Journal of International Islamic Law, Human Right and Public Policy
(JISHUP Journal) | ISSN (e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volumes 4 No. 2 (2026)

ELECTRONIC MEDICAL RECORD DATA PROTECTION IN DIGITAL HEALTH SERVICES

Helviana Hasibuan[1], Rahmayanti[2], Poltak Marusaha Tambunan[3]
[1,2,3]Universitas Pembangunan Panca Budi, Medan
Correspondebce Email:rahmayanti@dosen.pancabudi.ac.id

Received: 02/03/2026 | **Revised:** 11/03/2026 | **Accepted:** 01/04/2026 | **Published:** 06/05/2026

Abstract

Digital transformation in the healthcare sector is driving the adoption of electronic medical records as an effort to improve efficiency, service quality, and patient data integration. However, this digitalization also poses risks to the protection of sensitive patient personal data, such as potential data leaks, information misuse, and privacy violations. This study aims to analyze the legal protection provisions for electronic medical records and assess the effectiveness of law enforcement in digital healthcare services in Indonesia. The research method used is normative juridical with a statutory and conceptual approach. The legal materials consist of laws and regulations, scientific literature, and previous research results, which are analyzed qualitatively using descriptive-prescriptive methods. The research results show that, normatively, the protection of electronic medical records is regulated through the Personal Data Protection Law and sectoral regulations in the health sector, which emphasize the principles of confidentiality, security, and accountability of patient data. However, regulatory harmonization remains problematic, particularly regarding the division of legal responsibilities and cross-system data management mechanisms. Furthermore, the effectiveness of law enforcement remains suboptimal due to weak oversight, limited institutional capacity, low legal awareness, and uneven distribution of technological infrastructure. In conclusion, the protection of electronic medical records requires strengthening through regulatory harmonization, increased law enforcement capacity, and enhanced security systems and digital literacy. These efforts are crucial to ensure the protection of patient privacy rights while supporting the development of secure and reliable digital healthcare services.

Keywords: Electronic Medical Records, Personal Data Protection, Privacy, Law Enforcement, Digital Health.

INTRODUCTION

Digital transformation in the healthcare sector is a logical consequence of the increasingly rapid development of information technology. The digitalization of healthcare services aims not only to improve efficiency and quality of service but also to expand public access to faster and more integrated healthcare services. One concrete manifestation of this transformation is the implementation of electronic medical records (EMR) as a replacement for conventional paper-based medical records. Electronic medical records enable the systematic storage, processing, and distribution of patient data in an integrated digital system across healthcare facilities. This aligns with the Indonesian government's policy mandating the implementation of electronic medical records through Minister of Health Regulation Number 24 of 2022 as part of strengthening the national digital-based healthcare system.

On the one hand, the implementation of electronic medical records offers various strategic benefits, such as improved service quality, accelerated medical decision-making, and efficiency in operational time and costs. Empirical studies have shown that the use of electronic medical records can improve the quality of healthcare services and patient safety through faster and more accurate data access. However, on the other hand, the digitization of health data also raises new legal issues, particularly regarding the protection of highly sensitive patient personal data. Medical record data contains not only patient identity but also medical history, diagnoses, medical procedures, and even financial information. Misuse can lead to serious harm, such as identity theft, discrimination, and data misuse for commercial or criminal purposes.

Vulnerability to data breaches in electronic medical record systems is becoming an increasingly relevant issue in the era of digital healthcare. Various studies have shown that the risk of data breaches can arise from both technical and non-technical factors, such as security system weaknesses, human error, and cyberattacks by external parties. Furthermore, the implementation of electronic medical records without adequate security standards has the potential to increase the risk of patient privacy breaches. In this context, data security is not only related to technological aspects, but also concerns governance, professional ethics, and compliance with applicable regulations.

Normatively, Indonesia already has a legal framework governing the protection of personal data, including health data, through Law Number 27 of 2022 concerning Personal Data Protection, as well as various sectoral regulations in the health sector. Furthermore, technical provisions regarding electronic medical records are stipulated in the Minister of Health Regulation, which requires healthcare facilities to ensure the security, confidentiality, and integrity of patient data. This regulation even requires the use of security mechanisms such as encryption to protect electronic medical records from unauthorized access. However, these regulations are not yet fully capable of ensuring optimal patient data protection.

The main problem lies in the suboptimal harmonization of personal data protection regulations with sectoral regulations in the health sector. Some provisions remain partial and have not been comprehensively integrated, potentially creating legal uncertainty in their implementation. Furthermore, there is a dilemma between the need for data access for healthcare purposes and the obligation to maintain patient data confidentiality. In practice, the obligation to provide data access for specific purposes, such as national system integration, has the potential to conflict with patients' right to privacy, a fundamental human right.

