Journal of Medical Record and Infomation Technologi (JOMRIT)
Vol. 1, No. 1, December 2023,

Security and Confidentiality of Medical Record Data in Hospitals in the Use of Electronic Medical Records : Literature Review

Chamy Rahmatiqa[1], Werman Werman[2], Masruqy Arrazy[3], Nurul Abdillah[4]
[1,4]Sekolah Tinggi Ilmu Kesehatan Syedza Saintika, Padang, Sumatera Barat, Indonesia
[2]Badan Penyelenggara Jaminan Sosial Kesehatan, Padang, Sumatera Barat, Indonesia
[3]Badan Pusat Statistik, Padang, Sumatera Barat, Indonesia

Article Info

Article history:
Received September 12, 2023
Revised September 28, 2023
Accepted December 3, 2023

Keywords:
Data Security
Data Confidentiality
Electronic Health Records
Hospital

ABSTRACT

Ministry of Health Regulation No. 24 of 2022 states that all hospitals must have electronic health records. Hospitals are not yet capable of implementing electronic health records perfectly, including data security and confidentiality of medical records. The aim of this research is to identify the factors causing the Security and Confidentiality of Medical Record Data in Hospitals in the Use of Electronic Health Records. The research method employed is a systematic review. The data sources for this study are literature obtained through the internet, consisting of published research results on the Security and Confidentiality of Medical Record Data in Hospitals in the Use of Electronic Health Records from all accessible journals. Data collection took place from October 10, 2023, to January 10, 2024. The document analysis results indicate that the factors causing the Security and Confidentiality of Medical Record Data in Hospitals in the Use of Electronic Health Records are human resources at 77.7%, the lack of clear and strict policies at 33.3%, inadequate facility support at 33.3%, and limited funds at 11.1%. It is expected that every hospital should have clear and strict policies to address the Security and Confidentiality of Medical Record Data in Hospitals in the Use of Electronic Health Records. With clear and strict policies regarding the readiness of human resources, facilities, and financial conditions, these issues can be addressed simultaneously.

Corresponding Author:
Chamy Rahmatiqa, SKM, MPH
Program Studi Manajemen Informasi Kesehatan, Sekolah Tinggi Ilmu Kesehatan Syedza Saintika
Jl. Prof. Dr. Hamka No. 228 Air Tawar Timur, Padang, Sumatera Barat, Indonesia
E-mail: chamyrahmatiqa@gmail.com

1. INTRODUCTION (10 PT)

In the midst of the rapid progress of information technology and communication, timely and accurate information is increasingly becoming a primary need for decision-makers [1]. In other words, information is a fundamental requirement for every management to make informed decisions. Hospitals, as institutions that store a vast amount of data, also require proper and accurate data processing that can be presented in the form of reports [2,3]. The presentation of reports in the form of information should be in line with the utility value and function of each department. For example, a financial director needs information in the form of statistical reports on the occupancy rate (the number of admitted patients divided by the available bed capacity) for each ward. Such a report would assist the director in decision-making regarding the need for additional beds. Information is crucial because it is processed correctly and effectively, resulting in valuable outcomes for both management and operational purposes [4,5].

Indonesia is in the era of Industry 4.0, which is a revolution in information technology and its application, now becoming a necessity for industries [6]. Hospitals, as part of the healthcare industry, are actively intensifying strategies to enhance service quality through the contribution of Hospital Information

Systems. One of the Hospital Information Systems contributing to the improvement of quality and efficiency in hospital services is the Electronic Medical Record (EMR) [7].

Electronic Medical Record (EMR) is a crucial technological tool for healthcare, modernizing medical information management, and contributing to high-quality patient care and efficient management. Specifically, EMR is defined as a digital repository of patient data, securely stored, accessible to authorized users, containing retrospective and prospective information [8]. Its primary purpose is to support integrated, sustainable, efficient, and high-quality healthcare. The implementation of EMR impacts patient satisfaction, documentation accuracy, accelerates patient data access, and reduces clinical errors in healthcare facilities, including community health centers (Puskesmas) and hospitals [9].

