International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

HIPPA Compliance Based Health Care Data Security - A Review

Saranya D[1], Srinidhi G A[2]

[1]Research Scholar, SSIT, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India

[2] Research Supervisor, SSIT, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
Email: *sharanyadamodharan[at]gmail.com*

Abstract: ***Information technology (IT) is assuming a vital and significant role in the health sector. Data security holds paramount significance in the healthcare sector and across the globe. The incidence of data breaches affecting confidential healthcare information is increasing. Cloud computing is highly effective for ensuring data security. Due to a data storage issue, there is a necessity for utilizing electronic communication, and various methods have been established for data security technology. The Insurance Portability and Accountability Act (HIPAA) serves as a valuable framework for facilitating healthcare research. On file we can develop a conversational and analytical method to maintain the medical records of patients in a hospital or clinic database. The patients are in a well - maintained and suitable environment. The method encompasses the enhancement of operational opportunities through providing all the essential information required for the patient. All information must be clearly identified. The safeguarding of individual privacy. The patients and the security of their information represent the most critical challenges in obtaining their intakes when considering the utilization of valuable health data within the electronic sector of healthcare industries.***

Keywords: Information Technology, HIPAA, Cyber Security, Healthcare

1. Introduction

Health holds significant importance and pertains to all living entities, including humans, plants, animals, space, and the environment. The safety issue is increasingly concerning and affects the security of everyone. To conduct a study on the technology applicable to addressing healthcare issues, it is essential to explore all avenues that can facilitate the creation of a sustainable environment where individuals and their surroundings can thrive in health and harmony. The risk management process identifies the necessary precautions based on the characteristics of the data and the surrounding environment. Throughout the data treatment process, it is advisable to implement all necessary precautions to mitigate risks and ensure data security, as outlined in Article 34 of the law referred to as “Informatics and Freedoms.”

The research conducted under European regulation 2016/679 on 27 April 2016, commonly referred to as the “General Data Protection Regulations” (GDPR), outlines that the safeguarding of personal data necessitates the implementation of suitable technical and organisational measures to ensure a level of safety that is commensurate with the associated risks and the security of patient healthcare [1, 2].

Effective communication is essential in developing the caregiver - groomed relationship. The absence of effective communication directly affects the quality and safety of patient care. The literature extensively addresses this subject, highlighting that the absence of communication is a significant factor contributing to EIAS, while also emphasising the challenges patients face in comprehending medical explanations. These challenges in comprehension elevate the mortality rate. Various initiatives are currently being implemented to this end, especially within the context of the National Patient Safety Program (PNSP), aimed at enhancing patient safety for both healthcare professionals and users. This approach facilitates objective decision - making and the identification of measures that are both necessary and appropriate to the context.

However, it can be challenging to implement such an approach and ensure that the minimum requirements have been met when one is not familiar with these methods. To advance the field of data security policies, it is crucial to understand the methods for storing and securing data to prevent any potential losses. - It is essential to possess sufficient knowledge regarding data security policies.

The primary significance of our study lies in the impact of digital tool diffusion, including the dematerialisation and individualisation of tasks, the rise of mobile work, the security of data in physical and spatial contexts, the aspiration or requirement for autonomy, the blending of professional and personal life, and the expansion of the organisation. In prior years, data management in healthcare relied on security technology to assist decision - makers in establishing effective data control and management. Numerous sources indicate that the incorporation of hospital information systems and medical service facture systems remains relevant today. The discussion surrounding the privacy of medical records has been intensified by various long - term trends. Reaching agreement on safeguards for an information system among various stakeholders within an organisation has proven to be more challenging than addressing numerous technical issues that may occur [3]. They are rapidly adopting IT without thorough planning and a clear understanding of the security concerns, leading to potential future issues. The impacts of security breaches on company protocols that inadequately protect stored records are considerably more significant than those associated with paper records. As technology advances, the likelihood of increased intrusions into personal medical records is expected to rise, especially concerning DNA testing. The potential application of DNA test results by insurers and employers to exclude certain individuals from risk pools is increasingly apparent.