Furthermore, the effectiveness of law enforcement against electronic medical record data breaches remains a crucial issue. Several studies have shown that despite the existence of a regulatory framework, implementation in the field still faces various obstacles, such as limited human resources, weak oversight systems, and the absence of a firm and consistent law enforcement mechanism for personal data breaches in the healthcare sector. This has resulted in low levels of compliance and an increased potential for violations that could harm patients as data subjects.

Furthermore, the effectiveness of legal protection is also related to the readiness of technological infrastructure and institutional capacity to securely manage electronic medical records systems. Research shows that implementing security systems such as access control, user authentication, and training for healthcare workers are crucial factors in preventing data breaches. However, the implementation of these measures remains uneven across healthcare facilities, particularly in those with limited resources.

Thus, it is understandable that protecting electronic medical records in digital healthcare is a complex issue, as it involves the interaction of legal, technological, and institutional governance aspects. On the one hand, the state has an obligation to guarantee the right to health through the use of digital technology, but on the other hand, it must also ensure optimal protection of patients' privacy and personal data. An imbalance between these two interests has the potential to create risks of human rights violations and undermine public trust in the digital healthcare system.

Based on this description, it is important to conduct a comprehensive study of the legal regulations and the effectiveness of law enforcement in protecting electronic medical records in Indonesia. This study is not only academically relevant but also has practical urgency in supporting the formulation of policies that are more adaptive and responsive to developments in digital health technology. Based on this background, the research questions are formulated as follows: How are the legal regulations for protecting electronic medical records in the digital health care system in Indonesia? How effective is law enforcement in dealing with violations of electronic medical records protection in digital health care?

LITERATURE REVIEW

1. Electronic Medical Record Data Protection in Digital Health Services

Advances in information technology have driven the transformation of healthcare systems toward digitalization, one example of which is the implementation of electronic medical records (EMR). Various studies have shown that EMRs are a key foundation for modernizing healthcare services, improving the efficiency of patient data management, the accuracy of medical information, and the quality of clinical decision-making.

However, the digitization of medical records also poses serious consequences for the protection of patients' personal data. Health data is a sensitive category containing identity information, medical history, and even medical procedures, thus posing a high risk of leakage or misuse. The literature shows that the significant increase in the use of health information systems is directly proportional to increasing challenges related to data privacy and security.

2. Implementation of Electronic Medical Records in Health Services

Previous research has shown that EMR implementation in Indonesia is part of a national strategy to improve the effectiveness of healthcare services. This system enables digital, real-time integration of patient data, reducing administrative errors and improving hospital operational efficiency. However, EMR implementation is not without challenges, such as limited technological infrastructure, human resource readiness, and organizational culture in health data management. Empirical studies also show that recording culture and institutional readiness are critical factors in the success of EMR implementation in Indonesia.

3. Electronic Medical Record Data Security and Privacy Issues

Security and privacy are central issues in electronic medical records management. Literature shows that EMR systems are at high risk of data breaches due to cyberattacks, security weaknesses, and human error. Therefore, data protection is a top priority in implementing these systems. Other literature studies confirm that privacy protection in EMRs requires the implementation of robust security technologies, such as data encryption, access controls, and regular system audits. Without adequate security systems, patient data is vulnerable to unauthorized access, potentially leading to legal and social harm to patients. Furthermore, recent studies have shown that technological developments such as blockchain and artificial intelligence are beginning to be used to improve data security and integrity in EMR systems. These technologies are considered capable of strengthening transparency, access control, and protecting against data manipulation in digital health systems.

4. Principles of Personal Data Protection in Digital Health Systems

Global literature emphasizes that health data protection must be based on personal data protection principles, such as lawful processing, purpose limitation, data minimization, and confidentiality and accountability. These principles have become the standard for patient data management in the digital age. In the context of EMR, patients, as data subjects, have the right to control the use of their personal data, including the right to consent, access, and restrictions on data use. Therefore, managing electronic medical records involves not only technological aspects but also legal and ethical aspects in maintaining patient privacy rights.

5. Research Challenges and Gaps

Although various studies have discussed the implementation and benefits of EMR, there are still research gaps in several important aspects, namely:

a. The integration between legal, technological, and governance aspects in protecting electronic medical record data is not yet optimal.
b. Limitations of studies that specifically analyze the effectiveness of law enforcement against health data breaches in Indonesia.
c. There is a lack of research examining the harmonization between personal data protection regulations and health sectoral regulations in the context of digital services.

