RECHTSVINDING
Vol. 3, 1 (June, 2025), pp. 35-42
EISSN: 2987-4424, DOI: 10.59525/rechtsvinding.v3i1.665

Protection of Personal Data in Electronic Medical Records (RME) in Healthcare Facilities Reviewed from a Human Rights Perspective

Hawreyvian Rianda Seputra[1], Carolina Kuntardjo[2], Krisnandifa Marshafira Riyandini[3], Nanang Zuli Purwanto[4]

[1] Universitas Wisnuwhardana Malang, Indonesia; hriandaseputra@gmail.com
[2] Universitas Wisnuwhardana Malang, Indonesia; carolinakuntardjo@gmail.com
[3] Universitas Wisnuwhardana Malang, Indonesia; krisnandifamarshafira@gmail.com
[4] Universitas Wisnuwhardana Malang, Indonesia; nanangzuli5758@gmail.com

ARTICLE INFO

Keywords:

Personal Data Protection;
Electronic Medical Records;
Human Rights

Article history:

Received 2025-01-19
Revised 2025-03-30
Accepted 2025-05-05

ABSTRACT

The advancement of digital technology has transformed medical record systems from conventional formats to Electronic Medical Records (EMRs). While EMRs enhance healthcare service efficiency, they also introduce challenges concerning the protection of patients' personal data. Privacy issues have become increasingly critical and require examination from a human rights perspective, particularly the right to privacy and personal data protection. This study employs a normative qualitative method focusing on legal frameworks, human rights principles, and relevant regulations. Data were collected through literature reviews of national laws, international human rights conventions, academic journals, and official documents. A descriptive-qualitative analysis was used to construct a systematic and logical scientific argument. Findings show that patient data protection in EMRs is regulated under the Personal Data Protection Law and Ministry of Health regulations, emphasizing confidentiality, data integrity, and security in accordance with human rights standards. However, practical implementation faces several challenges, including inadequate technological infrastructure, low awareness among healthcare personnel, and weak oversight and law enforcement. These gaps result in a high risk of data breaches, driven by technical vulnerabilities, human error, misuse of access by internal staff, and the absence of effective monitoring systems. Although patients' rights to access and correct their data are legally acknowledged, consistent implementation across healthcare facilities remains limited.

Corresponding Author:
Hawreyvian Rianda Seputra
Universitas Wisnuwhardana Malang, Indonesia; hriandaseputra@gmail.com

1. INTRODUCTION

Electronic medical records (RME) are innovations in the field of health services that aim to accelerate, facilitate, and improve accuracy in recording patients' health histories (Adrian et al., 2023). The use of digital technology in medical record management brings many benefits such as time efficiency, reduced recording errors, and ease of data access for health workers. However, behind its advantages, RME also opens up opportunities for threats to the confidentiality and security of patients' personal data. The leakage of medical information can be fatal, not only to personal losses to patients, but also to the credibility of the healthcare facility itself (Hadiyantina et al., 2023).

The protection of personal data in electronic medical records is a major challenge as the use of digital systems in the health sector increases. Medical data is a category of sensitive data that should receive maximum protection in accordance with the principles of Human Rights (HAM), especially the right to privacy (Rosyada et al., 2017). Many healthcare facilities have not fully implemented adequate information security standards, leading to potential misuse of data by unauthorized parties. This condition raises concerns about the extent to which health facilities are able to protect patients' rights in the current digital era (Ningtyas & Lubis, 2018).

Demands for privacy protection are getting stronger along with the many reports of data breaches in various sectors, including the health sector. Various cases show that security gaps in the management of RME can lead to the dissemination of patient information to third parties without legitimate consent (Yunisca et al., 2022). This violation not only violates national legal norms, but also goes against international human rights principles that affirm the importance of protecting the personal data of every individual. This is stated in the Universal Declaration of Human Rights (DUHAM) 1948, in particular in Article 12 which states that no one shall be subjected to arbitrary interference with his or her privacy, family, home, or correspondence, and that everyone has the right to legal protection against such interference. This situation indicates that the protection of personal data in health facilities requires serious attention from various parties, including policymakers, health workers, and information system managers (Apriliyani, 2021).