Paper ID: SR241013121605 DOI: https://dx.doi.org/10.21275/SR241013121605

2. Purpose

HIS is a system designed to facilitate communication both internally and externally among healthcare providers. Hospital Information Systems serve as a centralised repository for comprehensive information regarding a patient's health history. The system must ensure that data is stored securely and regulate access to that data under specific conditions. - ese systems improve the capacity of healthcare providers to coordinate care by delivering a patient's health information and visit history precisely when and where it is required.

The essence of HIPAA compliance lies in its robust approach to safeguarding patient data and privacy, particularly through the implementation of electronic healthcare records. The varying formats of data necessitate the implementation of HIPAA, which establishes a suitable framework to enhance data accessibility and control.

3. Review of Relevant Literature

The article authored by Dumez and Minvielle was deemed highly engaging and innovative, as it concentrated on health - proofed sanitation within a context where these concepts remain inadequately defined. The authors present a narrative review of the literature [5], aiming to analyse the rebalancing of power in favour of the patient within the context of e - health. The authors maintain performativity as a framework for interpreting the earlier works of Austin [6]. - ey focus on the concepts of "performativity framed, " which arises when a theory anticipates the mechanisms that will facilitate the effectiveness of practices, and "performativity by overflow, " which occurs when unanticipated mechanisms (in this instance, related to health democracy) are implemented, leading to practices and performances that unfold in unforeseen manners. The analysis identifies four instances of engagement related to e - health: the collaboration between patients and health professionals; the collaboration enhanced by the expertise gained by patients through e - health; the independent management of the disease; and the existing state of affairs [7]. The authors effectively highlight the paradox of autonomous disease management, where the patient - physician relationship may be rebalanced through the information acquired by the patient. However, this shift also fosters a new dynamic of dependency and asymmetry concerning e - health operators, arising from safety risks and potential misuse of data generated by connected health technologies. The physical discomfort was significant prior to the implementation of the voice system.

The analysis of the company's demographic data indicates a consistent turnover within the population of order preparers. - ey are seldom retained in positions for more than 5 years of seniority. The research conducted by Gomez and Chevallet indicates that 50% of the preparers employed around 2002, aged between 25 and 34, were no longer engaged in preparation by 2007 [8]. - There were 57 recruitments within a total workforce of 110. A predominantly young recruited population, consisting of 51 operators aged between 18 and 24 years, is entirely male and lacks qualifications. This situation is often described as recruiting a physical workforce, a process facilitated by the local employment pool. ARRA is an additional approach to recording data through the adoption of electronic systems to ensure compliance with usage policies. However, it has not been enhanced to support the medical system store, and despite having 100% digital records, the healthcare sector continues to encounter penalties. It is essential to prioritize the privacy of patient data. The study "Collaboration 2020: hype or competitive advantage?" by Johnson Controls, published in 2012, indicates that this marks the onset of a significant evolution.

Johnson Controls indicates that collaboration platforms must advance to support the teamwork of collaborators situated at various locations [11, 12]. The current prevalence of IT implementation projects in healthcare facilities across Europe, North America, and other regions globally offers a unique opportunity to explore various research questions pertinent to the field of information systems. Examples of this include organisational and individual adoption, resistance to change, escalation of projects, strategic alignment, and the governance of information systems. These issues hold significant relevance in hospital organisations, which represent one of the most intricate organisational models. The development of digital health applications is currently recognised as a transformative force within the health system, with the potential to significantly alter its operations.

To effectively present the strategic actions for promoting the evaluation of health technologies in developing and emerging countries, it is essential to ensure security and facilitate informed decision - making regarding the introduction of health systems evaluation while safeguarding all data. The objective is to enhance information for an improved health system, which may involve the subset of secondary data to reinforce clinical care programs, facilitating data management and ensuring the health of the population, as illustrated in Table 1.

