Harmonization Over the Regulations of Electronic Medical Records and its Potential to be Abused

Maskun[1], Rian Nugraha[1], Hasbi Assidiq[1,2], Muhammad Tayyib[1], Armelia Syafira[1]

[1]Faculty of Law, Hasanuddin University,
[2]Faculty of Law, Hasanuddin University, Makassar, South Sulawesi, Indonesia

Abstract

The rapid development of information and communication technology has brought changes to the mechanism for storing electronic medical records (EMR). EMR is very important to protect and provide comfort and convenience for health services. However, it is very susceptible to be abused by hackers. This study aims to harmonize amongst relevant laws on EMR and to identify the legal protection of EMR from abuse by hackers. This research uses a normative research method to harmonize legal norms and regulations related to EMR that already exist in Indonesia. Legal protection of EMR in Indonesia has not been implemented proportionally even though the regulation on EMR has been stipulated clearly in the Minister of Health Regulation No. 269/ 2008 concerning Medical Records and various relevant Laws on it. There are no derivative laws related to EMR as mandated by the Minister of Health Regulation No. 269/2008 which becomes an obstacle to the effective implementation of EMR. The existence of an EMR is Also very susceptible to be abused by hackers. So, cyber security is needed for health workers, both individually and institutionally to protect EMR. In conclusion, EMR has been regulated in Indonesian Laws, but it has not been governed into derivative laws to be implemented a proportionally. Therefore, harmonization those laws will narrow the gaps amongst them. Further norms and regulations regarding EMR are needed to create cybersecurity which is potential to be hacked.

Keywords: *Legal Protection; Electronic Medical Records; Hackers.*

Introduction

The development of information technology today gives a colour to the world of health. The use of electronic medical records (EMR) is one form of these developments. EMR is a form of innovation in responding to the challenges of the times in the health sector. Medical records in the past are identical to paper administrative documents containing the patient's identity, history and actions given by a doctor to a patient. With EMR, health workers can obtain patient medical history data more easily, regardless of distance and time, the application of EMR has even been adopted in hospitals in various countries since 1999[1].

In 2003, RAND Health Information Technology (HIT) began conducting research related to the role and importance of EMR in improving health services and informing the government to maximize the benefits of EMR and increase its use. The results of this study indicate the benefit of implementation of EMR and its network can save more than 81 million dollars per year, which can increase productivity and efficiency in health care[2].However, it remains to be aware that the use of systems based on electronics and the internet is very vulnerable to be abused and hacked by irresponsible parties.

EMR consists of notes and documents including the patient's identity, examination results, medications that have been given, and other actions and services that have been provided to patients[3].The presence of multiple personal identities stored in the EMR is very susceptible to the misuse of data by parties who are not responsible. This can be taken place because the EMR repository can be accessed by the third parties – called hacker – and the tool to access it is computer and internet as a media. Therefore, some actions shall be done to protect on patient data, including regulation approach.

In general, regulations related to EMR has been governed in the Minister of Health Regulation

Number 269 of 2008 concerning on Medical Records (PermenkesMedical Records). In this regulation, it is explained that EMR documents, which is the data are qualified as personal data of a person need to be maintained and kept confidential to avoid data misuses. The content of a patient's medical record, basically, contains juridical consequences in the form of the patient's personal identity. It must, then, be kept confidential[3]. All information in medical records is confidential, therefore, its use must be with the patient's consent, except[3]for the purposes of education and research which are implemented for the benefit of the state

EMR is the use of information technology tools for collecting, storing, processing and accessing data stored in patient medical records in hospitals in a database management system that collects various sources of medical data[4].Some modern hospitals have even combined EMR with the Hospital Management Information System (SIMRS) application which is the main application that not only contains EMR but also has added features such as administration, billing, nursing documentation, reporting and a score card dashboard.

If you look more deeply, the use of technology, namely computers and the internet, allows cybercrime to occur against patient EMR. Therefore, it is considered important to protect the EMR of patients, where this protection aims to safeguard personal data and broadly protect national health system data from abuse and cybercrime by those who want to hack. In general, the implementation of EMR has been categorized as an electronic document as stipulated in the Law Number 11 of 2008 as amended by the Law Number 19 of 2016 concerning Information and Electronic Transaction. It means that EMR as a norm and law has been accommodated in this Law, although it has not been specifically explained regarding EMR[5].

