Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 1927495, 7 pages
https://doi.org/10.1155/2019/1927495

Research Article

Healthcare Data Security Technology: HIPAA Compliance

Scholas Mbonihankuye,[1] **Athanase Nkunzimana**,[2,3] **and Ange Ndagijimana**[1]

[1]*Department of Computer Science and Technology, Nanjing University of Information Science and Technology, Nanjing 210044, China*
[2]*Department of Geographical Sciences, Nanjing University of Information Science and Technology, Nanjing 210044, China*
[3]*Department of Geography, University of Burundi, P. O. Box 5142, Bujumbura, Burundi*

Correspondence should be addressed to Scholas Mbonihankuye; scholas.mbonihankuye@yahoo.fr

Received 22 June 2019; Accepted 5 September 2019; Published 17 October 2019

Guest Editor: Iván García-Magariño

Information technology (IT) plays an increasingly important and prominent role in the health sector. Data security is more important than ever to the healthcare industry and in world in general. The number of data breaches compromising confidential healthcare data is on the rise. For data security, cloud computing is very useful for securing data. Due to data storage issue, there is a need to use the electronic communication, and a number of methods have been developed for data security technology. Health Insurance Portability and Accountability Act (HIPAA) is one of the methods that can help in healthcare research. On stored database of patient in hospital or clinic, we can develop a conservational and analytical method so as to keep the medical records of the patients in a well-preserved and adequate environment. The method includes the improvement of working possibilities by delivering all the details necessary for the patient. All the information must be identified clearly. The protection of the privacy of the patients and the security of their information are the most imperative obstacles to obtain their intakes when considering the adoption of useful health data in the electronic field of healthcare industries.

1. Introduction

Health is very important and concerns all living things including human beings, the plants, the animals, the space, and the environment. The safety issue is becoming of more concern and concerns the security for all. In order to conduct a study on the technology that one can use to handle healthcare issues, it is important to look for all means that can enable to create a livable environment where people and surrounding live healthy and in harmony. The risk management determines the precautions to be taken regarding the nature of the data and surrounding environment. During the data treatment process, it is suggested to take all the precautions so as to avoid all the risks and preserve the data security as stated in the Article 34 of the Law known as "Informatics and Freedoms."

The research done by European regulation 2016/679 on 27 April 2016 (known as "General Data Protection Regulations" or RGPD) specifies that the protection of personal data requires taking appropriate technical and organizational measures to ensure level of safety appropriate to the risk and security of health care of a patient [1, 2].

Communication is a key element in the construction of the caregiver-groomed relationship. The lack of communication has a direct impact on the quality and safety of the patients. The literature is abundant on this subject, on the one hand to show that the lack of communication is one of the major causes of EIAS and on the other hand to underline the difficulties of patients to understand the medical explanations. These difficulties of understanding increase the mortality rate. Multiple actions are being developed to this effect, particularly within the framework of the National Patient Safety Program (PNSP) to improve patient safety for health professionals and users. Such an approach allows for objective decision making and the determination of measures strictly necessary and appropriate to the context. However, it is sometimes difficult, when you are not familiar with these methods, to implement such an approach and to

ensure that the minimum has been implemented. In order to develop the field of data security policies, it is of high concern to know how to store and secure the data to avoid any losses. This requires to have enough knowledge about data security policies.

Main significance of our study is the influence of the diffusion of digital tools: dematerialization and individualization of tasks, increase of mobile work, secure data on physical and space, aspiration or injunction to autonomy, porosity of times of pro/personal life, and expansion of the company or enterprise. In previous years, the data management in health care was based on the security technology to support decision makers to establish a good data control and management. Many of these sources showed that including hospital information systems and medical service facture systems may be valid to date. The debate regarding the privacy of medical records has been sharpened by several long-term trends. Achieving consensus regarding safeguards for an information system, among different stakeholders in an organization, has become more difficult than solving many technical problems that might arise [3]. They are rushing headlong into adopting IT without carefully planning and understanding the security concerns, which creates future problems [4, 5]. The impacts of security breaches of company protocols that inadequately protect stored records are much more significant than paper records. However, as technology progresses, the potential for more intrusions into personal medical records will grow, particularly in the area of DNA testing. The potential use of DNA test results by insurers and employers to exclude "undesirables" from risk pools is becoming more and more evident.