The development of Electronic Medical Records (EMR) globally, especially in developed countries, has been rapid. In the United States, it began around 2004. Denmark implemented EMR since the mid-1990s. In 2009, Denmark's Central Region (Anentire Hospital) decided to adopt comprehensive EMR. The adoption of EMR in Japan has also progressed rapidly, starting around the year 2000. Most developed countries use EMR to enhance the quality of healthcare [10,11]. In contrast, many developing countries lack healthcare information technology infrastructure to develop EMR, including Indonesia. The development of EMR in Indonesia is not specifically regulated. The enactment of the Information and Electronic Transactions Law (UU ITE) in 2008 and the Ministry of Health Regulation No. 24 of 2022 serve as the legal basis for the legitimacy of EMR as legal evidence and the development of EMR in Indonesia [12].

The development of Electronic Medical Record (EMR) implementation still faces several challenges, especially related to the capabilities of Human Resources (HR) in creating information technology, high investment, and management support. Various issues arise during the implementation of EMR [5,13]. Project failure in EMR implementation is identified due to insufficient integration into practices and organizations. The acceptance level of EMR by users is also recognized as a slow process. User acceptance of EMR requires high costs and learning efforts. Issues related to the slow acceptance of EMR include a lack of financial incentives, uncertain rewards, suboptimal technology, low priority, and resistance from EMR users.

2. METHOD (10 PT)

The research is a systematic review. The data sources for this study are literature obtained through the internet (Google Scholar), consisting of published research results on the Security and Confidentiality of Medical Record Data in Hospitals in the Use of Electronic Health Records from all journals that have been published and are accessible online. Data collection took place from October 10, 2023, to January 10, 2024.

Inclusion and Exclusion Criteria: The inclusion criteria for documents deemed suitable for a systematic review are research journals that discuss the causes of Security and Confidentiality of Medical Record Data in Hospitals in the use of Electronic Medical Records (Figure 1).

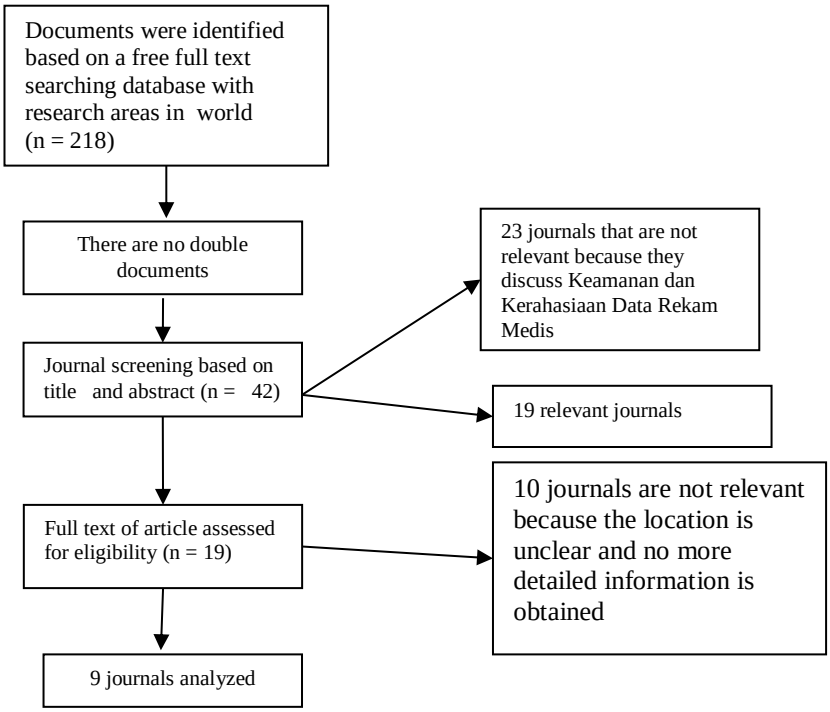

Figure 1. Literature Review Techniques

The research data on family medical records and health information from the years 2020 to 2024 totaled 824 studies, consisting of 379 research outcomes (theses and dissertations) and 445 published studies (journals and proceedings). This data was then narrowed down based on research published in journal form, resulting in 218 journals. This was done to maintain the relevance of the writing based on the most recent research findings. The research sample included 19 studies from various locations. The inclusion criteria encompassed studies examining the Security and Confidentiality of Medical Record Data.