Misuse of EMR is a legal issue to be discussed by among legal practitioners in this modern era, including in Indonesia. Some debates coming from many parties that EMR does not have a clear legal standing, especially with regard to guaranteeing against elements of privacy, confidentiality and information security in general[4].The result of this controversy raises a distrust of the EMR system. As it is known that a person's data, especially medical history data, is very private and will be a danger if it is accessed by irresponsible parties. Of course, this will be very detrimental to the victim, particular in this case of the patient's data has leaked to the party who should be prohibited from accessing the information.

Therefore, the focus of this paper is to analyse various regulations related to the implementation of EMR. Starting from general regulations such as the Law Number 29 of 2004 concerning Medical Practice (Law on Medical Practice) and the Law Number 11 of 2008 as amended by the Law Number 19 of 2016 concerning Information and Electronic Transaction, to specific regulation as if the Permenkes Medical Records. Those laws then shall be harmonized in order to carry out the important reasons why EMR is pivotal in medical practice and why it shall be protected. Indeed, the last point to be underlined in this paper is the identification of various cyber-rime vulnerabilities that will occur from misuse in the EMR.

Materials and Method

This study is a normative study to analyze various EMR regulation, which is well adapted to the analysis of relevant norms and principles. Those regulation are reference sources coming from legal materials called laws and the principles of law, and a scientific journal. All those legal materials will be analyzed qualitatively to deal with the EMR legal issues. The various materials obtained are then analyzed qualitatively to lay down EMR in the right position as an advanced development of medical records, before technology gets involved in the area of medical records.

Result and Discussion

Harmonization of Medical Records Law:

Obligation to Make Medical Records: Medical records refer to the Law Number 29 of 2004 concerning Medical Practice. Article 46 paragraph (1) of the Law Number 29 of 2004 states that an obligation for doctors and dentists to have medical records of the patients in carrying out their medical practice. In the explanatory of the Article 46 paragraph (1) further explains the definition of "medical record" as a file containing notes and documents about the patient's identity, examination, treatment, actions and other services that have been provided to patients. Medical records should be equipped with the affix name, time, and signature of the person who provides services or actions.

Furthermore, Article 47 of the Law Number 29 of 2004 explains that[6]: Medical record documents as

referred to in Article 46 belong to a doctor, dentist, or health service facility, while the contents of the medical record are the property of the patient. Due to the contents of the medical record is belong to the patient, it is the duty of the doctor or dentist and the head of health service facilities to keep and maintain its confidentiality.

As it is known, medical records have a very important role and become an indicator of good and responsible medical practice, which shows the good performance and discipline of health workers. The medical record contains various data in the form of patient identity and all actions taken (from the beginning) to patients in the context of providing health services. The recording must be listed chronologically, systematically and accurately, so that it can provide a description of a person's disease information, investigative actions carried out on him/her, information on management plans, observational records, clinical and treatment results, approval or rejection, and summary of discharge[7].

Regarding to EMR, it is specifically regulated in the Minister of Health Regulation (Permenkes) Number 269 of 2008 concerning Medical Records (Permenkes Medical Records). Even though in the explanatory of article 46 paragraph 3 of the Medical Practice Law has provided space for the implementation of EMR, the clear position of EMR basically is stipulated in the Permenkes on Medical Records. This Permenkes states that if the medical records created in electronic form, the signature of the doctor or dentist or other health professionals can be replaced by using a personal identification number. This is very important because Article 2 of the Permenkes provides a legality basis for the implementation of medical records which must be written, complete and clear or electronically[3].It means that the contents of the medical record should be in written form and is belong to the patient which consisting of notes and documents regarding the patient's identity, examination, treatment, actions and other services that have been provided to the patient[3].According to the Permenkes, the contents of medical records can be categorized as categories for out-patients, in-patients, emergency services, disaster situations and for the services of a specialist doctor or specialist dentist. The medical records have minimally contents such as personal identity, complaints of illness, and health measures are necessary[3].