1.1. Objective. The HIS is a system that aims to provide internal and external communication among healthcare providers. Hospital Information Systems provide a common source of information about a patient's health history. The system has to keep data in a secure place and control who can reach the data in certain circumstances.

These systems enhance the ability of healthcare professionals to coordinate care by providing a patient's health information and visit history at the place and time that it is needed.

The originality of HIPAA compliance is that it is a method very secure of patient data and privacy, especially adoption of electronic healthcare records. As the data have different formats, the HIPAA enables to create a good format which is appropriate to facilitate data access and data control.

1.2. Literature Review. The article written by Dumez and Minvielle was found to be very interesting and innovative since it focused on health-proofed sanitary, in a context where these concepts are still poorly defined. The authors propose a narrative review of the literature [5], with the objective of analyzing the rebalancing of power in favor of the patient in the context of e-health. In the affiliation of the works of Austin [6], the authors retain the performativity as a reading grid of the previous writings. They pay particular attention to the notions of "performativity framed," which occurs when a theory foresees the devices that will enable to make the practices effective, and "performativity by overflow," which occurs when devices not anticipated by the theory (in this case that of the health democracy) are put in place and make the practices and performance in an unexpected way. The analysis highlights four cases of engagement associated with e-health: the case of coconstruction between patients and health professionals; the case of coconstruction with increased expertise acquired by patients via e-health; the case of autonomous management of the disease; and the status quo [7]. The authors accurately underline the paradox of autonomous management of the disease where the patient-physician relationship would be rebalanced, as a result of the information the patient acquires, whereas a new relationship of dependency and asymmetry is created in relation to e-health operators, due to safety risks and abusive uses of data generated by connected health. The physical painfulness was strong before the introduction of the voice system.

The analysis of the demographic data of the company shows a constant renewal of the population of the order preparers. They are rarely held in employment beyond 5 years of seniority. The research done by Gomez and Chevallet shows that half of the preparers hired around 2002, who were between 25 and 34 years old, are no longer preparing in 2007 [8]. There were 57 recruitments on a total workforce of 110. A very young recruited population (51 operators are between 18 and 24 years old), at 100% male, and without qualifications: the consecrated expression is to say that one recruits a physical force, something all the easier in the context of a local employment pool [9, 10]. ARRA is another method of record data with adoption electronic of system for following meaning use policies. But it is not upgraded to facilitate the medical system store even if it has 100% digital records, the health care still facing on penalties, and it is necessary to care about the privacy of patient's data. According to the study "Collaboration 2020: hype or competitive advantage?" of Johnson Controls published in 2012, this is only the beginning of a profound evolution. According to Johnson Controls, collaboration platforms should continue their development to accompany teamwork of collaborators located on different sites [11, 12]. The current abundance of IT implementation projects in healthcare facilities in Europe, North America, and elsewhere in the world provides a privileged ground for studying a range of research questions specific to the field of systems of information. To name a few, these include organizational and individual adoption, resistance to change, escalation of projects, strategic alignment, or the governance of information systems. These issues are of particular importance in hospital organizations, which are one of the most complex organizational models. The development of the uses of digital health is currently being apprehended as a source of transformation of the health system which can substantially reshape its functioning.

In order to present the strategic actions in promoting the evaluation of health technologies in developing and emerging countries with the security and to facilitate the

information decision making on the introduction of the health systems evaluation and make a good security of all data. In the purpose of having better information for better health system which sometimes intended to subset secondary data in order to strengthen clinical care programs for easy data working and management so as to secure the population's health as shown in Table 1.