The objective of this research is to explore the Security and Confidentiality of Medical Record Data in Hospitals through the use of Electronic Medical Records, providing insights to address issues related to the security and confidentiality of medical record data. Data collection involved determining the necessary variables through a literature review on the internet. The unit of analysis for this research is the journal.

3. RESULTS AND DISCUSSION (10 PT)

Summary of research related to the Security and Confidentiality of Medical Record Data in Hospitals through the use of Electronic Medical Records (Table 1). This table provides an overview that the researcher extracted from various journals worldwide. There are 9 journals summarized with their respective findings. It can be concluded that non-compliance with the Security and Confidentiality of Medical Record Data has been the subject of numerous studies.

Table 1. Summary of research related to the Security and Confidentiality of Medical Record Data in Hospitals through the use of Electronic Medical Records.

No.	Penulis	Location	Sampel	Metode	Hasil
1.	Cheng-Kun Wang[14]	Taiwan	13,960 citations of 410 articles in the period 2004-2013	high-quality database of SSCI (Social Science Citation Index) and SCI (Science Citation Index)	Currently, hospitals and clinics are adopting electronic medical records to store patient health data. Health data is stored on computers and transmitted via the internet. Some health information is stored in cloud databases. Electronic medical devices generate a substantial amount of health data transmitted to centralized databases. Threats to health records can be categorized into three main types: (1) human threats, such as from employees or hackers. Human-made disasters can be intentional (e.g., terrorist acts) or unintentional. (2) Natural and environmental disasters, such as floods, earthquakes, storms, and fires; and (3) technological failures, such as computer system damage.
2.	Annisa Maulida Ningtyas[15]	Yogyakarta	20 articles that match the keywords	Literature Review	Security techniques that can be implemented include utilizing cryptography methods, firewalls, access controls, and other security techniques. These methods have proven to be highly promising and successful in maintaining the privacy and security of Electronic Medical Records (EMR).

3.	Muh Amin, Winny Setyonugroho, Nur Hidayah[16]	Yogyakatya	Private Islamic Hospital in Yogyakarta	A qualitative research with a case study	The implementation of Electronic Medical Records (EMR): The implementation of EMR requires contributing factors for its success, such as human resources support, hardware, financial resources, leadership, training, and technical support. However, there are also obstacles encountered during the implementation of EMR, such as system errors, imperfect system design, lack of compatibility with other systems, insufficient computer skills, and power outages. In the implementation of EMR, attention must be paid to the confidentiality or security of the data within the EMR system.
4.	O. M. Enaizan, N. H. Alwi, N. J. Zaizi[17]	Malaysia	100 articles that match the keywords	Literature Review	Privacy and security factors play a crucial role in enhancing the acceptance level; therefore, these issues are addressed in this context, including confidentiality, integrity, availability, trust, and the CFIP model. This research concludes that authentication, data confidentiality, data integrity, non-repudiation, availability, data collection, secondary use, unauthorized access, and errors are the most concerning factors for healthcare professionals.
5.	Jibril Adamu, Raseeda Hamzah, Marshima Mohd Rosli[18]	Malaysia	250 articles that match the keywords	Literature Review	The security features of the three most popular and powerful PHP frameworks have been reviewed and compared. Laravel ensures a more secure Electronic Medical Record (EMR) by protecting against various attacks mentioned in this paper through its default best security features, minimizing the attack surface area by default.
6.	Jose Luis Fernandez Aleman[19]	Spanyol	A total of 49 articles were selected	A systematic literature review	From the articles in our review, and based on the five security areas analysed, we can conclude the following: Compliance, Information systems acquisition, development, maintenance, Access control, Communications and operations management.
7	Ismail Keshta, Ammar Odeh[20]	Arab Saudi	500 individuals	cyber-security measure	From the reviewed articles and based on the analysis in the security field, it can be seen that various regulations and standards related to privacy and security are used in electronic medical records. However, the harmonization of these