Disrupting the Kill Chain and Enhancing Health Care to Safeguard Against Attacks

The kill chain outlines the sequence employed by hackers or attackers to penetrate a network, potentially establishing a presence within it and subsequently extracting data from systems compromised by malware. We have recognised that the typical hierarchy of successful cyber attacks facilitates improved preparation to prevent both current and future breaches. This concept pertains to the framework of an attack in light of recent advancements in healthcare technology [16]. It involves the identification of targets, the deployment of forces to those targets, the decision - making and issuance of orders for the attack, culminating in the destruction of the target. The method kill chain incorporates defensive or preemptive measures. The following actions are defensible:

a) Identify: ascertain if an intruder is exploring
b) Deny access to prevent information disclosure and unauthorised access.
c) Disrupt: halt or modify outbound traffic (to the attacker)
d) Degrade: counterattack command and control
e) Deceive: disrupt command and control
f) Include: modifications to network segmentation

These sophisticated phishing attacks consistently lead to the most invasive and expensive breaches of PHI and other sensitive information. In medical testing, certain binary classifications may yield a false positive, leading to inaccuracies in data reporting when the test result incorrectly suggests the presence of a condition, such as a disease. It is referred to as positive; however, it may not actually be present. It can occasionally include false negative errors that inaccurately suggest the absence of data conditions and information security. - There are two types of errors in a binary test [17]. The false discovery rate (FDR) [18] represents the likelihood that a "significant" result is, in fact, a false positive.

The development of advanced antispam software remains essential in thwarting typical attacks, effectively positioning antispam initiatives as the primary line of defence. Recent developments in web filtering have emerged as an essential supplementary layer of defence- is entails the prevention of malicious links from directing unsuspecting users to websites that have been compromised by attackers. The cyber kill chain outlines the phases of a cyber attack, ranging from initial reconnaissance to the ultimate objective of data exfiltration. The kill chain can serve as a management tool to facilitate the ongoing enhancement of network defence. The driving forces highlighting the necessity for action indicate, as illustrated in Figure 1, that the current moment is exceptionally favourable for advancing the utilisation of data to meet the requirements of the health system.

Growth in Digital Data Volume

The defining properties or dimensions of big data are volume, variety, and velocity (3Vs). Volume denotes the quantity of data, variety indicates the diversity of data types, and velocity pertains to the pace of data processing. The 3V model indicates that the challenges associated with big data management arise from the growth of all three properties, not solely from the volume of data that needs to be managed.

The volume of accessible digital data is increasing rapidly. Data are provided by federal, provincial, territorial, and governmental entities. Significant financial resources are allocated to various information technologies to enhance the support, delivery, and coordination of health care services. For instance, over fifty percent of Canadian primary health care providers currently utilise electronic medical records in their practice, as opposed to just over one - third in 2009 (increasing from 37% to 56% in 2012) [7]. The implementation revealed that the health initiative requires enhancement to facilitate the accessibility of electronic data. For instance, electronic records at the point of service are being utilised more frequently in clinics, hospitals, and long - term care facilities.

The results obtained from diagnostic tests, including laboratory and diagnostic imaging reports, are frequently scanned in numerous services. Recent technological advancements facilitate the gathering of digitised data from sensory aids and surveillance devices utilised in both clinical and home environments, alongside emerging sources like genomic analysis and social networking platforms.

Technological Developments

A variety of methods are established to enhance appropriate technology within the health system, which is partially driven by technological advancements. Information technology has become more affordable and powerful compared to previous years, providing enhanced methods for managing information from any location. The new methods of analysis, the enhanced efficiency of treatment approaches, and the automation of existing analytical processes enable the drawing of conclusions based on health data and the presentation of the information obtained in a practical format. - Through innovative approaches, systems are capable of learning, integrating predictive and real - time functions, and processing unstructured data, such as in natural language processing. The results indicate that the existing technology must be enhanced to effectively address the project objectives and ensure the clarity of the information generated through the digitalisation of health data, which is essential for health security. Technological advancements will enhance privacy and security measures, leading to improved utilisation of health data to inform decision - making within health systems. The electronic collection of personal health information is increasingly becoming a focus for policymakers in order to enhance the security and privacy of personal data. Users are increasingly gaining access to tools that enhance the safety and security of healthcare data, as well as the confidentiality of private healthcare information. The design and implementation of suitable security and privacy measures are derived directly from health.

