Medical Internet of Things and Legal Issues Regarding Cybersecurity

Chien-Cheng Chou[1,2(✉)]

[1] Center for General Education, Taipei University of Marine Technology, No. 150, Sec. 3, BinHai Rd., Danshui Town, New Taipei 25172, Taiwan
garyl2081l@gmail.com
[2] Chinese Society of Health Law and Policy, New Taipei, Taiwan

Abstract. The Internet of Things (IOT) raises legal and regulatory challenges, mainly in the area of privacy and security. To the Medical application, IOT controlling/liability are more important to the Cybersecurity. This article will refer certain legal issues regarding privacy and security matters to MIOT, and provide certain updated standards, regulations and protective measures.

Keywords: Telemedicine · MIOT · IOT · Cybersecurity · Privacy

1 Introduction

IOT poses extreme legal and regulatory challenges to the sensitive personal information matters, according to the general legal norms, the sensitive personal information includes medical, psychological, sexual, social, financial, and legal data. The aforementioned information also concerns to a universal substance of human rights, i.e. privacy and its security. Nevertheless, although law and technology have long been proposed whether a solution to either ethical, commercial, or political equation is possible, the practice of IOT concerned to Big Data and the Cloud technics, the combination of these three applications is still under-explored in the legal field.

Accordingly, IOT is a combination network of physical devices and many items, mainly refers a network connectivity that enables data collections and exchanges among electronics, software and sensors. MIOT is aforementioned applications to medical matters, which converges medication, medicine and certain physical devices; such applications will transform healthcare into not only less costs and inefficiencies method but also more live savings. Such objects are in accordance with the current healthcare policy majorly concentrated on cost control, increased access and eventual universality, and the quality standards maintenance and enhancement. In other words, healthcare policy tries to reach a triangle of access versus cost versus quality, which leads certain achievements: (1) the care experience improvements, (2) the health populations improvements, and (3) the cost reductions [3]. These achievements are affordable via a pre-patient treatment term, which tends to keep the wellness of people before they become ailing. The strategies are provisions of ones' own care engagement, coordinated care designation, and real-time diagnosing, that keeps people healthy and out of the hospital [1].

Y.-B. Lin et al. (Eds.): IoTaaS 2017, LNICST 246, pp. 50–53, 2018.
https://doi.org/10.1007/978-3-030-00410-1_7

2 The Challenges Fall into Two Main Categories: Fiscal/Policy and Technology

Since IOT applications refer a network connectivity that enables data collections and exchanges among electronics, software and sensors, MIOT is an adoption of Electronic Health Records (EHRs) in the IOT applications. The adoption seems simple, but had reformed a tradition ink-and-paper medical records managing system. In recent decades, certain the medical records managing system might be digitized because of the events of computer technology, but the managements were mainly kept in a closed system. Data exchanges were established merely upon medical institutions for the purposes of diagnosis and therapy to individual patient [6].

MIOT new data exchange mechanism for EHRs will enable researchers and healthcare providers to share information and reach a macro observation from the EHRs cloud or big data. Since MIOT provided a revolutionary treatment method, certain fiscal, policy and technology issues emerged. In particular, privacy and security will be a major concern in both policy and technology matters.

A huge technical barrier is the state of EHRs data. Although the collection of information is named cloud or data, the collection is actually composed by numbers of silos. Every exchanging individual records between silos and collecting data from different sources also refer to probability of data leakage. However, personal information of medical records and medical treatment is highly sensitive, and is covered by many regulations regarding collecting and usage. To the matters of MIOT, FDA provided a draft guidance, which introduced a variety of privacy-related measures to IOT and wearable technology.

3 Legal Issues to MIOT

In 2015, the US FDA (Food and Drug Administration) issued and updated the guidance document to inform associated manufacturers, distributors, and other entities about the possible MIOT applications to the regulatory authorities [4]. In other words, the document provided an expansion applicability of mobile apps that would be concluded into FDA's jurisdiction.

The U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to enforce HIPAA requirement. The Privacy Rule addresses the use and disclosure of the health information for individuals by covered entities subject to the Rule. It also creates a standard for individual privacy rights to control and understand how their health information is used. To the matters of privacy and security, certain MIOT devices are addressed to comply the HIPAA (Health Insurance Portability and Accountability Act) requirements.