					systems is needed to resolve potential conflicts and inconsistencies between standards. Many encryption algorithms have been proposed by various articles.
8.	Laurinda B. Harman, PhD, RHIA, Cathy A. Flite, MEd, RHIA, and Kesa Bond, MS, MA, RHIA, PMP [21]	Amerika Serikat	Dokumen rekam medis	Qualitative	There are three major ethical priorities for electronic health records: privacy and confidentiality, security, and data integrity and availability.
9.	W. Bani Issa 1,2 PhD, RN , I. Al Akour 3 PhD , A. Ibrahim 4 PhD , A. Almarzouqi 5 PhD, RN , S. Abbas 6 PhD, RN , F. Hisham 7 RN & J. Griffiths 8 PhD, RN, MSc[22]	Sharjah	hospitals and primary healthcare centres [PHCs]	This study used an exploratory parallel mixed-method approach (QUAN + qual), with quantitative (survey) and qualitative (focus group interviews)	Nurses in our study voiced concerns related to data integrity, especially access by unauthorized personnel and lack of auditing of errors that occur within the system. As front- line EHR users, nurses in the UAE must study the legal and ethical aspects of storing patient data on computers to increase their professional knowledge and safeguard patient information. Knowledge and awareness in healthcare infor- matics, federal law and EHR data integrity will allow nurses to provide advice to patients and other providers on best practices to maintain data integrity and build ‘a safer system for better care’.

Table 1. Explanation of Security and Confidentiality of Medical Record Data in Hospitals through the Use of Electronic Medical Records is conducted through literature review and qualitative research involving journal samples as well as hospitals. In general, the researchers conducted a study related to the Security and Confidentiality of Medical Record Data on 5 indicators.

Table 2. Frequency Distribution of Security and Confidentiality of Medical Record Data in Hospitals

NO.	Variable	Distribution	
		total	Percentage (%)
1.	**Human Resources as a Threat** (employees are not aware of the security and confidentiality of medical record data, and breaches are initiated by employees)	7	77.7
2.	**Infrastructure and facilities** (EMR is not adequate to maintain the security and confidentiality of data; the system is not perfect and often encounters errors)	3	33.3
3.	**Policy** (lack of clear standard operating procedures, insufficient guidance to complete medical records, absence of	3	33,3

	policies, guidelines, and SOPs, lack of guidance, monitoring, and outreach)		
4.	**Funds** (insufficient funds to make EMR more perfect)	1	11,1

The analysis through document review results indicates that many parties suspect that electronic medical records do not have clear legal standing (33.3%), especially concerning assurance that stored data is protected against elements of privacy, confidentiality, and general information security. Technically, encryption technologies, including various biometric markers (such as fingerprints), would be more protective in safeguarding data than regular signatures [23]. However, the issue is not on technical matters but on legal aspects. A recurring question is: to what extent can hospitals provide protection against the security of patient data from irresponsible individuals? What is the validity of electronic documents? What if there are errors in the writing of patient medical data? All these questions often hinder the development of Electronic Medical Records (EMR). Therefore, clear regulations and legal provisions are needed, but unfortunately, the creation of regulations itself cannot match the speed of information technology progress. In some states in the US, some hospitals only print medical records when they are used as legal evidence. In Wan Fang Hospital, Taipei, it is the opposite; the hospital always keeps printed medical records that must be signed by doctors as a result of patient EMR printouts.