The design and implementation of suitable security and privacy measures are derived from health information systems, which is a crucial factor that can enhance the utilisation of data to inform decision - making within the healthcare system [13].

Table 1: Treats and corresponding impacts

Security concern/threat	Impact
Information disclosure (loss of confidentiality)	Patient embarrassment; loss of trust; legal consequences; loss of reputation
Withholding information or services (loss of availability)	Poor quality of services; Insufficient patient treatment; legal claims; Financial impact
Modification of information (loss of integrity)	Insufficient or inappropriate patient treatment; poor management; financial loss
Table of repudiation	Financial loss; lack of accountability; loss of reputation
Nonauditability	Poor management; inability to claim penalties and take legal action
Loss of authenticity/validity	Insufficient patient treatment

Paper ID: SR241013121605 DOI: https://dx.doi.org/10.21275/SR241013121605

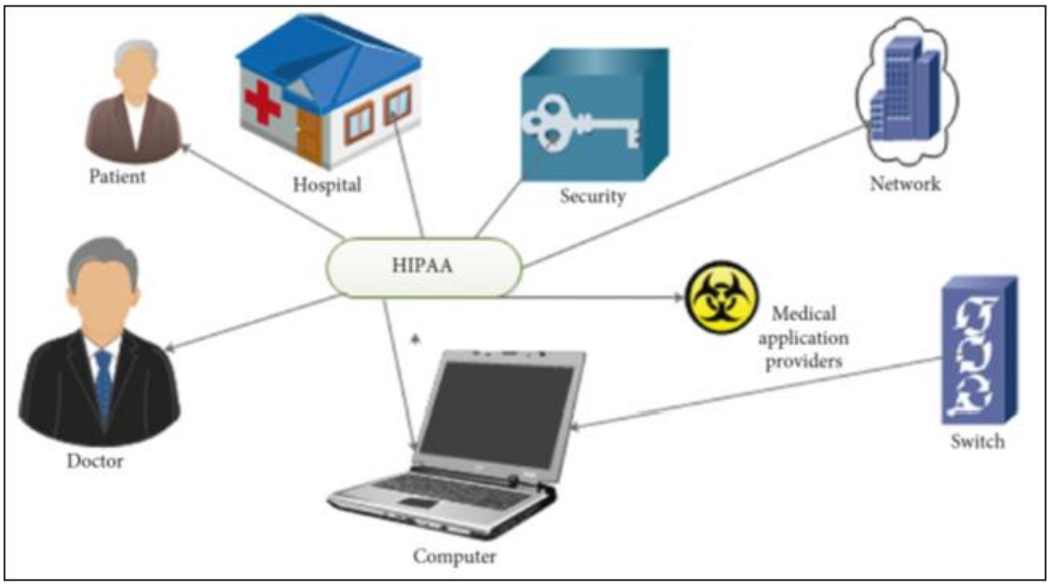

Figure 1: Information system

4. Fundamental Privacy of Selfhood Identifiable Information System for the HIPAA Privacy Rule

HIPAA establishes comprehensive requirements for the safeguarding and confidentiality of patient data, significantly altering the perspectives and approaches of health services, insurance, life sciences, and other organisations regarding health issues, security, and confidentiality. From a technological standpoint, HIPAA encompasses a broad spectrum of domains, including websites, medical devices, electronic medical records, and medical imaging.

Recent technology trends, such as the success of virtualisation, cloud computing, devices, and mobile applications, have introduced new challenges for payers and health service providers in their efforts to comply with HIPAA.