Along with the strengthening of national regulations regarding the protection of personal data, the challenges of its implementation in health facilities are not only related to technical aspects, but also aspects of legal and ethical awareness of health service actors. There are still health facilities that do not have an adequate data management system or do not fully understand data protection standards based on human rights principles. The inconsistency in the application of this data protection policy creates a risk of injustice for patients, who are essentially entitled to security guarantees of their personal medical information.

This study aims to analyze the protection of personal data in electronic medical records in healthcare facilities from a Human Rights perspective. The focus of the study is directed at the identification of patient data protection problems, analysis of the protection efforts that have been carried out, and evaluation of their conformity with human rights principles. This research is expected to make an academic and practical contribution in strengthening the guarantee of patients' privacy rights in the midst of information technology developments in the health sector.

2. METHOD

The research method used in this study is a qualitative research method with a normative approach. The normative approach was chosen because this study focuses on the analysis of legal rules, human rights principles, and normative provisions related to the protection of personal data in electronic medical records in health facilities. The analysis was carried out on various legal sources such as national laws and regulations, international conventions related to human rights, and other official documents related to patient data protection. This approach allows researchers to understand how personal data protection should be implemented based on applicable normative provisions.

The data collection technique is carried out through literature studies, namely collecting data from scientific journals, legal books, academic articles, and relevant laws and regulations. The data collected

includes theories about the protection of personal data, electronic medical records, as well as the principles of Human Rights that govern the right to privacy and security of personal information. The data collection process is carried out systematically by selecting credible and relevant sources in order to obtain a strong theoretical basis and legal basis for analysis. The literature search also includes the results of previous research that discuss similar issues to enrich the analytical perspective.

The data analysis technique uses a descriptive-qualitative analysis method, which is by describing the content of various sources that have been collected, then studying and comparing them to find the relationship between theories, human rights principles, and legal provisions regarding personal data protection. The analysis was carried out by classifying data based on key themes, such as the concept of personal data protection, protection standards in electronic medical records, and the application of human rights principles in the health system. The classified data is interpreted to formulate scientific arguments that answer the formulation of research problems in a logical, systematic, and structured manner.

3. RESULTS AND DISCUSSION

Forms of Patient Personal Data Protection in Electronic Medical Records in Health Facilities

The protection of patients' personal data in electronic medical records (RME) in healthcare facilities is strictly regulated through regulations and the implementation of information technology security standards. Patient data in RME includes highly sensitive information, such as medical history, examination results, diagnosis, and treatment. The confidentiality of this data is the main foundation of trust between patients and healthcare providers, so privacy protection is a very crucial aspect. The risk of data leakage or misuse can lead to serious impacts, ranging from privacy breaches to social and economic losses for patients (Naurah et al., 2024).

The main regulation that regulates the protection of patient data in RME in Indonesia is the Regulation of the Minister of Health (Permenkes) No. 24 of 2022 concerning Medical Records. This Regulation requires all health facilities, including independent doctor practices, health centers, clinics, hospitals, pharmacies, laboratories, and telemedicine services, to implement RME. The three main principles that must be met in the management of an RME are confidentiality, integrity, and availability. Confidentiality ensures that only the authorities can access patient data through strict access control and authentication. Integrity guarantees that data cannot be changed without permission, and any changes must be clearly recorded. Availability ensures that data can be accessed at any time by the authorities, supported by a backup system and protection from interference (Rubiyanti, 2023).

Healthcare facilities are required to implement various technical measures to protect patient data. These measures include the use of data encryption during storage and transmission, two-factor authentication, restriction of access rights to authorized users only, and recording of data access activities. In addition, the regular use of the latest security technologies and data backup systems is also mandatory. The implementation of international standards such as ISO/IEC 27001:2013 is a reference in the management of information security in healthcare facilities, including routine security audits to detect and address potential security gaps (Indriyajati et al., 2023).

In terms of patients' rights, regulations provide guarantees for the confidentiality of their data as well as the right to access, request changes, or corrections of medical record data. Patients are also entitled to their medical record data in electronic or printed form as needed. Any exchange or recording of RME data must be made based on the patient's consent, and the use of data is only permitted for healthcare purposes. Health workers are required to maintain data confidentiality, not to leak information without permission, and to use data only for medical purposes. Violations of this data protection can be subject to disciplinary sanctions, administrative, and compensation to aggrieved patients (Wahyuntara et al., 2024).