Furthermore, research also shows that the biggest challenge is not only the availability of technology, but also the implementation of security systems and regulatory compliance, which are still uneven across healthcare facilities.

METHOD

This research uses a normative juridical approach that focuses on analyzing the legal norms governing the protection of electronic medical records in digital healthcare services in Indonesia. This approach was chosen because the research aims to assess the suitability, synchronization, and effectiveness of applicable legal regulations, particularly in relation to the protection of patient personal data as part of the right to privacy. Furthermore, this research also uses a conceptual approach and a statutory approach to understand the legal principles underlying data protection and to examine various relevant regulations.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations relating to the protection of personal data and electronic medical records, including Law Number 27 of 2022 concerning Personal Data Protection, Law Number 17 of 2023 concerning Health, and Minister of Health Regulation Number 24 of 2022 concerning Medical Records. Secondary legal materials were obtained from peer-reviewed scientific journal articles, legal textbooks, and relevant previous research results within the last five years. Meanwhile, tertiary legal materials include legal dictionaries, encyclopedias, and other sources that support the conceptual understanding in this study. The legal data collection technique was conducted through library research, exploring valid and verifiable scientific sources, both through national and international journal databases. The literature was selected selectively, considering the relevance, credibility, and novelty of the sources, thus supporting a comprehensive and up-to-date analysis. The research also considered empirical findings reported

in various studies related to the implementation of electronic medical records and patient data protection to strengthen the normative analysis. The legal analysis technique used in this study employed a qualitative analysis method with a descriptive-analytical and prescriptive approach. Descriptive analysis was used to systematically describe the applicable legal regulations regarding electronic medical record data protection. Furthermore, an evaluative analysis was conducted to assess the suitability and effectiveness of these regulations in practice. A prescriptive approach was used to provide legal arguments and recommendations regarding identified issues, particularly with regard to strengthening legal protection and the effectiveness of law enforcement in the digital health sector.

To address the research problem, this study examines two main aspects: legal regulation and law enforcement. The analysis of the legal regulation aspect focuses on the harmonization of personal data protection regulations and sectoral regulations in the health sector. Meanwhile, the analysis of the law enforcement aspect focuses on the effectiveness of legal norm implementation, including oversight mechanisms, sanctions, and factors influencing compliance with electronic medical record data protection. By using this method, the research is expected to be able to provide a comprehensive, systematic, and argumentative analysis of the protection of electronic medical record data in digital health services, as well as produce relevant recommendations for legal development in Indonesia.

RESULTS AND DISCUSSION

1. Legal Protection Regulations for Electronic Medical Record Data in the Digital Health Service System in Indonesia

The legal protection of electronic medical records in Indonesia essentially has a fairly comprehensive normative foundation, both through the personal data protection regime and sectoral regulations in the health sector. Generally, this protection is based on the principle that health data is a specific and sensitive form of personal data, requiring a higher standard of protection than other personal data.

Within the national legal framework, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is the primary instrument governing data protection principles, such as data subject consent, limitations on processing purposes, data security, and data controller accountability. In the context of electronic medical records, patients are considered data subjects with the right to information, access, and control over the use of their personal data. This aligns with personal data protection theory, which emphasizes the importance of individual control over their data (Pramesti et al., 2024).

On the other hand, sectoral regulations, through Minister of Health Regulation Number 24 of 2022 concerning Medical Records, specifically govern the implementation of electronic medical records, including the obligation of healthcare facilities to maintain the confidentiality, integrity, and availability of patient data. This regulation also requires the use of security systems such as access authentication and user activity recording (audit trails) to prevent unauthorized access. Furthermore, Law Number 17 of 2023 concerning Health emphasizes the obligation of healthcare workers and healthcare facilities to maintain the confidentiality of patient data as part of their professional ethics and legal responsibilities.

Although these regulations normatively reflect adequate legal protection principles, research shows that regulatory harmonization remains problematic. Several provisions in the PDP Law and sectoral health regulations have not been fully integrated systematically, potentially leading to multiple interpretations during implementation. For example, there is tension between the principle of patient data confidentiality and the need for data integration within the national health system, which requires data exchange between health facilities (Indra et al., 2024).

Furthermore, regulations regarding legal liability in the event of data breaches remain largely unresolved within the health sector. The PDP Law does provide for administrative and criminal sanctions for personal data breaches, but it does not specifically address liability in electronic medical records systems, which involve various parties, such as system providers, healthcare workers, and healthcare institutions. This indicates a legal gap that could potentially hamper the effectiveness of legal protection.