Solutions can assist organisations in fulfilling HIPAA requirements while also enhancing their overall security and risk management strategies. These solutions offer effective protection against threats in customer premises, in virtualized environments, and on mobile devices. The document provides a summary of its influence across various technology sectors, along with an analysis of how trends like cloud computing and mobility may impact compliance initiatives. This report also outlines how existing solutions can assist companies in their efforts to comply with HIPAA today and the conception of individualism is based on the right to privacy in the insistence on maintaining the confidentiality of the idea. Concern regarding healthcare privacy is paramount, as individuals desire to maintain confidentiality by fostering an environment free from interference. The emphasis is placed here on the deceased, which individuals seek to establish selfhood. Health privacy is intertwined with personal choices and access to health information.

It can be perceived as a confidential domain of existence from which individuals not involved in the healthcare security sector may be excluded. Therefore, these different conceptions, along with the related criteria, are presented in the first part to delineate the right to privacy. In the subsequent section, it is essential to define the extent of the supervision implemented by the employer. The analysis focusses on the reasonable expectation of privacy of the employee, the waiver of the right to privacy, and the limitation of this right based on the principles of rationality and proportionality. - The NPP is required to inform patients about the uses and disclosures of PHI that the practice may undertake, as well as to clarify the patient's rights to access and amend their medical information. Additionally, individuals are entitled to review and obtain a copy of their protected health information.

1) Administrative Safeguards

There is a necessity to practice, develop, and uphold current policies and procedures aimed at educating and assisting individuals in safeguarding the security of PHI. Examples of administrative safeguards include the following:

Acceptance of policies that empower trainers or employees with the rights and responsibilities for handling PHI. Sanction policies are essential for addressing violations of HIPAA law by employees.

Information access policies provide suitable access to computer workstations, health records, transactions, and other programs or processes. It is essential to implement security awareness training. Employees receive training and are regularly reminded of the policies and procedures concerning software updates, computer log monitoring, password updates, and other essential security measures. Contingency planning involves ensuring that appropriate preparation policies and procedures are established to effectively respond to emergencies. In the event of fire, vandalism, or other natural disasters, it is essential to develop, test, and revise an incident and emergency response plan, with all critical activities assigned to a designated owner.

2) Technical Safeguards

Practices require established procedures along with appropriate software and equipment to ensure the protection of PHI. Practices are required to establish technical policies and procedures that facilitate access for individuals who need it to perform their job functions effectively. Practices must include encryption and decryption in the processes of backing up, restoring, and transmitting electronic patient information.

It is essential to establish policies and procedures for the destruction of PHI when it is no longer required to perform a job or function.

a) **Physical Safeguards:** It is essential to implement measures to safeguard the location and devices within your practice. Access controls for the facility must be established, and all access should be monitored. It is essential to comprehend and oversee who is accessing the practice, ensuring that security measures are established both prior to and following any potential incident. HIPAA mandates that each practice appoint a security officer and a privacy officer for compliance.
b) **Patient Security:** The patient's safety is characterised by minimising any potential risk of avoidable harm to the patient. The main objective is to prevent any reversal of the benefit/risk to be addressed [17]. An adverse event related to care is an unforeseen occurrence that interrupts or postpones the care process or directly affects the patient's health. This event results from the actions taken in prevention, diagnosis, or treatment. It diverges from the anticipated outcomes or standards of care and is not associated with the natural progression of the disease [18]. This adverse event can be classified as severe (AES) if it involves an unexpected death, a serious complication affecting vital prognosis, or a permanent loss of function that is not attributable to the natural progression of the disease. Technology security officers receive training from various organisations, as illustrated in Figure 2; it represents a system that includes SANS, Microsoft, and the computer system industry.
c) **Oversee the Risk Management Process:** A risk management approach focusses on ensuring patient safety and the quality of care provided, specifically aiming to minimise the likelihood of adverse events and mitigate their potential consequences.
d) **Unfavourable Incident:** An adverse event associated with care (EIAS) refers to an unforeseen occurrence that interrupts or postpones the care process or has a direct effect on the patient's health. The establishment of a safety culture is also achieved through the development of professionals. It is essential to prioritise the instruction of these concepts early in the training of future professionals. The World Health Organisation (WHO) has released a pedagogical guide for health professionals, outlining essential elements for teaching the fundamental principles and concepts of patient safety [19, 20].