The next challenge is the classic reason of funding availability (11.1%). Financial aspects become a crucial issue because hospitals need to prepare Information Technology infrastructure (computers, wired and wireless networks, electricity, security systems, consultants, training, and so on). Hospitals typically have limited budgets, especially for information technology. Electronic Medical Records (EMR) are not a priority because hospitals prioritize other systems such as computerized billing systems, accounting systems, payroll systems, and so on [13]. Hospitals believe that these systems are prioritized as they can ensure fast, transparent, and accountable financial management of the hospital. EMR is often sidelined because transaction processing for medical service functions can still be done manually. No hospital cashier rejects the opinion that computers can provide faster and more effective billing services than manual systems. Conversely, how many doctors and nurses believe that their work will become faster, easier, and safer with the presence of computers?

The obstacles to the implementation of the EMR system are related to human resources (77.7%). One of the primary obstacles is the busy schedule of the EMR system, often leading to errors. Many EMR systems are used during busy hours, resulting in errors, slow performance, and failure to save entered data[24]. There are delays in entering data, where the EMR system is supposed to be real-time, but in the Emergency Room (IGD), one has to wait for patient procedures to be completed before entering data, and the EMR system is already closed. The initial use of the EMR system increases the workload for healthcare workers, where they have to back up both hard and soft files, making the process difficult, longer, causing longer queues, and the speed of doctor services is not matched with the speed of prescription services.

The researcher's assumption is the lack of readiness of human resources in the Security and Confidentiality of Medical Record Data in Hospitals, with the most prominent aspect being the unpreparedness of human resources and human resources as a threat. The absence of clear policies, according to the researcher's assumption, is due to the hospital's lack of willingness to improve hospital quality according to Ministry of

Health Regulation number 24 of 2022 and to enhance hospital accreditation. Therefore, the researcher suggests that every hospital should have clear and firm policies, especially regarding the security and confidentiality of data in Electronic Medical Records (EMR). Facilities and financial conditions, which will also be addressed in such policies, can be managed simultaneously.

REFERENCES

[1] Rahmatiqa C, Sulrieni IN, Novita Sary A. Kelengkapan Berkas Rekam Medis Dan Klaim Bpjs Di Rsud M.Zein Painan. J Kesehat Med Saintika 2020;11:11. https://doi.org/10.30633/jkms.v11i1.514.

[2] Buyl R, Beogo I, Fobelets M, Deletroz C, Van Landuyt P, Dequanter S, et al. E-Health interventions for healthy aging: A systematic review. Syst Rev 2020;9. https://doi.org/10.1186/s13643-020-01385-8.

[3] Tebeje TH, Klein J. Applications of e-Health to Support Person-Centered Health Care at the Time of COVID-19 Pandemic. Telemed e-Health 2021;27:150–8. https://doi.org/10.1089/tmj.2020.0201.

[4] Roziqin MC, Prameswari ADA, Wicaksono AP, Vestine V. Sistem Rekam Medis Elektronik Berbasis Web. JOINTECS (Journal Inf Technol Comput Sci 2022;7. https://doi.org/10.31328/jointecs.v7i3.3915.

[5] Sapriadi, Lase SPR. Hubungan Penggunaan Rekam Medis Elektronik Dengan Kepuasan Pengguna Rekam Medis Elektronik Di Unit Rawat Jalan Rumah Sakit Umum Mitra Medika Amplas Medan Tahun 2022. J Kesehat Dan Fisioter (Jurnal KeFis) 2023;2.

[6] Rahmatiqa C, Abdillah N, Yuniko F. Factors that cause compliance filling medical records in hospitals. Int J Community Med Public Heal 2020;7:4180. https://doi.org/10.18203/2394-6040.ijcmph20204393.

[7] Mukarom MZ, Septiawan C. Alternatif Kebijakan Ketidaklengkapan Pengisian Rekam Medis Pasien Tindakan Catheterisasi di Rumah Sakit. J Public Heal Educ 2022;1. https://doi.org/10.53801/jphe.v1i3.50.

