KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research (JSSR)
Vol.4, No.5 Oktober 2026
e-ISSN: 3025-9851, p-ISSN : 3025-986X, Hal 86-95
DOI : https://doi.org/10.61722/jssr.v4i5.11998

SAFETY AND CONFIDENTIALITY OF PATIENT DATA IN ELECTRONIC MEDICAL RECORD SYSTEMS

Reliana Cristiana de Jesus[1*], Aulia Nur'aini[2], Adeleo Ariko Verdiansyah[3], Amalia Fajriyatun Sholihah[4], Renata de Araujo[5], Ahmad Sunandar [6]
[1-6] Departemen Rekam Medis , ilmu kesehatan, Politeknik Indonusa Surakarta , Jl. Palem No. 8 Jati, Cemani, Grogol, Kabupaten Sukoharjo, Jawa Tengah 57552.
*Penulis Korespondensi: relianacristianadejesus@gmail.com

Abstract. *The development of information technology has brought great changes in health services, one of which is through the implementation of the Electronic Medical Record System (RME). The use of RME provides various advantages, such as ease of information access, increased service efficiency, and reduced use of paper-based documents. However, behind these benefits there are challenges related to the security and confidentiality of patient data. Health data is private and very sensitive information so it requires maximum protection from various threats, such as data leakage, unauthorized access, data manipulation, and cyber attacks. This article aims to examine the importance of the security and confidentiality of patient data in the electronic medical record system, identify threats that can occur, and explain various efforts that can be made to maintain the security of health information. This research uses the literature study method by analyzing various national and international journals, books, and regulations that apply in Indonesia. The results of the study show that the implementation of information security technology combined with compliance with regulations and improving human resource competence is the main factor in maintaining the confidentiality of patient data.*

Keywords: *Electronic Medical Records; Information Security; Data Confidentiality; Patient Data; Health Information System.*

Abstrak. Perkembangan teknologi informasi telah membawa perubahan besar dalam pelayanan kesehatan, salah satunya melalui penerapan Sistem Rekam Medis Elektronik (RME). Penggunaan RME memberikan berbagai keuntungan, seperti kemudahan akses informasi, peningkatan efisiensi pelayanan, dan pengurangan penggunaan dokumen berbasis kertas. Namun, di balik manfaat tersebut terdapat tantangan yang berkaitan dengan keamanan dan kerahasiaan data pasien. Data kesehatan merupakan informasi yang bersifat pribadi dan sangat sensitif sehingga memerlukan perlindungan yang maksimal dari berbagai ancaman, seperti kebocoran data, akses tanpa izin, manipulasi data, maupun serangan siber. Artikel ini bertujuan mengkaji pentingnya keamanan dan kerahasiaan data pasien pada sistem rekam medis elektronik, mengidentifikasi ancaman yang dapat terjadi, serta menjelaskan berbagai upaya yang dapat dilakukan untuk menjaga keamanan informasi kesehatan. Penelitian ini menggunakan metode studi literatur dengan menganalisis berbagai jurnal nasional maupun internasional, buku, serta regulasi yang berlaku di Indonesia. Hasil kajian menunjukkan bahwa penerapan teknologi keamanan informasi yang dipadukan dengan kepatuhan terhadap regulasi dan peningkatan kompetensi sumber daya manusia menjadi faktor utama dalam menjaga kerahasiaan data pasien.

Kata kunci: Rekam Medis Elektronik; Keamanan Informasi;Kerahasiaan Data; Data Pasien; istem Informasi Kesehatan

1. INTRODUCTION

Digital transformation in the healthcare sector has advanced rapidly in response to the growing demand for effective, efficient, and high-quality healthcare services. One of the major forms of this transformation is the implementation of Electronic Medical

Naskah Masuk:01 Juli 2026; Revisi: 02 Juli 2026; Diterima: 03 Juli 2026; ; Terbit:15 Juli 2026

Records (EMRs), a system used to store, manage, and access patients' health information digitally. The implementation of EMRs offers numerous benefits, including improving the efficiency of healthcare services, enhancing coordination among healthcare professionals, reducing documentation errors, and facilitating reporting processes as well as clinical decision-making.

In Indonesia, the implementation of Electronic Medical Records has been strengthened through the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records, which requires healthcare facilities to gradually adopt electronic medical record systems. This digitalization represents an important step toward improving the quality of healthcare services while supporting the national healthcare transformation agenda.