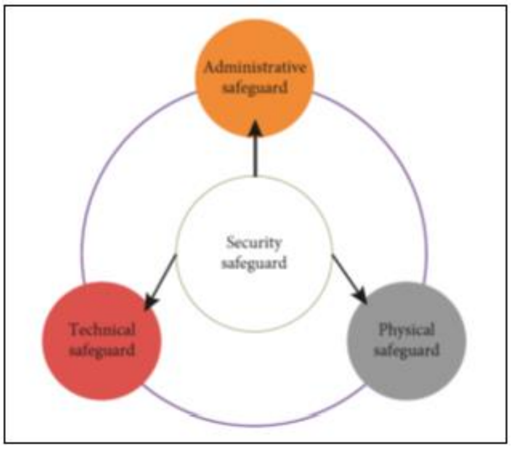

Figure 2: Process of HIPAA

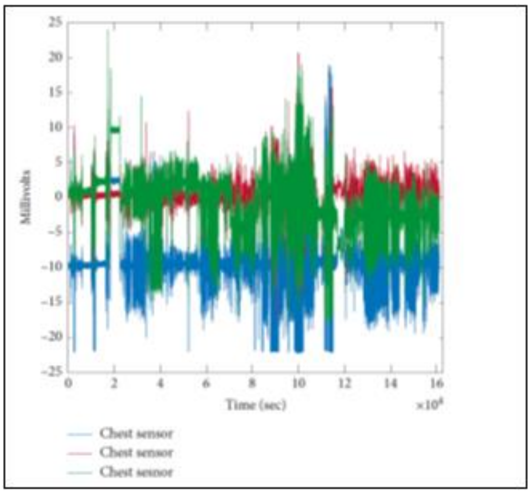

Figure 3: Acceleration from the chest sensor

5. Experimentation and Validation

The data utilised originates from the University of Granada (UGR), gathered by Oresti Bonas, Rafael Garcia, and Alejandro Saez on October 22, 2013. The units of measurement include acceleration (m/s²), gyroscope (deg/s), magnetic field (local), and ECG (mV). Figure 3 illustrates the significant acceleration recorded by the chest sensor, particularly during the midtime measurement. - indicates that managing such large data sets is quite challenging. Data mining is an effective approach for extracting information, facilitating the organisation of data by category. The electrocardiogram signal curve illustrates the variations in data recorded during the patient's examination in the clinical service. In this instance, it has been observed that the data must be substantial; however, it is essential for preservation. Should the patient encounter a similar issue in the future, the hospital can refer the patient to other clinics, allowing them to access the most recent results from various facilities, thereby facilitating accurate disease diagnosis. The previous result output can be utilised in the evaluation of the disease and can therefore inform the decision regarding any changes to examination or diagnostic materials. Figure 4 presents the histogram of the magnetometer data obtained from the left - ankle sensor. Figure 5 presents the curve of the Gyro from the right - lower arm sensor. The response differs significantly from that shown in the electrocardiogram signal depicted in Figure 4. The gyro from the right - lower - arm sensor demonstrates significant vibration, with the exception of the maximum phase. Figure 6 presents the histogram of the magnetometer data collected from the left - ankle sensor, illustrating the movement associated with the left ankle.

The sensation is observed to be approximately zero, fluctuating between - 100 and +100. The primary sensation is close to zero, with the maximum value recorded at zero.

Figure 7 illustrates the histogram of the magnetometer data from the right - lower - arm sensor, which demonstrates a movement rate comparable to that of the left - lower - arm sensor. Nonetheless, the scale is distinct. The highest value is 2.5, compared to over 4.5 in Figure 6.