The challenges in protecting patient data at RME are still quite large, especially related to vulnerabilities to cyber threats such as hacking and data leaks. Many health institutions still face

inadequate security infrastructure, low awareness among health workers of the importance of data privacy, and weak oversight and enforcement of privacy violations. Therefore, efforts to protect patients' personal data in RME must continue to be improved through strengthening regulations, increasing technological capacity, and education and training for all parties involved in medical data management.

Factors Causing Personal Data Protection Violations in the Management of Electronic Medical Records

The factors that cause personal data protection violations in the management of electronic medical records are very complex and interrelated. One of the main causes is the weak technological security infrastructure in many healthcare facilities. Many healthcare institutions, especially in the regions, are still using systems and hardware that do not yet meet modern cybersecurity standards. This condition causes electronic medical record systems to become vulnerable to cyberattacks such as hacking, malware, and ransomware. When systems do not have adequate protection, cybercriminals can easily access, steal, or even damage highly sensitive patient data, thereby increasing the risk of massive data leaks (Asih et al., 2024).

Human error is also a significant factor in the violation of patient personal data protection. These errors can be in the form of negligence when entering data, using weak passwords, to the practice of sharing accounts or unauthorized access to other parties. The lack of training and understanding of health workers on the importance of maintaining the confidentiality of patient data exacerbates this situation. Many healthcare workers do not understand the legal implications of data privacy breaches, so they tend to ignore standard security procedures. The practice of using the auto-fill feature without verification, incomplete data filling, and undisciplined access management are often loopholes that irresponsible parties take advantage of (Ramadhian et al., 2024).

System errors or software failures are also often the cause of data breaches. Health information systems that are not maintained, not updated regularly, or have bugs and security holes can cause patient data to be leaked or lost. System malfunctions can lead to data duplication, errors in sending data to the wrong department, or even failures in the data storage and retrieval process. Malware attacks that infiltrate unprotected systems can also lead to massive data corruption or theft of information. The lack of security assessment and penetration testing exacerbates the vulnerability of systems to digital threats (Pb & Sutabri, 2024).

The complexity of information technology used in the management of electronic medical records is also a challenge. Integration of various applications, devices, and networks that are not yet optimal often creates weak points in the system. Any interaction between the user and the system, especially if it is not supported by a friendly user interface and clear security protocols, increases the risk of errors or access breaches. The reliance on technology vendors that do not have high security standards also increases the likelihood of data leaks due to gaps in third-party applications or software used (Budiman et al., 2025).

Another internal factor that is no less dangerous is the misuse of data by medical personnel or healthcare staff who have access to electronic medical records. This misuse can be in the form of unauthorized access, disclosure of data to third parties without the patient's consent, or the use of data for personal or commercial purposes. This kind of action is not only unlawful, both administrative and criminal, in accordance with the Personal Data Protection Law (PDP Law) and related regulations. The lack of internal supervision and weak law enforcement in the health facility environment increase the risk of violations by internal personnel (Setiawan, 2024).

Weak supervision and enforcement are also the main factors that allow personal data protection violations in electronic medical records. Many cases of violations are not detected or not followed up decisively due to the lack of security audits, lack of incident reporting, and the lack of optimal sanction mechanisms for violators. Low compliance with regulations, both in terms of health facilities and medical personnel, causes data protection efforts to often be only formal. Without consistent

supervision and strict law enforcement, violations will continue to occur and public trust in the digital health system will decline (Herisasono, 2024).

Conformity of Personal Data Protection in Electronic Medical Records with Human Rights Principles

The protection of personal data in electronic medical records (RME) in health facilities has in principle been directed to be in line with human rights (HAM), especially the right to privacy and personal data protection guaranteed in Article 28G paragraph (1) of the 1945 Constitution. This constitution affirms every individual's right to personal self, family, and honor protection, which includes the confidentiality of health information. Regulations such as Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and Regulation of the Minister of Health (Permenkes) No. 24 of 2022 concerning Medical Records are the main legal basis. The PDP Law regulates the principles of legality, specific objectives, transparency, accuracy, security, and accountability in data management, while Permenkes 24/2022 requires health facilities to implement an RME system with strict information security standards, including encryption and periodic audits.