1.3. Interrupting the Kill Chain and Advanced Health Care to Secure Attacks. In the steps of kill chain, the series used by hackers or attackers to infiltrate a network may establish residency in the network [13–15] and then extract data from the network of the data infected by virus. We have understood that typical hierarchy of successful cyber attacks allows for better preparation to prevent the current and future breaches. It is a concept related to the structure of an attack with the recent development of healthcare technology [16], consisting of target identification, force dispatch to target, decision and order to attack the target, and finally the destruction of the target. Method kill chain has defending or preemptive action. Defensible actions are as follows:

(i) Detect: determine whether an attacker is poking around

(ii) Deny: prevent information disclosure and unauthorized access

(iii) Disrupt: stop or change outbound traffic (to attacker)

(iv) Degrade: counterattack command and control

(v) Deceive: interfere with command and control

(vi) Contain: network segmentation changes

These sophisticated phishing attacks constantly result in the most invasive and costly attacks on PHI and other sensitive information. In medical testing, some binary classifications may find a false positive which results in some errors in data reporting when the test result improperly indicates presence of a condition such as a disease. It is called positive though in reality it is not present; it sometimes contains false-negative error which improperly indicates the no presence of data condition and information security. There are two kinds of errors in a binary test [17]. False discovery rate (FDR) [18] is the probability that a "significant" result is a false positive. Advanced antispam software development continues to be crucial in preventing a typical attack, essentially making antispam efforts the first line of defense. Advances in web filtering have been developed as a vital "second line" of defense. This involves preventing malicious links from leading unknowing users to websites that have been compromised by attackers. Cyber kill chain reveals the stages of a cyber attack: from early reconnaissance to the goal of data exfiltration. The kill chain can also be used as a management tool to help continuously improve network defense. Driving forces exposing the need to act show us in Figure 1 that a moment has never been so conducive to the progression of the use of data for the needs of the health system.

1.4. Increasing Volume of Digital Data. Three defining properties or dimensions are volume, variety, and velocity of big data (3Vs). Volume refers to the amount of data, variety refers to the number of types of data, and velocity refers to the speed of data processing. According to the 3V model, the challenges of big data management result from the expansion of all three properties, rather than just the volume alone—the sheer amount of data to be managed. The amount of accessible digital data increases rapidly. Data are made available by federals, provinces, territories, and governments. Billions of dollars are injected into various information technologies in order to support, deliver, and coordinate the health care. For example, more than half of Canadian primary health care providers now use electronic medical records as part of their practice; this is the research done for compared just over one-third in 2009 (from 37% to 56% in 2012) [7]. The implementation found that the health initiative has to be improved and has to enable the accessibility of electronic data. For example, electronic records at the point of service are increasingly being used in clinics, hospitals, and long-term care facilities. The results obtained from diagnostic tests, including laboratory and diagnostic imaging reports, are also scanned in many services. Technological advances enable the collection of digitized data from sensory aids and surveillance devices used in clinical and home settings, as well as new sources such as genomic analysis and social networking sites.

1.5. Technological Advances. Many means are set out in order to improve a suitable technology in health system, which is partly induced by technological advances. Information technology is now cheaper and more powerful than a few years ago and offers more ways of dealing with information from anywhere. The new methods of analysis, the increased efficiency of the methods of treatment, and the automation of current analytical analyses facilitate, for example, the drawing of conclusions based on data on health and presentation of the information obtained in a usable format. Through innovations, systems can learn, integrate predictive and real-time functions, and process unstructured data (as in natural language processing). The result found has shown that the current technology should be better to deal with the project goals and check the clarity of the generated information by the digitalization of the health data useful for health security.

Technological advances will also contribute, through the strengthening of privacy and security options, to better use of health data in order to inform health system decision making. The electronic collection of personnal health information is becoming more and more the preoccupation of policy makers or order to enhance tre security and privacy of personnal data. Fortunately, users are beginning to have tools to ensure the safety guide of healthcare data security and the secrecy of private healthcare information. The design and implementation of appropriate security and privacy measures are directly obtained from health