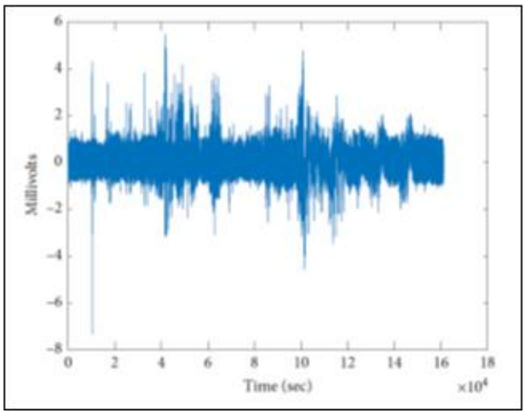

Figure 4: Electrocardiogram signal

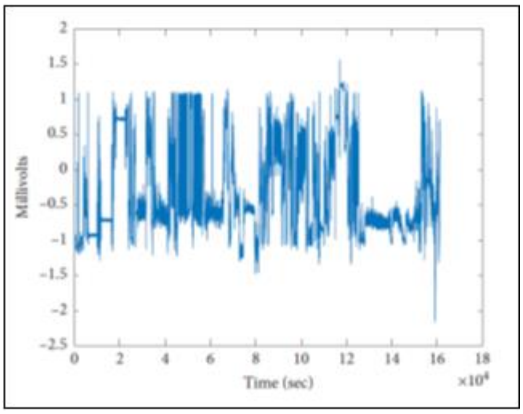

Figure 5: Gyro from the right - lower - arm sensor.

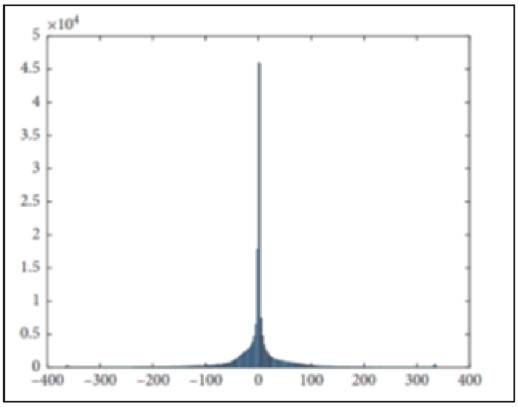

Figure 6: Magnetometer from the left - ankle sensor

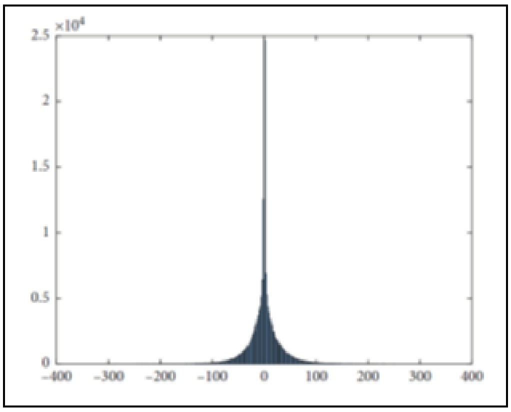

Figure 7: Magnetometer from the right - lower - arm sensor

6. Conclusions

Information technology in health care plays a crucial role in safeguarding patients' lives and ensuring the security of their information. This situation may result in complex legal and ethical challenges for mental health professionals. Occasionally, the patient returns for additional treatments, and in such instances, it is straightforward to access their data, which aids in understanding the evaluation of the disease. One may perceive the endeavour of educating potential clients and fellow practitioners about health data services as a delicate balancing act, particularly when aiming to enhance experiences through social networks and data services. It is expected that matters concerning health care can be effectively addressed online, providing individuals with a sense of security due to HIPAA compliance. Technology is continuously evolving, presenting both positive and negative implications, along with associated risks. It is essential to recognise that insurance should not serve as your sole risk management strategy. To avoid potential lawsuits, it is essential to remain informed about current regulations. It is advisable that if an individual is uncertain about the data utilised, they should reach out to the secure data provided by industries or professional associations that have demonstrated significant advancements in healthcare technology.