Nowadays, the implementation of EMR has been able to be synergised to a hospital information system (SIRS) electronically. The SIRS may be contained various applications such as: (a) Application of Mobile and Web; (b) Server Applications; (c) Receptionist Application; (d) Telemedicine applications; (e) Update Medical Registration; (f) Application in the Medical Registration Room; (g) Application of Hospital Information Systems; (h) Application for Recording Doctor's Salary; (i) Result of Pathology Laboratory Test; and (j) Application of Radiology Test Results. With data storage based on Cloud Computing, this can make it easier for hospitals to store large data[8].

According to WimmieHandiwidjojo, the use of EMR has enabled information technology equipment for the collection, storage, processing, and accessing data stored in the EMR of patients in hospitals within a database management system that collects various sources of medical data, since 2009. Even some modern hospitals have combined EMR with the Hospital Management Information System (SIMRS) application which is the main application that not only contains EMR but has added features such as administration, *billing*, nursing documentation, reporting and a score card dashboard[9].

EMR as an Electronic Document: The existence of EMR is a development of technological advances in the health sector which is also part of the mandate of the Indonesian Medical Code of Ethics. Article 21 of the Code of Ethics explains that it requires doctors to keep developments in medical or health science and technology. According to IkaMeilia, every doctor should be willing and able to document patient management carried out in the EMR in accordance with applicable regulations[1]. As an implication of the development of electronic technology, the provisions in EMR are closely related to electronic documents stipulated in the Law Number 11 of 2008 as amended by the Law Number 19 of 2016 concerning Information and Electronic Transaction.

Article a point 4 of the Law Number 11 of 2008 as amended by the Law Number 19 of 2016 concerning Information and Electronic Transaction (the Information and Electronic Transaction Law) stipulates that electronic documents are defined as "any electronic information that is created, forwarded, sent, received, or stored in analogue, digital, electromagnetic, optical, or the like, which can be seen, displayed, and / or heard through a computer or electronic system, including but not limited to writing, sound, images, maps, designs, photographs or the like, letters, signs, numbers, access codes, symbols or perforations that have meaning or meaning or can be

understood by those who are able to understand them." Referring to the document electronic as stipulated in the Article 1 of the law Number 11 of 2008, EMR can be categorized as an electronic document. The legal implication of this is that the regulations related to EMR have an intersection stipulated in the Information and Electronic Transaction Law. So that all legal actions related to the abuse of this EMR can be subjected to sanctions of the Information and Electronic Transaction Law.

The crucial point from the harmonisation of the EMR as stipulated above, it cannot be denied, then, the protection of medical records is very necessary to neglect EMR misuse from unauthorized parties and for the sake of legal evidence[10]. However unfortunately, after 12 years since this legal basis was established, there are no derivative regulations of the Permenkes to become the legal basis for the enforcement of EMR in Indonesia as stated in Article 2 paragraph (2) the Permenkes on Medical Records. Even though this is very important to strengthen the legality of EMR implementation[7].

Abuse Vulnerability of EMR: EMR collect various medical history data, patient care or medication and it is very personal to the patient. The existence of various personal identities stored in EMR is very vulnerable to misuse of data by irresponsible parties. Medical record documents, both conventional and electronic, are confidential documents belonging to patients, so they must be protected as best as possible. In this case, the family or other parties who want to know this medical record need to get the consent of the patient or the patient's attorney. So that privacy of patient is very much guarded. (Rokhim 2020) EMR can be stored in an electronic device such as a computer or other electronic data storage device, including the Cloud.

EMR has at least two forms of security against the privacy of medical records, namely authentication and authorization. Authentication is a form of ensuring that the party authorized to enter and use the system. It can be in the form of a password, access card or more sophisticated with biometrics such as fingerprints. Meanwhile, in terms of authorization, only certain parties have the authority to access EMR. It means that not every officer in the health facility is allowed to use the existing EMR network system. Each user also has different access authority restrictions. This can increase EMR's privacy security[1].

In general, the misuse of EMR data can be categorized as cyber-crime. It is classified into two forms, namely; (a) crimes via computer media, Flash-disk- or various other hard storage devices; and (b) crime via hacking by the EMR Cloud based system. To guarantee the legal protection of patient data, therefore, it is very important to understand these two things to prevent and take legal measures that can be taken to protect EMR from misuse by the irresponsible party.