> ***"Connectors:*** applications that connect smartphones and tablets to FDA- regulated devices, thus amplifying the devices' functionalities."
> ***"Replicators:*** applications that turn a smartphone or tablet itself into a medical device by replicating the functionality of an FDA-regulated device."

> ***"Automators and customizers:*** apps that use questionnaires, algorithms, formulas, medical calculators, or other software parameters to aid clinical decisions."
> ***"Informers and educators:*** medical reference texts and educational apps that primarily aim to inform and educate."
> ***"Administrators:*** apps that automate office functions, like identifying appropriate insurance billing codes or scheduling patient appointments."
> ***"Loggers and trackers:*** apps that allow users to log, record, and make decisions about their general health and wellness [7]."

The HIPAA compliance included four main requirements.

> ***Administrative Safeguards***: …to ensure the proper employee management, training and oversight for staff that come into contact or manage protected health information.
> ***Technical Safeguards***: …technical measures manage providers, including encryption and decryption systems, audit controls, emergency access procedures.
> ***Physical Safeguards***: …physical measures around the security of the data, including data redundancy and failure requirements.

The HIPAA is a series of privacy regulations that requires health care providers and organizations to develop and follow procedures that ensure the confidentiality and security of protected health information (PHI). The HIPPA regulations also applies to the associated business entities. Therefore, the way PHI transferring, receiving, handling, or sharing are covered. The forms of PHI include paper, oral, and electronic, etc.

Therefore, under the requirement of both MITO guidance and HIPPA, manufacturers of mobile medical apps are subject to a network of privacy standards and are required to follow associated controls established by the regulations.

4 Conclusions

MIOT applications are seen as new realms, and are expected with remarkable benefits to the markets. On the other hand, privacy and security-related challenges are also considerable to the MIOT practices. Profound benefits will be brought by new technologies, but the preemptive policy interventions will also limit new innovation opportunities. To the lawmakers point of view: "It's always better to legislate in anticipation of problems being created, but sometimes it actually takes the event to have occurred, which triggers the political outrage that then makes it possible to legislate.[1]"

To the challenges raised by MIOT developments, the authorities should not turn a blind eye, because these technologies involve to consumers' lives and more careful consideration and constructive solutions to the social warfare. The major task will be a balance striking between approach to privacy and security concerns and economic and social innovation.

---

[1] By Sen. Ed Markey in the US Congress, Darren Samuelsohn, What Washington really knows about the Internet of Things (06/29/2015) http://www.politico.com/agenda/story/2015/06/internet-of-things-caucus-legislation-regulation-000086.

References

1. Affordable Care Act Patient Protection and Affordable Care Act § 2712(a), Pub. L. No. 111–148, 124 Stat. 119 (2010)
2. Bauer, H., Patel, M., Veira, J.: The Internet of Things: Sizing Up the Opportunity [Internet] McKinsey & Company, New York; c2016 [cited at 2016 Jul 1]. http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity
3. Berwick, D.M., Nolan, T.W., Whittington, J.: The Triple Aim: Care, Health, and Cost, 27 HEALTH AFF. 759, 759 (2008). http://content.healthaffairs.org/content/27/3/759.full.pdf
4. FDA, Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff. https://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm255978.htm
5. Flores, M., Glusman, G., Brogaard, K., Price, N.D., Hood, L.: P4 medicine: how systems medicine will transform the healthcare sector and society. Per Med. **10**(6), 565–576 (2013). [PMC free article] [PubMed]
6. Kruse, C.S., Kothman, K., Anerobi, K., Abanaka, L.: Adoption factors of the electronic health record: a systematic review. JMIR Med. Inform. **4**(2), e19 (2016). [PMC free article] [PubMed]
7. Cortez, N.: The Mobile Health Revolution? 47 U.C. Davis L. Rev. 1181, April 2014
8. Scheen, A.J.: Precision medicine: the future in diabetes care? Diabetes Res. Clin. Pract. **117**, 12–21 (2016). [PubMed]
9. van Leeuwen, N., Swen, J.J., Guchelaar, H.J., 't Hart, L.M.: The role of pharmacogenetics in drug disposition and response of oral glucose-lowering drugs. Clin. Pharmacokinet. **52**(10), 833–854 (2013). [PubMed]
10. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of things for smart cities. IEEE Internet Things J. **1**(1), 22–32 (2014)