

Cybersecurity: Legal Case Studies in Medicine

Rujittika Mungmunpantipantip^{1, *}, Viroj Wiwanitkit²

¹Research Scholar, 26 Medical Center, Bangkok, Thailand

²Adjunct Professor, Joseph Ayobabalola University, Ilara-Mokin, Nigeria

²Honorary Professor, Dr DY Patil University, Pune, Maharashtra, India

Abstract

At present, internet is the widely used communication technology. The cyberspace is the world without boundary. Due to the increased volume of use, it is no doubt that there might be a new emerging problem. The cybersecurity becomes a new concern in law, IT technology and computer engineering. The control of the cybersecurity is needed. The legal control is an important mean to manage the cybersecurity that is worldwide used. The specific security laws are implemented in several countries. The legal case regarding the cybersecurity is an interesting issue in law. In fact, the legal problem on the cybersecurity is observable in any activities. In medicine, the problem of cybersecurity is also observable and there are already some existed legal cases. Here, the authors specifically discuss on the legal case studies in medicine.

Keywords: internet, security, law, medicine

***Author for Correspondence** E-mail: rujittika@gmail.com

INTRODUCTION

Communication by computer network is the advanced widely used technology. It is accepted as the fast and convenient way for communicating among people around the world. The Internet becomes an important basic tool used around the world. The cyberspace becomes the largest social group. Several activities are based on the information technology (IT). The advantage of the IT is acceptable. Increase volume of IT use is seen daily. With increased user, the problem due to some bad users can be expected.

The security problem of IT is not uncommon and the problem is observable around the world. The cybersecurity is a very important consideration at present. , it is no doubt that there might be a new emerging problem. The cybersecurity becomes a new concern in law, IT technology and computer engineering. The control of the cybersecurity is required. The legal control by laws is generally practiced. The specific security laws exists several countries. The legal case regarding the cybersecurity is an interesting issue for studying. In fact, the legal problem on the cybersecurity is detectable in any activities. In medicine, the IT becomes an important tool. The problem of cybersecurity is also

observable in medical society and there are already some existed legal cases. Here, the authors specifically discuss on the legal case studies in medicine.

LEGAL CONCERN ON CYBERSECURITY IN MEDICINE

The IT is widely used in medicine at present. It can serve several activities and proven for the advantages. Similar to any other field, the IT security becomes an important consideration in medicine. Lundgren and Möller noted that “Apart from providing the basic criteria for a definition-correct demarcation and meaning concerning the state of security-it also aims at being a definition suitable for any information security perspective [1]” and also proposed that “Besides being too broad as well as too narrow, it cannot properly handle the soft issues of information security, nor recognize the contextual and normative nature of security [1].” A great consideration on the IT security is usually on the medical record. Kruse et al. mentioned that “The sensitive nature of the information contained within electronic health records has prompted the need for advanced security techniques that are able to put these worries at ease [2]” and also proposed that “It is imperative for security

techniques to cover the vast threats that are present across the three pillars of healthcare [2].” The health care center usually invests a lot on the IT security protection [3]. Claunch and McMillan noted that continuous improvement of action plan for IT security in medical center was necessary.

An important control of the cybersecurity is the use of legal control. Regarding the legal control, there are some interesting reports as shown in Table 1.

Legal case studies on cybersecurity in medicine

There are some interesting legal case studies on cybersecurity in medicine. Cyberattack is the important common problem [12]. The attack to data in NHS database is the good lesson learnt. After the attack, the security of the patient’s data becomes a widely discussed issue [13–14]. The cyber threat to internet health information is an emerging problem and it is considered an important crime. As noted by Luna et al., “*Current healthcare cybersecurity systems do not rival the capabilities of cyber criminals* [15].” Based on a recent report from USA, Nuzback concluded that “*since it began offering cyber liability coverage in December 2011, the Texas Medical Liability Trust has received more than 150 cyber liability claims, most of which involved breaches of electronic protected health information* [16].” There are many interesting legal cases of hackers on hospitals. The scenario of hackers rings up big phone bills for hospital is a good example [17]. In addition to hacker, the disguised information uploaded by a bad person is also reported in medicine. The case of a third-party plagiarism performed by a bad researcher is a good example. In that scenario, a bad doctor uses the internet to perform a plagiarism on the other’s doctor name. That indexed case was investigated and managed by specific cybersecurity laws [18].

Legal case in medicine can be successfully managed only if there is a good cyber space laws in that specific setting. It is no doubt that medical centers have to strict follow the legal control for cybersecurity [19].

Table 1: Some Interesting Reports on Cybersecurity Laws in Medicine.