From a legal protection theory perspective, this situation indicates that preventive legal protection has developed sufficiently through various existing regulations, but repressive legal protection still requires strengthening, particularly in terms of clarity of accountability mechanisms and sanctions. Therefore, it can be concluded that the legal protection provisions for electronic medical records in Indonesia are well-founded, but still require harmonization and strengthening of the legal substance to provide optimal protection.

2. Effectiveness of Law Enforcement against Electronic Medical Record Data Protection Violations in Digital Health Services

The effectiveness of law enforcement regarding electronic medical record data protection is a crucial aspect that determines the extent to which established legal norms can be implemented in practice. In the context of digital healthcare, law enforcement depends not only on the existence of regulations but also on institutional readiness, human resource capacity, and the prevailing legal culture within the community.

Empirically, various studies have shown that the effectiveness of law enforcement against personal data breaches in the healthcare sector remains relatively low. This is due to several key factors, including limited oversight, a lack of legal awareness among healthcare workers, and suboptimal mechanisms for reporting and handling data breach cases (We'e, 2023). In many cases, data breaches go unreported or are not seriously pursued, thus failing to deter perpetrators.

In terms of legal structure, the institutions responsible for overseeing and enforcing personal data protection laws are still being strengthened. Coordination between institutions, such as the Ministry of Health and data protection authorities, is also not yet fully effective. This has resulted in weak oversight of the implementation of electronic medical records in various healthcare facilities, particularly in areas with limited resources.

Furthermore, technological factors also pose challenges to law enforcement. Not all healthcare facilities have adequate security systems to protect electronic medical records. Research shows that some facilities still lack security standards such as data encryption, role-based access control, and adequate audit systems (Siregar & Sinaga, 2025). This situation increases the risk of data breaches and complicates the process of establishing evidence in law enforcement.

From a legal culture perspective, awareness of the importance of personal data protection remains relatively low, both among healthcare professionals and the public. In some cases, data breaches occur due to negligence or a lack of understanding of data protection standards. This demonstrates that law enforcement requires not only a repressive approach but also an educational approach to increase awareness and compliance.

When analyzed using law enforcement theory, it can be seen that the three main elements—legal substance, legal structure, and legal culture—have not been functioning optimally and supporting each other. Legal substance that is not yet fully harmonized, legal structure that is still being strengthened, and an immature legal culture are the main factors hampering the effectiveness of law enforcement.

Thus, the effectiveness of law enforcement against violations of electronic medical record data protection in Indonesia still faces various multidimensional obstacles. Therefore, comprehensive efforts are needed, including strengthening regulations, increasing institutional capacity, and raising public legal awareness, to optimally protect patient data in digital healthcare.

CONCLUSION

Based on the results and discussion, it can be concluded that the legal protection of electronic medical records in digital healthcare services in Indonesia is normatively well-founded through the personal data protection regime and sectoral regulations in the health sector. The existence of the Personal Data Protection Law and the Minister of Health Regulation on medical records demonstrate the state's commitment to ensuring the security and confidentiality of patient data. However, these regulations still face challenges in terms of harmonization and synchronization between regulations, particularly regarding the division of legal responsibilities, cross-system data management mechanisms, and the balance between the need for data access for healthcare services and the protection of patient privacy rights. This condition indicates that, in terms of legal substance, the protection of electronic medical records still requires strengthening to be more comprehensive and to prevent multiple interpretations in its implementation.

On the other hand, the effectiveness of law enforcement against violations of electronic medical record data protection remains suboptimal. This is influenced by various factors, including weak oversight, limited capacity of law enforcement institutions, suboptimal coordination between institutions, and low legal awareness among healthcare workers and health information system administrators. Furthermore, the uneven readiness of technological infrastructure contributes to the increased risk of data breaches and complicates the law enforcement process. Thus, it is understandable that the problem of electronic medical record data protection lies not only in the regulatory aspect, but also in the implementation aspect, which involves legal structures and culture., In line with these findings, strategic steps are needed to strengthen the protection of electronic medical records in digital healthcare services. First, the government needs to harmonize and synchronize regulations between the Personal Data Protection Law and sectoral regulations in the health sector, particularly by clarifying the division of legal

responsibilities and data protection mechanisms within an integrated system. Second, law enforcement must be strengthened by increasing the capacity of supervisory institutions, establishing more effective oversight mechanisms, and implementing firm and consistent sanctions for personal data breaches. Third, increasing legal awareness and digital literacy among healthcare workers and the public is crucial to encourage compliance with data protection principles. Fourth, strengthening the technological infrastructure and security standards of electronic medical records systems needs to be implemented evenly across all healthcare facilities. Thus, efforts to protect electronic medical records must be carried out comprehensively through regulatory, institutional, and cultural approaches to ensure the protection of patients' privacy rights while supporting the development of safe, reliable, and sustainable digital health services in Indonesia.