Table 1: Threats 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

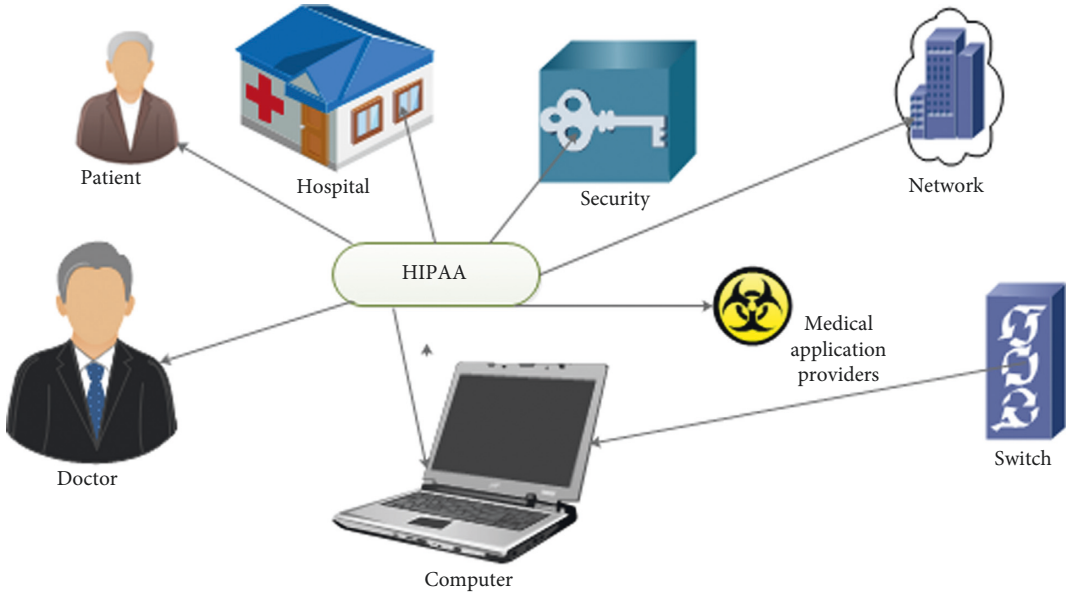

Figure 1: Information system.

information systems which is an important condition that may appropriate the used data to lighten the decision making on the healthcare system [13].

2. Standard Privacy of Selfhood Identifiable Information System for the HIPAA Privacy Rule

HIPAA has detailed requirements for the protection and confidentiality of patient data and has changed the way of how health services, insurance, life sciences, and other companies view and address health problems, security, and confidentiality. From a technology perspective, HIPAA covers a wide range of areas including websites, medical devices, electronic medical records, and medical imaging. A number of recent technology trends, including the success of virtualization, cloud computing, devices, and mobile applications, have created new challenges for payers and health service providers to comply with HIPAA. Solutions can help companies meet HIPAA requirements as well as improve their overall security and risk management situation. These solutions provide effective protection against threats in customer premises, in virtualized environments and on mobile devices. It includes a summary of its impact on a number of technology areas, as well as how trends such as cloud and mobility can affect compliance efforts. This report also describes how current solutions can support companies in their efforts to comply with HIPAA today and individualism conception based the right to privacy in Insistence of idea secret, Concern healthcare privacy, all person want to keep secret by developing an area free from interference [14]. The emphasis is placed here on the dead which individual want to do selfhood. Liberty of health privacy confided with personal must do or not and knowledge access in health. Thus allows to be conceived as a secret sphere of life from which it is possible to dismiss the people that are not concerned by the healthcare security field. Therefore, these different conceptions as well as the related criteria are presented, in a first part, to delimit the right to privacy. In a second part, it is a matter of establishing the scope of the supervision exercised by the employer. The analysis then aims at the reasonable expectation of privacy of the employee, the renunciation of the right to privacy, and the

restriction of this right based on the criteria of rationality and proportionality. The NPP must inform patients of the uses and disclosure of PHI that the practice may make and define the patient's rights to access and amend their medical information, and individuals have the right to review and obtain a copy of their protected health information [17, 18].

2.1. Administrative Safeguards. There is a requirement to practice, create, and maintain updated policies and the procedures used to learn and help followers to maintain the security of PHI.

Some examples of administrative safeguards include the following:

(i) Acceptance use of policies that help trainers or employees to have the right and responsibilities to handing PHI.

(ii) Sanction policies are needed to discipline employees who violate HIPAA law.

(iii) Information access policies grant appropriate access to computer workstation, health records and transaction, and other programs or processes.