However, the adoption of electronic systems also increases the risk of information security threats. Patient data contain not only personal identification information but also medical histories, examination results, clinical interventions, and payment information, all of which are highly confidential. Data breaches may lead to the misuse of personal information, identity theft, discrimination, and financial losses for both patients and healthcare institutions.

Therefore, ensuring the security and confidentiality of patient data is one of the most critical aspects of implementing Electronic Medical Records. Such protection should not rely solely on information security technologies but must also be supported by organizational policies, compliance with applicable regulations, and increased awareness among healthcare professionals regarding the importance of maintaining the confidentiality of patient information.

2. LITERATURE REVIEW

According to the Ministry of Health

In accordance with the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022, Article 29, Electronic Medical Records (EMRs) must comply with the following data and information security requirements:

A. Confidentiality

Data and information must be protected from unauthorized access or intervention by both internal and external parties. Electronic Medical Record data must not be accessed, used, or disclosed by individuals who do not have authorized access.

B. Integrity

Integrity ensures that the data and information contained in Electronic Medical Records remain accurate, complete, and can only be modified by individuals who have the appropriate authority.

C. Availability

Availability means that when access rights are granted by the head of a healthcare facility, the data and information contained in Electronic Medical Records must be accessible and available to authorized users whenever needed.

Electronic Medical Records (EMRs)

Electronic Medical Records (EMRs) are medical records created using electronic systems to record, store, manage, and provide information regarding patient identity, examination results, diagnoses, treatments, medical procedures, and other healthcare services provided to patients. The implementation of EMRs aims to improve the efficiency of healthcare services, facilitate access to medical information, enhance the quality of healthcare delivery, and support the continuity of patient care. Compared with conventional paper-based medical records, EMRs provide significant advantages, including integrated data storage, easier information retrieval, and improved data exchange among healthcare facilities.

Information Security

Information security refers to the process of protecting information from various threats in order to ensure service continuity, minimize risks, and maintain users' trust. According to the ISO/IEC 27001:2022 standard, information security is the practice of preserving the confidentiality, integrity, and availability of information through the implementation of appropriate policies, procedures, technologies, and security controls.

Within Electronic Medical Record systems, information security is particularly important because patient data are highly sensitive and should only be accessed by authorized individuals.

CIA Triad Theory

The CIA Triad is the fundamental concept of information security, consisting of three primary principles:

a. Confidentiality refers to the principle that ensures information can only be accessed by authorized individuals. In EMR systems, confidentiality is maintained through user authentication, role-based access control (RBAC), and data encryption.

b. Integrity is the principle that ensures information remains accurate, complete, and protected from unauthorized modification. Maintaining data integrity is essential to ensure that medical information used in healthcare services remains reliable and trustworthy.

c. Availability is the principle that ensures information is accessible to authorized users whenever it is needed. To maintain data availability, healthcare facilities should implement data backup systems, disaster recovery plans, and reliable information technology infrastructure. These three principles serve as the foundation for developing secure Electronic Medical Record systems.

Patient Data Confidentiality

Patient data confidentiality is the obligation of healthcare professionals and healthcare facilities to protect all information regarding a patient's health condition from being disclosed to unauthorized parties without the patient's consent, except in circumstances permitted by applicable laws and regulations. Patient confidentiality is both an ethical responsibility of healthcare professionals and a means of safeguarding patients' right to privacy.

In Electronic Medical Record systems, maintaining data confidentiality becomes even more critical because information is stored digitally, making it more vulnerable to data breaches if appropriate security measures are not implemented.

Personal Data Protection

Personal data protection refers to a series of measures undertaken to ensure the security of personal data throughout its collection, storage, use, processing, and disposal.

Health data are classified as specific categories of personal data and therefore require a higher level of protection than general personal data.

In the implementation of Electronic Medical Records, every healthcare facility is required to manage patient data in accordance with personal data protection principles to ensure that patients' rights are fully protected.

Electronic Medical Record Regulations in Indonesia

The implementation of Electronic Medical Records in Indonesia is regulated by the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records. The regulation requires every healthcare facility to implement Electronic Medical Records while ensuring data security, confidentiality, integrity, and availability.

Furthermore, patient data protection is reinforced by Law Number 27 of 2022 on Personal Data Protection, which regulates the rights of data subjects and the responsibilities of data controllers in safeguarding personal information. These provisions are further supported by Law Number 17 of 2023 on Health, which guarantees every patient's right to the confidentiality of their health information.