Some scholars use the terms "computer misuse", "computer abuse", "computer fraud", "computer-related crime", "computer-assisted crime", or "computer crime". However, scholars at that time generally accepted the use of the term "computer crime". It was because it was considered more extensive and commonly used in international relations. The British Law Commission defines "computer fraud" as computer manipulation in any way done in bad faith to obtain money, goods or other benefits or intended to cause harm to other parties (Suhariyanto 2012)[11].

In this case, those who can obtain EMR data are those who can legally access the data, such as health workers and patients themselves in accordance with applicable regulations. One such case was at Howard University Hospital, Washington in which data security is not properly guaranteed causes data leakage. In this case, a staff member at the hospital has access to patient data, name, address and patient medical record number and sells the information to insurers. Another case is a worker managed to steal a laptop and download 34,000 patient data on his personal laptop in a hospital. EMR data is not encrypted. It means that anyone can guess the data password and can access patient data. Based on this, according to Meilia, it becomes a challenge in the medical world to improve the safety of patient EMR data[1].In this context, the EMR abused can be categorized as Computer Crime because it uses a computer device as a tool to conduct crime. In this case a computer is a tool to commit a crime to gain certain advantages that harm other parties.

Storage system based EMR Cloud computing is one of development technology. In this context, to store EMR no longer requires a separate server because it has been supported by the virtual server. This cloud-based storage method can save infrastructure costs and can easily share data with various health care facilities. However, on the other hand, EMR data storage based on the Cloud is very vulnerable to the risk of hacking[11]. As

it is known, a hacker can hack a network system so that it is possible to access data from a network system that has been hacked. This applies to any network system that is open and accessible to anyone. If EMR data exists in an internet network such as those based on the cloud, then there is a great potential that these data can be hacked.

In the typology of cybercrime, hackers against cloud-based EMR systems can be categorized as occurring, namely: (a) offenses against the confidentiality, integrity and availability of computer data and systems, such as illegal access (hacking / cracking), illegal data acquisition (data espionage), Illegal interception, data interference, system interference[12]. To reduce this risk, it is necessary to have a cybersecurity system that is qualified and evaluated and tested regularly network security[10].

Regarding to abused EMR via hacking, in Article 30 paragraph (1), paragraph (2) and Paragraph (3) jo. Article 46 paragraph (1), paragraph (2) and paragraph (3) of Law No. 11 of 2008 concerning Electronic Information and Transactions as amended by Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions have regulated legal sanctions on hackers, or people who deliberately access other people's computers or certain electronic systems unlawfully, with various criminal sanctions and fines that can be prosecuted to hackers. Referring to those articles on the Information and Electronic Transaction Law, which is then linked to EMR, it is an electronic information and / or electronic document and anyone who misuses a patient's EMR data can be subject to the article. However, this is a step when the criminal act has occurred. Even though there should be preventive steps beIn EMR practice, debate on legal standing of EMR is still taking place. Some regulation such as the Medical Practice Law and/or the Permenkes on Medical Records do not derive to lower regulation to show EMR position to be more practical. Article 2 paragraph (2) Permenkes on Medical Records states that EMR as an alternative to recording medical records will be regulated in a separate regulation, but until today the regulation has not yet existed. Even though EMR system has been used by several hospitals in Indonesia such as Dr.Soetomo Hospital[13] Surabaya and RS Paru Jember[14]

The absence of a clear legal standing in EMR security system is indicative of a lack of trust in the security of patient data. On July 20, 2018, for example, hackers pretend to be patients visited the clinic database and clinic of SingHealth, the largest health operator in Singapore. The hackers then illegally accessed and downloaded data on 1 May 2015-4 July 2018. The medical information data of 1.5 million Singaporeans including data belonging to Prime Minister Lee Hsien Loong was hacked into[15].

Conclusion

Harmonization of law is required related to the protection of EMR data, which has a legal basis as stipulated in the Medical Practice Law, and specifically in the Permenkes on Medical Records. As an electronic document, EMR's position is also directly regulated in the Information and Electronic Transaction Law. In addition, special regulations are needed related to EMR itself which is the mandate of the Permenkes on Medical Records. The aim of derivative regulationto strengthen the legal standing of the EMR and to neglect abuse of EMR done by the irresponsible parties either via computer crime or via hacking.