(iv) Security awareness training must be implemented. So, employees are trained and reminded of policies and procedures relating to software updates, computer log monitoring, password updates, and other key security measures.

(v) Contingency planning, so adequate preparation policies and procedures are in place in order to respond to an emergency; if there is fire vandalism or other natural disasters, an incident and emergency response plan must be created, tested, and revised and all critical activities must have a designated owner.

2.2. Technical Safeguards. Practices need procedures and the right software and equipment to protect PHI. Practices must implement technical policies and procedures to allow access to any of those people who need access to do their jobs. Practices should incorporate encryption and decryption in backing up, restoring, and transmitting electronic patient information. Policies and procedures must be set up to destroy PHI when it is no longer necessary to fulfill a job or function.

2.2.1. Physical Safeguards. It must be implemented to protect the location and devices within your practice. Facility access controls must be created, and all access must be monitored. It is important that you understand and monitor who is accessing the practice, and security measures are put in place prior and after a potential incident. HIPAA requires that every practice designate a HIPAA security and HIPAA privacy officer.

2.2.2. Security of Patient. The patient's safety is defined as reducing any risk of preventable harm to the patient. It has the primary ambition to avoid any reversal of the benefit/risk to be treated [17]. An adverse event associated with care is an unexpected event that disrupts or delays the care process or directly impacts the patient in his or her health. This event is a consequence of the acts of prevention, diagnosis, or treatment. It deviates from the expected results or expectations of care and is not related to the natural evolution of the disease [18]. This adverse event can be severe (AES) as an unexpected death, a serious complication involving the vital prognosis or permanent loss of a function that does not result from the natural evolution of the disease. Technology security officers are trained by many different organizations as shown in Figure 2; it is a system with sans, Microsoft, and the computer system industry.

2.2.3. Manage the Risk. A risk management approach aims to ensure the safety of the patient and the care that is delivered and in particular to reduce the risk of adverse events for the patient and the severity of their consequences.

2.2.4. Undesirable Event. An adverse event associated with care (EIAS) is an unexpected event that disrupts or delays the care process or directly impacts the patient in his or her health. The development of a safety culture also goes through the formation of professionals. Teaching these concepts at an early stage in the training of future professionals should be a priority. As such, the World Health Organization (WHO) has published a pedagogical guide for all health professionals that provides all the elements for teaching basic principles and concepts of patient safety [19, 20].

3. Experiment and Validation

The data used are from the University of Granada (UGR), collected by Oresti Bonas, Rfael Garcia, and Alejandro Saez on October 22, 2013. The units of measurement are acceleration (m/s^2), gyroscope (deg/s), magnetic field (local), and ECG (mV).

In Figure 3, it can be seen how the acceleration from the chest sensor is very high especially during the midtime measurement. This means that it is not easy to handle such big data. Data mining is a good method for extracting data to enable picking up data by category.

The curve of electrocardiogram signal shows the variation of the data about the record done when examining the patient in the clinic service. In this case, it has been seen that the data must be very big, but it is necessary for saving because if the patient has a matter again, the hospital can transfer the patient to other clinics, and they can find the last result from other clinics or hospitals that can easily enable disease diagnostic. The previous result output can used in the evaluation of the disease and therefore can be considered to take a decision whether to change examination or diagnostic materials. Figure 4 shows the histogram of magnetometer from the left-ankle sensor.

Figure 5 exhibits the curve of Gyro from the right-lower-arm sensor. Its response is quite different from the one presented by the electrocardiogram signal in Figure 4. The

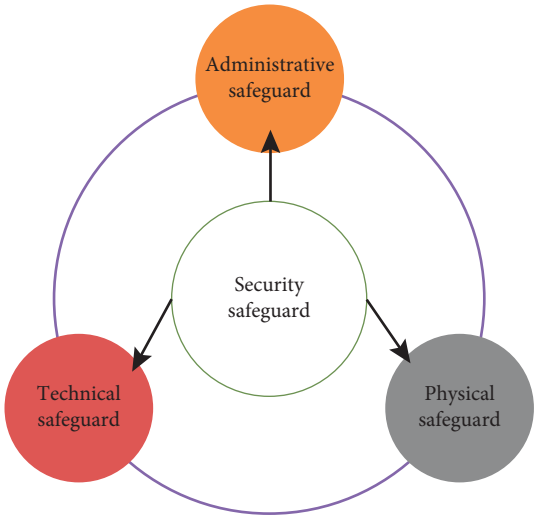

Figure 2: Process of HIPAA.