The Role of Medical Record Professionals in Information Security

Medical record professionals are responsible for managing medical records in a complete, accurate, secure, and confidential manner. In addition to managing patient data, they play important roles in access control management, data quality monitoring, medical record auditing, and supporting the implementation of information security policies within healthcare facilities. This role has become increasingly important with the growing adoption of Electronic Medical Record systems in Indonesia.

3. RESEARCH METHOD

This study employed a literature review methodology. Data were collected from various scientific sources, including national and international journal articles, books, government regulations, and official publications related to information security, Electronic Medical Records, and patient data protection. The collected literature was analyzed descriptively to provide a comprehensive understanding of data security

concepts, potential threats, and protection strategies that can be implemented in Electronic Medical Record systems.

4. RESULTS AND DISCUSSION

This study employed a literature review method by collecting various scientific sources related to the security and confidentiality of patient data in Electronic Medical Record (EMR) systems. The literature reviewed included national and international journal articles, reference books, government regulations, and other official publications governing the implementation of Electronic Medical Records and the protection of personal data. The analysis was conducted by identifying key concepts, comparing the findings of previous studies, and synthesizing these findings to provide a comprehensive understanding of the implementation of information security in EMR systems.

Implementation of Security and Confidentiality in Electronic Medical Records

The findings of the literature review indicate that the implementation of Electronic Medical Records (EMRs) has a positive impact on improving the quality of healthcare services. The digitalization of medical records enables patient data to be stored in an integrated manner, allowing healthcare professionals to access clinical information quickly and accurately. Several studies have reported that the use of EMRs can accelerate healthcare service delivery, reduce documentation errors, improve coordination among healthcare professionals, and support more accurate clinical decision-making.

On the other hand, the digitalization of medical records increases information security risks because patient data constitute one of the most sensitive categories of personal information. The information stored in Electronic Medical Records (EMRs) includes patient identification, medical history, diagnostic test results, diagnoses, medical procedures, treatments, and payment information. Unauthorized access to or disclosure of such information may result in privacy violations, harm to patients, and a decline in public trust in healthcare facilities.

These findings are consistent with the study by Nazuhra et al. (2026), which stated that protecting patient privacy is a fundamental component of Electronic Medical Record implementation. Furthermore, Setyaningrum and Ricky (2025) explained that data security in EMR systems must adhere to the principles of Confidentiality, Integrity, and

Availability (CIA Triad) to ensure the confidentiality, integrity, and availability of patient data.

Threats to Information Security in Electronic Medical Records

Based on the synthesis of several previous studies, threats to patient data security originate from both internal and external factors. Internal threats are generally caused by human error, such as the use of weak passwords, account sharing, failure to log out of the system, and misuse of access privileges by authorized personnel. Meanwhile, external threats include malware attacks, ransomware, phishing, hacking, theft of electronic devices, and disruptions to information technology infrastructure

Threats to Information Security in Electronic Medical Records (EMRs)

Based on the synthesis of several previous studies, threats to patient data security originate from both internal and external factors. Internal threats are generally caused by human error, such as the use of weak passwords, account sharing, failure to log out of the system, and the misuse of access privileges by authorized personnel. Meanwhile, external threats include malware attacks, ransomware, phishing, hacking, theft of electronic devices, and disruptions to information technology infrastructure.

The study conducted by Inggrid et al. (2026) found that the majority of information security incidents are still influenced by users' behavior. These findings indicate that the successful implementation of information security depends not only on technological solutions but also on the competence of human resources in consistently adhering to security procedures.

Conceptually, these findings support information security theory, which identifies human factors as one of the most vulnerable components of any information system. Therefore, enhancing **security awareness** has become an essential aspect of the effective management of Electronic Medical Records (EMRs).

Protection Measures for Patient Data in Electronic Medical Records (EMRs)

The findings of the literature review indicate that patient data protection should be implemented through a combination of technical, administrative, and regulatory measures. From a technical perspective, various studies recommend the implementation

of user authentication, role-based access control (RBAC), data encryption, audit trails, firewalls, antivirus software, data backup systems, and disaster recovery plans. The implementation of these technologies aims to prevent unauthorized access while ensuring the continuity of healthcare services in the event of system disruptions.