Harmonization between the public interest and patients' privacy rights remains a challenge. Although Permenkes 24/2022 requires health facilities to open access to RME to the government for the purpose of national health supervision and services, this has the potential to collide with human rights principles if it is not balanced with adequate security mechanisms. Article 17 of the PDP Law allows data processing without consent only in the interest of public health, but its implementation is vulnerable to a breach of confidentiality if not proportionately restricted. Studies show that the opening of RME access to the government has not fully met the principles of necessity and proportionality, due to the lack of derivative rules that govern the procedures, restrictions, and supervision of such access.

From the perspective of patient rights, regulations have provided strong guarantees through the principle of informed consent and the right to data correction. Article 26 of Permenkes 24/2022 states that the use of RME must be based on the patient's consent, except in an emergency. Patients also have the right to access, request a copy, or correct their medical data in accordance with Article 5 of the PDP Law. However, implementation in the field is often inconsistent. Many healthcare facilities do not yet provide transparent approval mechanisms or easy data access request procedures for patients. The unclear limitation of the "public interest" in Article 45 of the PDP Law also risks being used to open data without a valid reason, ignoring the principle of purpose limitation in human rights.

The principle of data security as part of human rights is implemented through the obligation of health facilities to implement a technical and administrative protection system. Permenkes 24/2022 requires data encryption, multi-factor authentication, and role-based access control. The ISO/IEC 27001:2013 standard on information security management is also adopted to prevent data leaks. However, reports show that 60% of healthcare facilities in Indonesia are still using vulnerable IT infrastructure, with security systems not yet meeting these standards. Weak supervision by the Ministry of Health and the absence of strict sanctions against violators exacerbate the risk of violating patients' privacy rights (Indra et al., 2024).

Efforts to align RME data protection with human rights still require improvements in regulations and institutional capacity. The recommendations from the legal study suggest the establishment of technical regulations derived from Permenkes 24/2022 involving human rights experts to ensure that the government's access mechanism does not violate privacy. Strengthening Health Law Number 36 of 2009 is also needed to accommodate the principles of data minimization and storage limitation as stated in the PDP Law (Mardiana et al., 2023). At the operational level, increasing healthcare workers' awareness of the ethics of medical confidentiality and investing in privacy-preserving technologies such as blockchain for RME could be a long-term solution. Thus, even though the legal framework is aligned with human rights principles, concrete implementation still needs to be strengthened to ensure a balance between individual rights and collective interests.

4. CONCLUSION

The protection of personal data in electronic medical records in health facilities has been comprehensively regulated through regulations such as Law Number 27 of 2022 concerning Personal Data Protection and Regulation of the Minister of Health No. 24 of 2022 concerning Electronic Medical Records, which affirm the obligation of health facilities to maintain the confidentiality, security, and integrity of patient data and limit access only to the authorities. Although this regulation has referred to human rights principles, especially the right to privacy guaranteed by the 1945 Constitution, implementation in the field still faces various obstacles such as inadequate technological infrastructure, low awareness of health workers, and weak supervision and law enforcement, so that the risk of data breaches remains high. Factors that cause breaches include technical weaknesses in security systems, human error, misuse of access by internal actors, and lack of effective oversight, all of which have the potential to threaten the confidentiality and integrity of patient data.

Safeguards include the implementation of encryption technology, multi-factor authentication, role-based access restrictions, and patients' right to access and correct their data, but the implementation of these mechanisms is not even across healthcare facilities. To ensure the protection of patients' personal data that is truly in line with human rights principles, it is necessary to strengthen technical regulations, increase technological and human resource capacity, and enforce strict laws to maintain public trust in the electronic medical record system and ensure patients' privacy rights as a whole.

REFERENCES

Adrian, H., Purnami, C. T., & Suryoputro, A. (2023). Analisis Dokumentasi Rekam Medis Elektronik di Fasilitas Pelayanan Kesehatan: Literature Review: Analysis of Electronic Medical Record's Documentation In Health Care Facilities : Literature Review. *Media Publikasi Promosi Kesehatan Indonesia (MPPKI)*, *6*(11).

Apriliyani, S. (2021). Penggunaan Rekam Medis Elektronik Guna Menunjang Efektivitas Pendaftaran Pasien Rawat Jalan di Klinik dr. Ranny. *Cerdika: Jurnal Ilmiah Indonesia*, *1*(10).