Authors	Details
Menon et al. [5]	Menon et al. noted that “ <i>Legal frameworks, at both the international and national levels, can empower governments to strengthen public health and preparedness systems to better detect and respond to infectious disease threats and public health emergencies</i> [5].” Menon et al. also mentioned for the requirement of specific cybersecurity laws [5].
O’Sullivan et al. [6]	O’Sullivan et al. discussed on the use of robotics and artificial intelligence in medicine. O’Sullivan et al. also mentioned for the important of specific laws aiming at cybersecurity purpose [6].
Mackey and Nayyar [7]	Mackey and Nayyar discussed on the importance of digital danger [7]. The cybersecurity threats posed by illicit online pharmacies are specifically discussed by Mackey and Nayyar [7]. Mackey and Nayyar concluded that “ <i>There is a critical need to build international consensus, conduct additional research and develop technology to combat illicit online pharmacies</i> [7].”
Kramer and Luxton [8]	Kramer and Luxton focused on the existing laws and regulations and summarized the risk management issues relevant to providing telemental healthcare to children and adolescents [8]. Kramer and Luxton concluded that “ <i>Although legal and regulatory challenges remain in providing telemental healthcare to children and adolescents, it is possible to overcome these challenges with knowledge of the issues and appropriate risk management strategies</i> [8].”
Langer [9]	Langer discussed on cyber-security issues in healthcare IT [9]. Langer noted that “ <i>legislation directed care providers to enable the portability of patient medical records across authorized medical centers, while simultaneously protecting patient confidentiality among unauthorized agents</i> [9].” Langer specifically focused on the complexity of computer criminal applications, defensive countermeasures, and the pervasiveness of Internet connected devices [9].
Dunn Cavely [10]	Dunn Cavely mentioned for a cyber-security policy that is decidedly anti-vulnerability and at the same time based on strong considerations for privacy and data protection [10].
Martínez-Pérez et al. [11]	Martínez-Pérez et al. discussed on privacy and security in mobile health apps [11]. Martínez-Pérez et al. discussed on security and privacy in mHealth with specific focus on the existing laws regulating these aspects [11].

CONFLICT OF INTEREST

None

REFERENCES

1. Lundgren B, Möller N. Defining Information Security. *Sci Eng Ethics*. 2017 Nov 15. doi: 10.1007/s11948-017-9992-1.
2. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security Techniques for the Electronic Health Records. *J Med Syst*. 2017 Aug; 41(8): 127.
3. McMillan M. The cost of IT security. *Healthc Financ Manage*. 2015 Apr; 69(4):44–7.
4. Claunch D, McMillan M. Determining the right level for your IT security investment. *Healthc Financ Manage*. 2013 May; 67(5): 100–3.
5. Menon AN, Rosenfeld E, Brush CA. Law and the JEE: Lessons for IHR Implementation. *Health Secur*. 2018 Fall; 16(S1):S11-S17.
6. O'Sullivan S, Nevejans N, Allen C, Blyth A, Leonard S, Pagallo U, Holzinger K, Holzinger A, Sajid MI, Ashrafian H. Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. *Int J Med Robot*. 2019 Feb; 15(1):e1968.
7. Mackey TK, Nayyar G. Digital danger: a review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies. *Br Med Bull*. 2016 Jun; 118(1): 110–26.
8. Kramer GM, Luxton DD. Telemental Health for Children and Adolescents: An Overview of Legal, Regulatory, and Risk Management Issues. *J Child Adolesc Psychopharmacol*. 2016 Apr; 26(3):198–203. 30–43
9. Cyber-Security Issues in Healthcare Information Technology. *J Digit Imaging*. 2017 Feb; 30(1): 117–125.
10. Dunn Cavelty M. Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Sci Eng Ethics*. 2014 Sep; 20(3): 701–15.
11. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M. Privacy and security in mobile health apps: a review and recommendations. *J Med Syst*. 2015 Jan; 39(1):181.
12. O'Dowd A. Major global cyber-attack hits NHS and delays treatment. *BMJ*. 2017 May 15; 357:j2357.
13. O'Dowd A. NHS patient data security is to be tightened after cyberattack. *BMJ*. 2017 Jul 14;358: j3412.
14. Haugh R. Cyber terror. *Hosp Health Netw*. 2003 Jun; 77(6): 60–4.
15. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: A systematic review. *Technol Health Care*. 2016;24(1): 1–9.
16. Nuzback K. Cyber crimes. *Tex Med*. 2014 Jul 1; 110(7): 27–33.
17. Gardner E. Hackers ring up big phone bills for hospitals. *Mod Healthc*. 1992 Nov 2;22(44): 43.
18. Miri SM, Rezamand S, Goodarzi Z. The experience of detecting a case of plagiarism in Hepatitis Monthly. *Hep Mon*. 2008; 8(2): 225 – 9
19. Barr P, Butcher L, Hoppszallern S. 2016 MOST WIRED. *Hosp Health Netw*. 2016 Jul; 90(7):

Cite this Article

Rujittika Mungmunpantipantip, Viroj Wiwanitkti. Cybersecurity: Legal Case Studies in Medicine. *National Journal of Cyber Security Law*. 2018; 1(2): 36-38p.