Conflict of Interest: The Authors declare that there is no conflict of Interest.

Source of Funding: Nil

Ethical Clearance: Taken from Medical Record Committee as stipulated by the Ministry of Health Regulation No. 269/Menkes/Per/III/2008.

Reference

1. Meilia PDI, Christianto GM, Librianty N. Buah Simalakama Rekam Medis Elektronik: Manfaat Versus DilemaEtik (The Horns of a Dilemma of Electronic Medical Records: Benefit vs Ethical Dilemma). Jurnal Etika Kedokteran Indonesia 2019;3(2). p.61.
2. Hillestad R, et. Al. Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs. Health Affairs 2005;24(5)
3. Ministry of Health of the Republic of Indonesia Regulation No. 269/MENKES/PER/III/2008 concerning on Medical Records.
4. Sudjana. Aspek Hukum Rekam Medisatau Rekam Medis Elektroniksebagai Alat Bukti Dalam Transaksi Teurapetik (Legal Aspect of Medical Record or Electronic Medical Record as Evidence in Therapeutic Transaction). Veritas et Justicia 2017;3(2). p. 369

5. Wahjuni E, Sari NK. Legal Aspects of Electronic Medical Records. Jurnal Dinamika Hukum 2017;17(3). p. 9
6. Law No. 29 of 2004 Concerning on Medical Practice. Art. 47
7. Samandari NA, Chandrawila W, Rahim AH. Kekuatan Pembuktian Rekam Medis Konvensional dan Elektronik (The Evidence Power of Conventional and Electronic Medical Records) . SOEPRA Journal of Health Law 2016;2(2). p. 155
8. Kartika AR, Yusuf A, Rohman AD, Sudirja S. Sistem Rekam Medik Berbasis Cloud Computing dan IdentifikasiFrekuensi Radio (Cloud Computing Based Medical Record Ssystem and Radio Frequency Identification). National Seminar on Information and Multimedia Technology, STMIK AMIKOM Yogyakarta 2014;2(1) p.30
9. Handiwidjojo W. RekamMedisElektronik (Electronic Medical Records). EKSIS Journal 2009;2(1). p.38
10. Budiyanti RT, Arso SP, Herlambang PM. Rekam Medis Elektronik Berbasis Cloud dalamPerspektif Etika dan Hukum di Indonesia (Cloud-Based Electonic Medical Record in the Perspective of Ethics and Law in Indonesia). Cermin Dunia Kedokteran 2018;45(9). p.695
11. Suhariyanto B. Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan CelahHukumnya (Tecnology Information Crime Regulatory Urgencies and Legal Loopholes). Jakarta: PT RajagrafindoPersada; 2012, p.9
12. Gercke M. Understanding Cybercrime: Phenomena, Challenges, and Legal Response. ITU Telecommunication Development Sector; 2012. pp. 12–33
13. BUANA. Membangun Implementasi Rekam Medik Elektronik (RME) "Terintegrasi di RumahSakit (Developing "Integrated" Electronic Medical Record (EMR) in Hospital) http://www.bvk.co.id/artikel/berita/159-membangun-implementasi-rekam-medik-elektronik-rme-terintegr-di-rumah-sakit (accessed).
14. RS ParuJember. Studi Banding Rekam Medis Elektronik RSUD Prof. dr.Soekandar Mojokerto di RS Paru Jember (Comparative Study on Electronic Medical Records at Regional Public Hospital Prof. dr.Soekandar Mojokerto at Pulmonary Hospital Jember) http://rspjember.jatimprov.go.id/berita/studi-banding-rekam-medis-elektronik-rsud-prof-dr-soekandar-mojokerto-di-rs-paru-jember.html?page=3 (accessed)
15. Yon Yoseph. Data Medis 1,5 Juta Masyarakat Singapura DibobolPeretas (1.5 Million Medical Record of Singaporeans was breached by hacker) https://dunia.tempo.co/read/1109140/data-medis-15-juta-masyarakat-singapura-dibobol-peretas (accessed) Fore this happens.