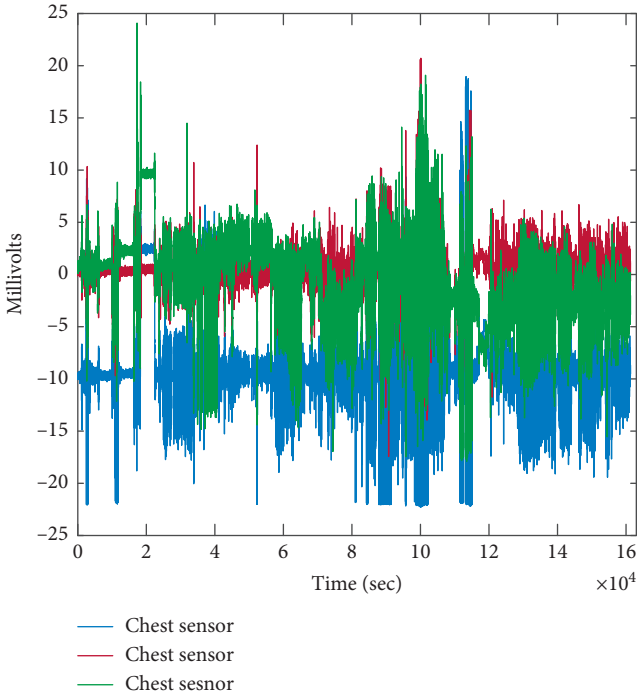

Figure 3: Acceleration from the chest sensor.

Gyro from the right-lower-arm sensor exhibits a high vibration except at the maximum phase.

Figure 6 shows the histogram of magnetometer from the left-ankle sensor that shows the movement on the left-ankle. It can be seen that the sensation is near zero varying from −100 to +100. The main sensation is near zero with the highest value observed at zero.

Figure 7 shows the histogram representing the magnetometer from the right-lower-arm sensor which exhibits similar movement rate as the left-lower-arm sensor. However, the magnitude is different. The highest value is 2.5, whereas it was more than 4.5 in Figure 6.

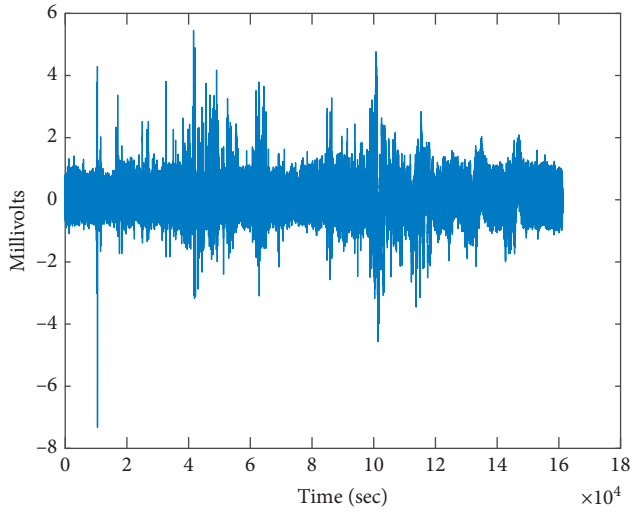

Figure 4: Electrocardiogram signal.