REFERENCES

Buku

Asshiddiqie, J. (2021). Hukum tata negara dan pilar demokrasi. Jakarta: Konstitusi Press.
Marzuki, P. M. (2021). Penelitian hukum. Jakarta: Kencana.
Rahardjo, S. (2022). Ilmu hukum. Bandung: Citra Aditya Bakti.
Soekanto, S. (2021). Faktor-faktor yang mempengaruhi penegakan hukum. Jakarta: Raja Grafindo.
Widodo, J. (2023). Hukum perlindungan data pribadi. Jakarta: Prenadamedia.

Jurnal Ilmiah

Adelina Siregar, R., & Sinaga, H. S. R. (2025). Perlindungan data pasien dalam rekam medis elektronik. Jurnal Hukum To-Ra, 11(1), 106–116.
Ardianto, E. T. (2024). Analisis aspek keamanan data pasien dalam rekam medis elektronik. Jurnal Rekam Medis dan Informasi Kesehatan, 3(2).
Asih, H. A. (2023). Perkembangan rekam medis elektronik di Indonesia. Jurnal Penelitian Kesehatan, 5(2).
Ayuni, A. S., Ikawati, F. R., & Ansyori, A. (2025). Implementasi rekam medis elektronik di rumah sakit. Jurnal Kesehatan Amanah, 8(1), 224–231.
Cahyani, M. B. (2024). Peran rekam medis elektronik dalam pelayanan kesehatan. Jurnal Manajemen Informasi Kesehatan Indonesia.
Farid, Z. M., Fernando, N. R., & Sonia, D. (2021). Efektivitas penggunaan rekam medis elektronik terhadap pelayanan pasien. Cerdika: Jurnal Ilmiah Indonesia, 1(9), 1247–1254.
Fitrianingsih, D. D., et al. (2025). Implementasi digitalisasi rekam medis. Enfermeria Ciencia, 3(2), 100–112.
Indra, I., Dewi, T. N., & Wibowo, D. B. (2024). Konflik kerahasiaan data pasien dalam rekam medis elektronik. Soepra Jurnal Hukum Kesehatan, 10(1), 97–117.
Isnaeni, D. R. (2025). Evaluasi kesiapan implementasi rekam medis elektronik. Jurnal Infokes.
Khasanah, L., & Budiyanti, N. (2023). Kesiapan penerapan rekam medis elektronik. Jurnal Informasi Kesehatan Indonesia, 9(2), 192–201.
Kurniawan, A., Saryadi, S., & Arini, L. (2025). Dampak rekam medis elektronik terhadap mutu pelayanan. Jurnal Ilmiah Kedokteran dan Kesehatan, 4(2), 596–610.
Meilani, A. H. (2025). Analisis implementasi rekam medis elektronik. Jurnal Infokes.
Mirsanda, M., et al. (2025). Kepuasan pengguna rekam medis elektronik. Jurnal Keperawatan, 13(2), 235–246.
Nasir, A. F., & Pranoto, E. (2025). Perlindungan hukum data pribadi pasien. Fiat Iustitia.
Pramesti, D. P. A., et al. (2024). Keamanan data medis pasien. Jurnal Kesehatan Masyarakat.
Putri, A., & Kurniawan, I. (2022). Integrasi sistem rekam medis elektronik. Jurnal Kebijakan Kesehatan Indonesia.
Rahman, F., et al. (2022). Rekam medis elektronik dan keputusan medis. Jurnal Pelayanan Kesehatan.
Rubiyanti, N. S. (2023). Kajian yuridis rekam medis elektronik. Jurnal Hukum.
Santosa, B., & Dewi, R. (2022). Tantangan implementasi rekam medis elektronik. Jurnal Teknologi Rumah Sakit.
Setyawan, D., & Nugroho, H. (2021). Sistem informasi rekam medis elektronik. Jurnal Administrasi Kesehatan.
Sidiq, M. A. (2025). Penegakan hukum perlindungan data kesehatan. Jurnal Hukum.
Tombokan, C. D. (2024). Perlindungan privasi data pasien. Lex Privatum.
We'e, A. (2023). Evaluasi keamanan rekam medis elektronik. Jurnal Permata Indonesia.

Peraturan Perundang-Undangan
Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 tentang Kesehatan.
Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis.