Journal of Business and Economics, ISSN 2155-7950, USA
September 2021, Volume 12, No. 9, pp. 958-963
DOI: 10.15341/jbe(2155-7950)/09.12.2021/004

http://www.academicstar.us

Securing Health and Personal Privacy on Medical Implantable Technological Devices in Healthcare Industry

Minh Hoang Dang
(Business Administration Department, FPT University, Vietnam)

Khoi Ho Anh Ngo
(Nam Can Tho University)

Abstract: The introduction of new information technologies applying in medical industry promises viable treatments for a number of diseases or healing human body defects. Among these, applying electronic implantable devices for medical purposes can be screened as one of the typical examples. However, the wide application of such devices for medical treatments has drawn some concerns over the security of personal privacy since the personal data are transmitted and stored on such devices and the connecting system. These concerns are even more emphasized on the cases where the operation of electronic implantable devices can be impacted due to the illicit motivations, which resulted directly on the health status of the patients. This article thus focused on demonstrating some risks that may happen to those who carry medical implantable devices to suggest some solutions to overcome the modern business dilemma situation of securing the health of patients while protecting their privacy. All are viewed on the background of the medical and technology development in the modern healthcare industrial world.

Key words: health economics; health care industry; medical implantable devices; personal information; personal privacy; information security

JEL codes: K14, K15, K22, K24, K38

1. Introduction

Medical implantable devices are used to install or implant on human body to treat a disease, improve the status or function of a specific part of the body or allow a person who gets implanted to have an ability to perform a task that they are impossible to do without the support of such devices (Hansen, 2010). Some medical implant devices applying widely nowadays can be named: pacemakers and defibrillators to monitor and treat cardiac conditions; neurostimulators for deep brain stimulation in cases such as epilepsy or Parkinson; drug delivery systems in the form of infusion pumps; and a variety of biosensors to acquire and process different biosignals. In the initial period, these devices were simply designed and focused on the appearance and physical functions

Minh Hoang Dang, LLM, Lecturer, Business Administration Department, FPT University; research areas: economics and law. E-mail: minhdh20@fe.edu.vn.
Khoi Ho Anh Khoi, Dr., Lecturer, Nam Can Tho University; Research areas: IT, IA and law.

(small size, durable battery) to adapt prescribed medical requirement. Recently, thanks to the rapid development of medical and information technologies, medical implantable devices can be integrated more functions to perform extra tasks (Callejon, 2012). These are designed with capability to transmit, exchange and store data of patients, their diseases and operational commands communicating between these devices and external system (Callejon, 2013). From such data, external system will store, analyze and generate reports serving physicalists and doctors to have information about patients' diseases and applying treatments, which may help them prescribe appropriate treating disease path. In many cases, modern computer system can handle this job on behalf of doctor's intervention by automatically commanding the implantable devices to adapt with patients' health conditions or, even the patients can adjust the implantable devices themselves if the system reports require simple tasks. Generally, this process can be considered as distancing collecting, analyzing patients' medica data before providing report, which are conducted wirelessly with the complimentary of electronic systems. Additionally, since the reports are produced by the computer system, patients may not need to present themselves at clinics or hospital but they can access to these reports simply via their smart phones or computers. Therefore, the development of both medical technologies and ICT has enabled implantable devices to be smarter and open larger opportunities for patients in disease treatments, in most flexible and convenient ways. On a global sphere and setting aside significant advantages of cost-effective, the data collected from patients could further expand the capability of computer system in establishing a network of observing and evaluating specific types of diseases in the community. This allows us to have a reliable source of data for medical researches as well as planning health care strategies in particular society.

From an overall perspective, integrating advance technologies into medical implantable devices to extend their functional features could be seen as a significant step in health care industry. The significant benefits from these 'smart' medical devices are undeniable. However, this also expose some potential risks relating to governance mechanism and patients' information security since their personal information and medical records are kept and stored electronically on the system. Hence, these concerns are gradually enhanced within the context of ICT development, where cyber-attacks are frequently happened due to certain illicit purposes. Such attacks, which can be conducted intentionally or negligently, can impact severely on the controlling of the external system and the operation of medical implantable devices. In another case, such attacks may set the target of changing or modifying the data collected from the medical implantable devices. As a consequence, the external system will analyze such wrong/ alternative data to have commands controlling the operation of implantable devices and thus enabling them to run over such commands. These actions put the medical status of patients under threats and sometimes it can result the patients' death. According to U.S. Food and Drug Administration (FDA), the attacks to which the targets are medical implantable devices and their respective controlling external system are difficult to identify. These attacks also cause the significant troubles in distinguishing between them and technical errors during the operation of such medical implantable devices (FDA, 2013). This gives raise to the need of comprehensive understanding of the operational process of medical implantable devices to have better preventions and resolution in case the unexpected incidents happen.

2. Potential Risks Analysis

Wireless connection and controlling, which are equipped on the latest generation of medical implantable devices, do exist some potential risks. These risks are even more highlighted when patients carrying these devices

do not often stay in medical environment with high attention of health care services (hospital, nursing homes…). In this light, some risks can be identified as following: firstly, the medical implantable devices are no longer invisible under human body as its design (Defend, 2008). Although these devices require to be implanted 2-3cm under skin, but these can be easily detected through their omission of communicating signals (Halperin, 2008). Secondly, the transmission of such signals via unsecured means can be a source of the infringement to the personal information and personal disease data. For example, the information of disease, programming of devices, prescribing methods, medical treatment tactics as well as other important information of patients' privacy, which are all stored on the system, can be possessed by hackers through a cyber-attack. Otherwise saying, the storage and communication of data conducted on a low-level security system do offer many risks of being attacked in a similar way happening in a normal computer network (Karger, 2009). After having data and successfully controlling the system, hackers can control or modifying the devices' operation easily without depending on the proximity to the victims (Panescu, 2008).

Until recently, there have been no recognized incident regarding to the information security of medical implantable devices in the real world, but the evidences of the possibility of conducting an attack to possess the control of such devices and their respective external systems were successfully proven in the laboratory (Halperin, 2008). Experiments conducted showed that hackers can control the system, reprogram the operation of the devices and create shocks to carriers by modifying its designed functional performance. Other tests aimed to make an effort in stopping the devices by depleting their battery and the result also demonstrated the high possibility to be happened. If this happens, victims should undertake some surgeries to replace a new one. The tests also shows that the magnetic atmosphere can have some certain influence on the medical implantable devices operation by causing the disability of pacemakers used to treat vascular cardio diseases (Medtronic, 2020). The possibility of magnetic attacks are clearer when the backtalkers get information about who are carrying such medical devices on their bodies due to a simple reason: switching off the peacemakers does not requiring the attackers to access the external system, which controlling the operation and functions of pacemaker medical devices implanted.

From the reasons as listed, the potentials of exploiting the loop hole of information security on the medical implantable devices are likely to be happen. The result of hacker successfully controlling the system is thus various and unprecedented. A medical device is created with certain function treating a specific disease or a certain deficiency of a part of human body, while the harmful impact can badly result on many aspects during the treating process (Hansen, 2010). For instance, an attack to the hearing supporter device could cause permanent deaf or headache and thus the sufferer may become distracted or failing to do their daily job effectively.

3. Preventions

In order to prevent informatic attacks conducted toward medical implantable devices as well as their carriers, it is highly recommended that new and modern devices must be equipped with strong mechanism in protecting privacy to ensure personal information security as well as the stable performance of these devices. For example, the mutual authentication between devices and medical staff is needed to secure that both parties are righteous ones with correct treatment methods and disease information. To medical implantable devices, only authenticated commands are eligible to receive and process while on the other hand of medical staff, they only consider data extracted from the authenticated devices without caring any other sources. Securing data storing and communicating via wireless connection also attract high attention. Devices (implanted and external) should have

privacy policies to minimize to the most any intervention from any unauthorized parties. This is to make sure that only the authorized ones can exploit such data and for the sole medical purposes. Protecting the integrity and correctness of data during transmission is also important. For example, if data is alternated or modified during the communication, a doctor may prescribe wrongly since his decision is based on the report generated, which is built on the basis of modified data. Additionally, if the external system communicates the commands to the devices and these are modified, the receiving devices will without doubt perform accordingly and thus form a significant risk to the patients' health.

Against that background, technologies and authentication mechanism should be equipped and integrated on the implantable devices from the very beginning of designing phase, in line with applicable regulations and recognized standards. However, the legal framework in the world and Vietnam governing this issue seems remaining unfulfilled. The quality control of medical implantable devices thus remains a lot of concerns. According to some data collected in the US within 10 years (2007-2018), there were approximately 3.6 millions incidents and errors of medical devices recorded, which caused 82.000 causalities and 1.7 millions got injured (Kim Tuyen, 2019). In Vietnam, the degree No. 36/2016/NĐ-CP governing the matter of medical equipment stipulates that implantable devices are classified as one of medical devices requiring the fulfillment of certain conditions before applying for treatment. Moreover, the code of national standards No. TCVN 6796:2001 (ISO 8828:1998) defining implantable materials used in surgery also mentions this issue. However, there is an absence of a detail guideline on the security of private information on both implantable devices and external system. In this light, if an information attack in Vietnam aiming at patients who are using implantable devices is conducted, the trial should be proceeded based on the regulations of information attacks on cyberspace or the laws governing the use and management of medical equipment? This refers to the necessity of having assessment methods and quality control in terms of personal information security of implantable devices, which are defined in laws. The implantable devices must meet these requirements before widely applying. In addition to that, the result of assessment as well as the security standards integrated on such implantable devices should be published, which is to serve the reference of medical professionals and patients before choosing to use.

4. Further Consideration

Besides the presented prevention methods, some considerations are worth noticing during the designing of devices and protecting the health of the users. These considerations are trading off between health and personal information protection, technologies employed, the duration of devices' performance and the time needed to response during the interaction of implantable devices and external system.

Health and personal information protection: together with the development of ICT, owning a device which allows Internet access is no longer a problem. This gives raise to the proliferation of information solutions with a common purpose is to protect personal privacy and information security. Integrating basis authentication to secure both patients' information and the data stored in the system is a must. However, set in the case of emergency, medical staff need to access immediately to both patients' information and system to get general status about patients' health, type of devices implanted and more to implement correct urgent solutions for saving patients. In this situation, security authentication is generally become a hurdle preventing urgent medical actions, which may have the result badly on the health of patients. The higher the level of security is, the more delay in deploying urgent treatments witnesses. This can be assumed as an urgent matter which requires high attention in the

relationship between applying high technology in treating diseases and the priority in protecting people's health.

The duration in the performance of implantable devices: integrating more technologies, tasks and functions on the implantable devices can obviously decrease the capacity of the battery (Panescu, 2008). As mentioned, the fast depletion of battery could increase the frequency of surgeries to replace the devices. This generally impacts the patients' health, particularly when the level of fast recovery of people are different by their ages and certain physical conditions. This requires to extend the lifetime of battery: 1) By designing devices with enhance the capacity of the battery or 2) Reprogram the authentication mechanism to be less complicated in terms of storage and processing, while securing the information security. Obviously, this is a very difficult mission and depends significantly on the development of science and technology, which often requires long time of research and development.

Response between implantable devices and external system: this issue has a similar nature to trading off between health and privacy protection. However, in a normal circumstance, many authenticating requirements integrated mean time to be fulfilled and authenticated is thus consuming. Sometimes, this cause inconveniences for patients particularly when they go abroad for treatment. Hence, the steps of ensuring information security should be studied and demonstrated to make sure that authentication process costs a reasonable amount of time in treating diseases.

Viable solutions for these concerns are to establish two authenticating mode: normal and emergency, which are designed on the implantable devices and external system. In the normal mode, patients can control who can interact with medical implantable device implanted on their body. In this case, it is needed to have 2 classes of security: authentication over accessing and encrypting data while communicating to remove bad attempts access. The implantable devices will automatically remove the requirements or commands which are unidentified. Ideally, medical implantable devices should be designed to be invisible from all, except the authorized party, during the communication of signals. On the other hand of emergency, medical staff should have privilege in accessing to the device easily, classifying the devices, extracting necessary information and even changing the performance of devices if needed. These 2 modes are sound to serve the patients' benefits but the problem of the current time is the unavailability to satisfy these requirements in the real life. In this situation, we have to have certain tradeoff between: protecting health and securing personal privacy. This is the key concern of the meantime and in order to find a comprehensive answer, it does require more researches to identify a balance point where technologies are solely employed to serve people's health.

5. Conclusion

The role of medical implantable devices in treating and promoting the quality of human life is significant. The latest devices are gradually integrated more functions and technologies, which enable them to be smarter and complement mainly to the medical observation and treatment. All are thanks to the development of medical and information technologies. On another perspective, risks are remaining on the security of the personal data, which can have certain impacts on the performance of implantable devices. The decision of weighting more on the data security or shortening the times of treatment is not comprehensive but rather, it depends on certain circumstances. The trend of more technologies are introduced and medical data is stored and analyzed on the computer system to better protect patients' health is indispensable during the significance of 4.0 revolution. Therefore, the current solutions should focus on enhancing basis standards in data security applied in implantable devices. These

standards should be legalized, checked and complied strictly to medical conditions. Although this remains a new topic both in the international level and in Vietnam, it does require an adequate attention in conducting further researches to fulfill and improve the current shortcoming of the legal system in governing the respective matter.

References

Defend B., Salajegheh M., Fu K., and Inoue S. (2008). "Protecting global medical telemetry infrastructure technical report", Institute of Information Infrastructure Protection (I3P).

Li C., Raghunathan A. and Jha N.K. (2011). "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system", trong *13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*.

Halperin D., Heydt-Benjamin T. S., Ransford B., Clark S. S., Defend B., Morgan W., Fu K., Kohno T., and Maisel W.H. (2008). "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses", trong *Proc. of the 29th Annual IEEE Symposium on Security and Privacy* pp. 129–142.

Panescu D. (2008). "Emerging technologies [wireless communication systems for implantable medical devices", *IEEE Eng. Med. Biol. Mag*., Vol. 27, No. 2, pp. 96–101.

Vietnamese Government (2016). Degree 36/2016/NĐ-CP of Vietnam regulating the governance of medical equipment, Vietnamese Government Degree.

Hansen J. A. and Hansen N. M. (2010). "A taxonomy of vulnerabilities in implantable medical devices", *in: Proc. of the Second Annual Workshop on Security and Privacy in Medical and Home-care Systems* SPIMACS'10, ACM, New York, USA, pp. 13-20.

Kim Tuyến (2019). "Lỗ hổng kiểm định chất lượng thiết bị cấy ghép y khoa", *Pháp Luật Journal*, received 10/07/2020, available online at: https://baophapluat.vn/song-khoe/lo-hong-kiem-dinh-chat-luong-thiet-bi-cay-ghep-y-khoa-450436.html.

Callejon M. A., Naranjo-Hernandez D., Reina-Tosina J. and Roa L. M. (2013). "A comprehensive study into intrabody communication measurements", *IEEE Trans. Instrum. Meas*., Vol. 62, No. 9, pp. 2446-2455.

Callejon M. A., Roa L. M., Reina-Tosina J. and Naranjo-Hernandez D. (2012). "Study of attenuation and dispersion through the skin in intrabody communications systems", *IEEE Trans. Inform. Technol. Biomed*., Vol. 16, No. 1, pp. 159-165.

Medtronic (2020). "Implantable pacemaker and defibrillator information", accessed on 10/7/2020, available online at: http://www.medtronic.com/rhythms/downloads/3215ENp7_magnets_online.pdf.

Leavitt N. (2005). "Mobile phones: the next frontier for hackers?", *Computer*, Vol. 38, No. 4, pp 20-23.

Vietnamese Government (2001). National standard No. TCVN 6796:2001 (ISO 8828:1998) regulating the implantable materials in surgery, Vietnamese Government Standard Report.

Karger P. A., Kc G. S. and Toll D. (2009). "Privacy is essential for secure mobile devices", *IBM J. Res. Dev.*, Vol. 53, No. 2, pp. 1-17.

U.S. Food and Drug Administration (FDA) (2013). "Medical device safety", accessed on 10/07/2020, available online at: http://wireless.fcc.gov/services/index.htm?job=service_bandplan&id=medical_implant.