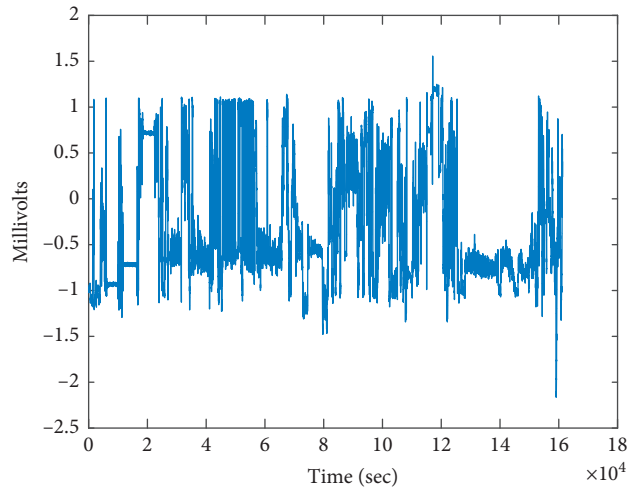

Figure 5: Gyro from the right-lower-arm sensor.

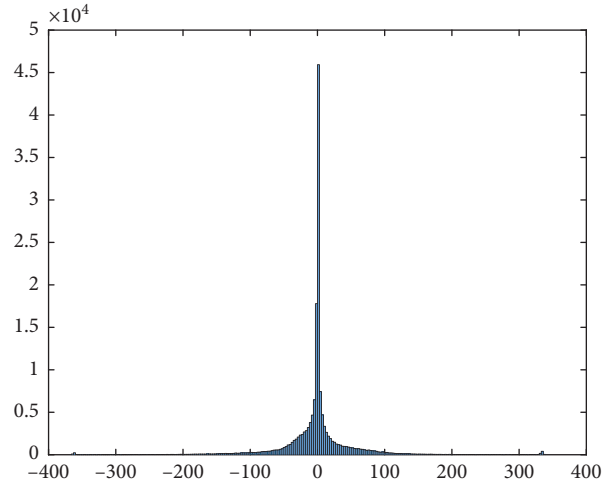

Figure 6: Magnetometer from the left-ankle sensor.

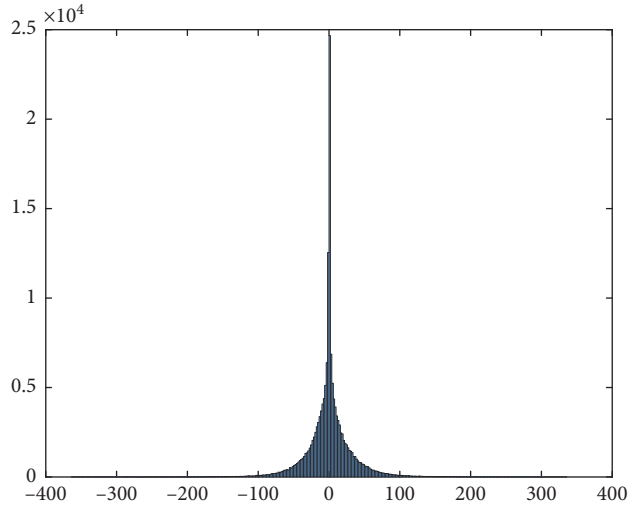

Figure 7: Magnetometer from the right-lower-arm sensor.

4. Conclusion

Information technology in health care is very important for patient's life or for clients especially in the security of their information. It can lead to tricky legal and ethical territory for mental health professionals. Sometimes, the patient comes back for other treatments, and in that case, it is easy to find his/her data, and it will facilitate to know how the disease is evaluated One might feel as though he is walking a fine jobs when trying to educate the potential clients and other practitioners of the services providing health data by improving the experiences through social network and data service. It is not surprising to see that for anything related to health care, people are able to get it resolved online and can truly feel secure enough by HIPAA compliance. Technology is always evolving such as in positivity action or negativity, and with it, we can get some risks. We must know that insurance should not be your only risk management tool. To prevent lawsuits in the first place, stay up to date on regulations. It is suggested that if someone is not sure about the data used, it is better to contact the secured data offered by industries or professional association that has a good evolution in healthcare technology.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

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. Paré, 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 santé au travail. Hypothèses et interprétations à partir d'une observation expérimentale," *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. Paré, "Technologies de l'information en santé: un regard innovant et pragmatique," *Systèmes 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 Santé, *Une meilleure information pour une meilleure santé: vision de l'utilisation des données pour les besoins du système de santé au Canada*, Institut Canadien D'information sur la Santé, 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, "The 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-content/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.