References

[1] J. Lu, A. V. D. Bossche, and E. Campo, “An IEEE 802.15.4 based adaptive communication protocol in wireless sensor network: application to monitoring the elderly at home, ” *Wireless Sensor Network*, vol.6, no.9, pp.192–204, 2014.

[2] K. Hill, *How Target Figured Out a Teen Girl Was Pregnant before Her Father Did*, Forbes, Jersey City, NJ, USA, 2012.

[3] G. Dhillon and J. Backhouse, “Technical opinion: information system security management in the new millennium, ” *Communications of the ACM*, vol.43, no.7, pp.125–128, 2000.

[4] B. Data in *Proceedings of the 5th International Conference on Intelligence Science and Big Data Engineering, IScIDE*, vol.9243, pp.1–626, 2015.

[5] G. Par´e, M. - C. Trudel, M. Jaana, and S. Kitsiou, “Synthesizing information systems knowledge: a typology of literature reviews, ” *Information & Management*, vol.52, no.2, pp.183–199, 2015.

[6] J. L. Austin, *Philosophical Papers*, Oxford University Press, Oxford, UK, 1961.

[7] M. Viceconti, P. Hunter, and R. Hose, “Big data, big knowledge: big data for personalized healthcare, ” *IEEE Journal of Biomedical and Health Informatics*, vol.19, no.4, pp.1209–1215, 2015.

[8] P. Gomez and R. Chevallet, “Impacts des technologies de l’information sur la sant´e au travail. Hypoth`eses et interpretations `a partir d’une observation exp´erimentale, ” *Revue Française de Gestion*, vol.37, no.214, pp.107–125, 2011.

[9] A. Visvanathan, A. P. Gibb, and R. R. W. Brady, “Increasing clinical presence of mobile communication Technology: avoiding the pitfalls, ” *Telemedicine and e - Health*, vol.17, no.8, pp.656–661, 2011.

[10] A. Appari and M. E. Johnson, “Information security and privacy in healthcare: current state of research, ” *International Journal of Internet and Enterprise Management*, vol.6, no.4, pp.279–314, 2010.

[11] R. Ologeanu - Taddei and G. Par´e, “Technologies de l’information en sant´e: un regard innovant et pragmatique, ” *Syst`emes D’information & Management*, vol.22, no.1, p.3, 2017.

[12] C. Diana, “How I learned to stop worrying and love the hackers, ” *Interactions*, vol.15, no.2, pp.46–49, 2008.

[13] Institut Canadien D’information sur la Sant´e, *Une meilleure information pour une meilleure sant´e: vision de l’utilisation des donn´ees pour les besoins du syst`eme de sant´e au Canada*, Institut Canadien D’information sur la Sant´e, Ottawa, Canada, 2013.

[14] R. April and R. April, “General overview of standards for privacy of individually identifiable health information, ” *Search*, vol.502, pp.2002 - 2003, 2003.

[15] J. J. M. Seddon and W. L. Currie, “Cloud computing and trans - border health data: unpacking US and EU healthcare regulation and compliance, ” *Health Policy and Technology*, vol.2, no.4, pp.229–241, 2013.

[16] M. Flyverbom, R. Deibert, and D. Matten, “ - e Governance of digital technology, big data, and the internet: new roles and responsibilities for business, ” *Business & Society*, vol.58, no.1, pp.3–19, 2017.

[17] A. Bagula, “Applications of wireless sensor networks, ” 2012, http: //wireless. ictp. it/wp - ontent/uploads/2012/02/WSN - Applications. pdf.

[18] Y. Weiss, A. Torralba, and R. Fergus, “Spectral hashing, ” in *Proceedings of the Advances in Neural Information Processing Systems*, pp.1753–1760, Vancouver, BC, Canada, December 2008.

[19] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, “Security techniques for the electronic health records, ” *Journal of Medical Systems*, vol.41, no.8, p.127, 2017.

[20] L. Shi, M. Li, S. Yu, and J. Yuan, “BANA: body area network authentication exploiting channel characteristics, ” *IEEE Journal on Selected Areas in Communications*, vol.31, no.9, pp.1803–1816, 2013.