[8] Lakhmudien L, Rano Indradi S, Ega Nugraha, Imam Agus Setiyono. PEMAHAMAN PEREKAM MEDIS TERHADAP PENERAPAN REKAM MEDIS ELEKTRONIK BERBASIS PERMENKES NOMOR 24 TAHUN 2022. J Cakrawala Ilm 2023;2. https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i9.5803.

[9] Meilia PDI, Christianto GM, Librianty N. Buah Simalakama Rekam Medis Elektronik: Manfaat Versus Dilema Etik. J Etika Kedokt Indones 2019;3:61. https://doi.org/10.26880/jeki.v3i2.37.

[10] Amalia N, Rustam MZA, Rosarini A, Wijayanti DR, Riestiyowati MA. The Implementation of Electronic Medical Record (EMR) in The Development Health Care System in Indonesia. Int J Adv Life Sci Res 2021;4. https://doi.org/10.31632/ijalsr.2021.v04i03.002.

[11] Kruse CS, Smith B, Vanderlinden H, Nealand A. Security Techniques for the Electronic Health Records. J Med Syst 2017;41. https://doi.org/10.1007/s10916-017-0778-4.

[12] Satria Indra Kesuma. REKAM MEDIS ELEKTRONIK PADA PELAYANAN RUMAH SAKIT DI INDONESIA: ASPEK HUKUM DAN IMPLEMENTASI. ALADALAH J Polit Sos Huk Dan Hum 2023;1. https://doi.org/10.59246/aladalah.v1i1.188.

[13] Noor AY, Ainy N. Kajian Yuridis Normatif Penyelenggaraan Rekam Medis Elektronik Di Fasilitas Kesehatan. J INFOKES-Politeknik Piksi Ganesha 2020;4.

[14] Wang CK. Security and privacy of personal health record, electronic medical record and health information. Probl Perspect Manag 2015;13.

[15] Ningtyas AM, Lubis IK. Literatur Review Permasalahan Privasi Pada Rekam Medis Elektronik. Pseudocode 2018;5. https://doi.org/10.33369/pseudocode.5.2.12-17.

[16] Amin M, Setyonugroho W, Hidayah N. Implementasi Rekam Medik Elektronik: Sebuah Studi Kualitatif. JATISI (Jurnal Tek Inform Dan Sist Informasi) 2021;8. https://doi.org/10.35957/jatisi.v8i1.557.

[17] Enaizan OM, Alwi NH, Zaizi NJ. Privacy and Security Concern for Electronic Medical Record Acceptance and Use: State of the Art. J Adv Sci Eng Res 2017;7.

[18] Adamu J, Hamzah R, Rosli MM. Security issues and framework of electronic medical record: A review. Bull Electr Eng Informatics 2020;9. https://doi.org/10.11591/eei.v9i2.2064.

[19] Señor IC, Alemán JLF, Toval A. Personal health records: New means to safely handle health data? Computer (Long Beach Calif) 2012;45. https://doi.org/10.1109/MC.2012.285.

[20] Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egypt Informatics J 2021;22. https://doi.org/10.1016/j.eij.2020.07.003.

[21] Harman LB, Flite CA, Bond K. Electronic health records: Privacy, confidentiality, and security. Virtual

Mentor 2012;14. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209.
[22] Bani Issa W, Al Akour I, Ibrahim A, Almarzouqi A, Abbas S, Hisham F, et al. Privacy, confidentiality, security and patient safety concerns about electronic health records. Int Nurs Rev 2020;67. https://doi.org/10.1111/inr.12585.
[23] Shahnaz A, Qamar U, Khalid A. Using Blockchain for Electronic Health Records. IEEE Access 2019;7. https://doi.org/10.1109/ACCESS.2019.2946373.
[24] Rahmatiqa, C., Elfentriani, Angelia I. Analisis Kelengkapan Pengisian Berkas Rekam Medis Rawat Inap Di Rumah Sakit Umum Daerah Sungai Dareh Tahun 2020. J Kesehat Med Saintika 2020;11.