sustainability behaviors. Business Ethics, the Environment & Responsibility, 34(1), 103-120.

Barrett M, Boyone J., Brandts J., & others, (2019) "Artificial Intelligence Supported Patient Self-Care in Chronic Heart Failure: A Paradigm Shift from Reactive to Predictive, Preventive and Personalised Care", 10 EPMA Journal, pp. 445, 448.

Bernelin M., Desmoulin S., Lefèvre T., (Sept-2020), « Données massives, big data et santé publique : de quoi parle-t-on ? », adsp N° 112, pp. 14-19.

ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.6052

Bibi L., Hamma H., Srikaran I. & Viard M., (2023), « Cas d'utilisation des dispositifs médicaux connectés en France », memory, DOI : 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, Vol. 55, pp. 272-289.

Dhali M., Hassan S., Zulhuda S. & S. Fadhilah S., (Feb-2022) "Artificial intelligence in health care: data protection concerns in Malaysia", in Oxford University Press, DOI: 10.1093/idpl.

Douville T., (2023), Droit des données à caractère personnel, LGDJ.

Etude de Kaspersky (2021)

French High Authority for Health, (Nov-2017), "Connected Medical Devices (CMD): Guide for Submitting a File to the National Commission for the Evaluation of Medical Devices and Health Technologies,".

Halperin D., Heydt-Benjamin T., Ransford B., & others, (2008), "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero Power Defenses",Proceedings—IEEE Symposium on Security and Privacy 129.

Health Insurance Portability and Accountability Act, (1996), USA.

Hussain Seh A., Aleneze M., Krishna Sarkar A., & others, (13 May 2020), "Healthcare Data Breaches: Insights and Implications", MDPI.

IBM Security, (2023), Report on the Cost of a Data Breach.

Jobran M., (Nov-2024), « Enregistrement des dispositifs médicaux SFDA (MDMA), PharmaKnowl Consulting.

Khallaf F. El- Shafai W., El-Rabaie E., and others, (Sep-2024), " Blockchain-based color medical image cryptosystem for industrial Internet of Healthcare Things (IoHT) ," in Springer Netherlands , Doi: 10.1007/s11042-023-16777-

Kosta-Eleni K. & Bowman D., (2012), "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" in Diana M Gasson and others (eds), Human ICT Implants: Technical, Legal and Ethical Considerations, p. 102.

Khattak, M. N., & Abukhait, R. (2024). Impact of perceived organizational injustice on deviant behaviors: moderating impact of self-control. Current Psychology, 43(12), 10862-10870.

Lindstad S. & Rosager-Ludvigsen K., (2023), "When is the processing of data from medical implants lawful? The legal grounds for processing health related personal data from ICT implantable medical devices for treatment purposes under EU data protection law", Medical Law Review, Vol. 31, Issue 3, pp. 317–339.

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

Mahendru P., (2024), "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., (2024), « L'état des ransomwares dans le secteur de la santé en 2024 », SOPHOS, https://news.sophos.com/fr-fr/2024/08/05/etat-des-ransomwares-dans-le-secteur-de-la-sante-en-2024/

Maisnier-Boché L., (31 Dec. 2019) , Données de santé à caractère personnel, Fasc. 945, Lexis Nexis.

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

National Cybersecurity Autority , Cloud Cybersecurity Controls, CCC – 1: 2020

Osama M., Abdelhamied A., Sayed M., & others , (Aug-2023), "Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions", in Multidisciplinary Digital Publishing Institute (MDPI).

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

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.

-Rapport State of the Phish 2023 de Proofpoint, (2023), ,https://www.proofpoint.com/fr/newsroom/press-releases/rapport-state-phish-2023-de-proofpoint-les-acteurs-de-la-menace-redoublent

Sarabdeen J.,. Chikhaoui E. & Mazahir M., (2002), "Creating standards for Canadian health data protection during health emergency – An analysis of privacy regulations and laws", Heliyon, Vol. 8, Issue 5, e09458.

Sarabdeen, J. & Ishak, M.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, Vol. 67, N°. 1, pp. 99-119. https://doi.org/10.1108/IJLMA-01-2024-0025.

SFDA , Requirements for Unique Device Identification (UDI) for Medical Devices, (24/05/2022), Version Number: 4.0,.

Vaugelade C., (2019), "The regulatory framework of medical devices", Bulletin de l'Académie Nationale de Médecine, Vol. 203, Issue 5, pp. 257-263.