Asih, H. A., Indrayadi, I., Soraya, S., & Khairunnisa, K. (2024). Evaluasi Keamanan Data Pasien Pada Rekam Medis Elektronik Dengan Systematic Literature Review. *Jurnal Ilmiah FIFO*, *16*(2).

Budiman, A., Isa, M., & Soekiswati, S. (2025). Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta. *Ranah Research : Journal of Multidisciplinary Research and Development*, *7*(3).

Hadiyantina, S., Ayub, Z. A., Cahyandari, D., Paramitha, A. A., Ambarwati, S. D., Mustofa, Y., Sudjati, X. Q. D., & Rahmatika, N. A. (2023). *Perlindungan Data Pribadi dalam Bidang Rekam Medis*. Universitas Brawijaya Press. https://doi.org/10.11594/ubpress9786232967366

Herisasono, A. (2024). Perlindungan Hukum terhadap Privasi Data Pasien dalam Sistem Rekam Medis Elektronik. *Jurnal Kolaboratif Sains*, *7*(12).

Indra, I., Dewi, T. N., & Wibowo, D. B. (2024). Perlindungan Kerahasiaan Data Pasien vs Kewajiban Membuka Akses Rekam Medis Elektronik. *SOEPRA*, *10*(1).

Indriyajati, F., Jawa, M. M. S. D., & Utomo, H. (2023). Analisis Keamanan Data Electronic Medical Record Digital Transformation Office (DTO) Kementerian Kesehatan Indonesia. *Sanskara Manajemen Dan Bisnis*, *2*(01).

Izza, A. A., & Lailiyah, S. (2024). Kajian Literatur: Gambaran Implementasi Rekam Medis Elektronik di Rumah Sakit Indonesia berdasarkan Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis. *Media Gizi Kesmas*, *13*(1).

Mardiana, N., Pd, M. A. S., & Pd, M. (2023). *Urgensi Perlindungan Data Pribadi dalam Perspektif Hak Asasi Manusia*. *1*.

Naurah, G., Simarmata, M., & Sidi Jambak, R. (2024). Hak dan Privasi Pasien Rumah Sakit di Era Digitalisasi. *COMSERVA : Jurnal Penelitian Dan Pengabdian Masyarakat*, *3*(12).

Ningtyas, A. M., & Lubis, I. K. (2018). Literatur Review Permasalahan Privasi Pada Rekam Medis Elektronik. *Pseudocode*, *5*(2).

Pb, A. P., & Sutabri, T. (2024). Analisis Keamanan Aplikasi Rekam Medis Elektronik Mengunakan Metode Penetration Testing pada UPTD RSD Besemah. *Router : Jurnal Teknik Informatika dan Terapan*, *2*(4).

Ramadhian, E. A., Bachtiar, A., Oktamianti, P., & Candi, C. (2024). Perilaku Kesadaran Keamanan Sistem Informasi Pada Sumber Daya Manusia Kesehatan di Layanan Kesehatan – Narrative Literrature Review. *Syntax Idea*, *6*(7).

Rosyada, A., Lazuardi, L., & Kusrini, K. (2017). Persepsi Petugas Kesehatan Terhadap Peran Rekam Medis Elektronik Sebagai Pendukung Manajemen Pelayanan Pasien Di Rumah Sakit Panti Rapih. *Journal of Information Systems for Public Health*, *2*(1).

Rubiyanti, N. S. (2023). Penerapan Rekam Medis Elektronik di Rumah Sakit di Indonesia: Kajian Yuridis. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *1*(1).

Setiawan, D. P. (2024). Penyalahgunaan Data Pribadi Pasien Dalam Rekam Medis Oleh Tenaga Medis/Tenaga Kesehatan Rumah Sakit. *Yayasan Daarul Huda Krueng Mane*, *2*(4).

Wahyuntara, J. K., Wahyati, E., & Tugasworo, D. (2024). Pelindungan Hak atas Rahasia Medis Pasien dalam Implementasi Rekam Medis Elektronik (Studi pada Rumah Sakit Bhayangkara, Semarang). *SOEPRA*, *10*(1).

Yunisca, F., Chalimah, E., & Sitanggang, L. O. A. (2022). Implementasi Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis Terhadap Hasil Pemantauan Kesehatan Pekerja Radiasi di Kawasan Nuklir Serpong. *Reaktor : Buletin Pengelolaan Reaktor Nuklir*, *19*(2).