In addition to technical measures, patient data protection also requires strong organizational policies through the development of Standard Operating Procedures (SOPs), regular evaluations of information system security, and continuous training for healthcare professionals on information security and patient data confidentiality. These findings are consistent with the study by Jawab et al. (2023), which reported that the effectiveness of patient data protection is influenced by the synergy among technological measures, organizational policies, and compliance with applicable regulations.

From a regulatory perspective, the implementation of information security in Indonesia is supported by the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records, Law Number 27 of 2022 on Personal Data Protection, and Law Number 17 of 2023 on Health. These regulations emphasize that healthcare facilities are responsible for ensuring the confidentiality, security, integrity, and availability of patient data.

The findings of this review suggest that strengthening the security of Electronic Medical Records (EMRs) not only protects patients' privacy rights but also improves the quality of healthcare services, enhances public trust in healthcare institutions, and supports the digital transformation of the healthcare system in Indonesia. From a theoretical perspective, the findings reinforce the concept that information security is built upon the integration of technology, human resources, and regulatory frameworks. From a practical perspective, healthcare facilities should implement comprehensive information security systems and continuously improve the competencies of healthcare professionals to minimize the risk of patient data breaches.

5. CONCLUSION AND RECOMMENDATIONS

The security and confidentiality of patient data are fundamental aspects of the implementation of Electronic Medical Records (EMRs). Although the digitalization of healthcare services offers significant benefits, it also increases the risk of information

breaches if not supported by adequate security measures. Patient data protection should be achieved through the implementation of security technologies such as authentication, authorization, data encryption, audit trails, firewalls, and data backup systems. These technical measures must be complemented by organizational policies and compliance with applicable regulations. Furthermore, enhancing the competencies of healthcare professionals in information security is essential for establishing a healthcare system that is secure, reliable, and of high quality.

Healthcare facilities should continuously strengthen their information security systems by adopting both national and international standards to ensure the optimal protection of patient data. In addition, all healthcare professionals should receive regular training on information security and patient data confidentiality to develop a thorough understanding of how to prevent data breaches and the unauthorized use of patient information.

Furthermore, the government is expected to strengthen oversight of Electronic Medical Record implementation by developing more comprehensive policies, conducting regular evaluations, and providing guidance to healthcare facilities to ensure that all Electronic Medical Record management processes comply with applicable regulations. Future research is recommended to investigate the effectiveness of emerging security technologies, such as artificial intelligence (AI) and blockchain, in enhancing the security, confidentiality, and integrity of health data within Electronic Medical Record systems.

REFERENCES

Herlina, Fernandes Andry, J., & Marcellus Susanto, F. (2023). Analisis Deskriptif Perilaku Konsumen Shopee: Technology Acceptance Model (TAM). *Journal of Technology and Informatics (JoTI)*, *4*(2), 63–68.

Inggrid, A., Maharani, P., Novratilova, S., Wulandari, R., Aulia, D. R., Dewi, A. T., & Saputra, A. J. (2026). *Studi Literature : Analisis Keamanan dan Privasi Data Rekam Medis Elektronik Fasilitas Pelayanan Kesehatan Berdasarkan UU Nomor 27 Tahun 2022 72 jam kepada otoritas PDP , menunjuk Data Protection Officer (DPO), dan melakukan Data mengenai keamanan dan p*. (24).

Jawab, T., Sakit, R., Data, K., Pada, P., & Medis, R. (2023). *J-LEE. 7*, 36–45.

Nazuhra, F., Novratilova, S., Aprilia, D. F., Pramudita, F. G., Kampus, A., Kh, I. J., No, S., Bumi, K., Laweyan, K., Tengah, J., Ii, K., Palem, J., Grogol, K., & Tengah, J. (2026). *Perlindungan dan Keamanan Privasi Data Pasien pada Sistem Rekam.*

Setyaningrum1, E., & Ricky, A. V. (2025). Analisis Keamanan Data Pasien dalam Rekam Medis Elektronik Berdasarkan Cia Triad di RSUD X Jawa Tengah. *Jurnal Ners*, *9*(3), 4216–4221. https://doi.org/10.31004/jn.v9i3.46352 *Medis Elektronik di Fasilitas Pelayanan Kesehatan : Studi Literatur Politeknik Indonusa Surakarta , Indonesia Indonesia . Dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal . 04*, 417–427.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO.

World Health Organization. (2021). Global Strategy on Digital Health 2020–2025. World Health Organization.

Republik Indonesia. (2022). Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis.

Republik Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Republik Indonesia. (2023). Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 tentang Kesehatan.