

Patient Data Protection Compliance Model in Electronic Medical Record Systems Following the Implementation of the Personal Data Protection Law in Indonesia

Elsy Nur Anggraeni¹, Dey Ravena², Aslan Noor³
anggraenielsy@gmail.com¹, dey@unisba.ac.id², aslan.noor@fh.unsika.ac.id³

^{1,2}Universitas Islam Bandung, Indonesia

³Universitas Singaperbangsa Karawang, Indonesia

Article Info

Received: 05-03-2026

Revised: 13-02-2026

Accepted: 24-06-2026

Keywords:

Electronic Medical Records, Personal Data Protection, Legal Compliance, GDPR, HIPAA.

Abstract

The implementation of Electronic Medical Records (EMR) in Indonesia has undergone significant development with the enactment of Minister of Health Regulation No. 24 of 2022. However, the main challenge in implementing EMR is the protection of patient personal data, which remains suboptimal. This study aims to analyse the management of personal data in the EMR system in Indonesia, compare national regulations with international standards, and formulate a compliance model that can improve the protection of patients' personal data. The method employed in this study is a normative juridical approach, which examines legislation, legal documents, and compares them with international standards, such as the GDPR and HIPAA. The results of the study indicate that, despite Indonesia's existing strong regulations on personal data protection, significant gaps remain in medical data management, particularly in areas such as audit trails, data security, and law enforcement. This study proposes a compliance model that incorporates the implementation of strict audit trails, enhanced data security through encryption, and more stringent law enforcement to ensure compliance with applicable regulations. In conclusion, collaboration among the government, the private sector, and healthcare facilities is essential to enhance the implementation of secure Electronic Medical Records that comply with Indonesia's personal data protection regulations.

I. Introduction

The development of digital technology has brought about significant changes in various sectors, particularly in the healthcare sector. One of the important changes that has occurred is the implementation of Electronic Medical Records (EMR), which replaces manual medical record systems with digital-based systems. EMR enables more efficient storage, management, and exchange of patient data, which is expected to improve the quality of health services, reduce examination redundancy, and facilitate cross-system data integration. In Indonesia, the implementation of EMR is being further encouraged by the enactment of Minister of Health Regulation No. 24 of 2022, which requires all healthcare facilities to switch from manual to electronic medical record systems (Izza & Lailiyah, 2024). However, despite promising efficiency, the implementation of EMR also poses significant challenges, particularly regarding patient data security and privacy (Hossain et al., 2025).

The protection of personal data in the EMR system is a significant issue that needs to be addressed, as medical data is highly sensitive information and directly related to patients' personal rights and autonomy. Based on research by Lestari et al. (2024), although Indonesia has passed Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), the application of personal data protection principles in EMR still faces various obstacles. Limitations in infrastructure and human resources (HR) in many healthcare facilities are the primary obstacles to maintaining the security and confidentiality of patient data (Hossain et al., 2025). This indicates that, despite regulations being in place, their implementation in the field still falls short of expectations.

The main challenge faced by Indonesia in implementing RME is the incompatibility of personal data protection regulations with international standards such as those applied in the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Although the PDP Law provides a clear legal basis, the management of patient personal data in RME still heavily depends on the internal policies of each healthcare facility. According to Indra, Dewi, and Wibowo (2024), varying policies across hospitals and clinics result in inconsistencies in data security and audit trails, which are crucial elements in maintaining transparency and accountability in medical data access.

Furthermore, despite regulations governing the protection of personal data, law enforcement in the health sector remains weak. Rohman (2020) points out that, although the PDP Law includes administrative sanctions, the inconsistent implementation of these sanctions and minimal supervision leave the door open

to data breaches that can harm patients. This raises an important question: How can an effective compliance model be adopted to ensure the security and confidentiality of patient data in the implementation of EMR in Indonesia?

This study aims to develop a compliance model for implementing Electronic Medical Records (EMR) that can assist health facilities in Indonesia in fulfilling their obligations to protect patients' personal data and enhance the implementation of existing regulations. This model will integrate national regulations with international standards, such as the GDPR and HIPAA, and introduce more effective mechanisms for audit trails, data security, and law enforcement. The specific objectives of this study include identifying gaps in the management of patient personal data between Indonesian regulations and international standards, designing an applicable compliance model for the implementation of EMR in Indonesia, and analysing the challenges of EMR implementation in the context of infrastructure, human resources, and existing regulations in Indonesia.

The uniqueness of this study lies in its approach, which combines legal regulations with a technical approach to managing Electronic Medical Records. This study not only examines applicable regulations but also designs a compliance model that can be applied in the field, particularly in Indonesia. Unlike previous studies, which focused more on the technical or ethical aspects of EMR use, this study focuses on the synergy between legal regulations and more effective operational procedures, as well as stricter law enforcement to ensure the security of patients' personal data. This study also provides a theoretical and practical framework for health facilities to comply with personal data protection regulations in a more systematic and structured manner.

2. Research Method

This study employs a normative juridical method, focusing on the analysis of legislation, legal documents, court decisions, and relevant academic literature related to the research topic. This approach was chosen because the main objective of the study is to identify, analyse, and construct an applicable legal compliance model related to personal data protection in the Electronic Medical Record (EMR) system in Indonesia. The normative juridical method enables researchers to examine the legal norms applicable in Indonesia and connect them to international principles related to the protection of patients' personal data, as outlined in the literature on legal methodology (Marzuki, 2019).

This type of research is descriptive and analytical, aiming to describe and analyse existing regulations and formulate a legal compliance model that can be

applied in the operational practices of health facilities in Indonesia. This study also aims to identify gaps between existing national regulations in Indonesia and international principles on the protection of personal data. By comparing existing regulations in Indonesia with global regulations, such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and guidelines from the Organisation for Economic Co-operation and Development (OECD) on privacy protection and cross-border personal data flows, this study seeks to assess the extent to which Indonesian regulations have adopted and implemented international standards in the protection of patient personal data (Indra, Dewi, & Wibowo, 2024).

The data sources in this study comprise two main types of legal materials: primary legal materials and secondary legal materials. Primary legal materials include Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), Law No. 36 of 2009 concerning Health, and Law No. 29 of 2004 concerning Medical Practice. Additionally, primary legal materials include related regulations, such as Minister of Health Regulation No. 24 of 2022, which governs the implementation of RME in Indonesian health facilities. Furthermore, primary legal materials also include international standards related to personal data protection, such as the GDPR, HIPAA, and OECD guidelines on privacy protection and cross-border personal data flows. These sources will provide a strong legal basis for comparing Indonesian regulations with international practices that have proven effective in protecting patient privacy and personal data (Kusumah, 2021; Darmadi, 2023).

The secondary legal materials used in this study comprise scientific journals, articles, books, and other relevant academic publications. The literature used in this study was selected from various academic databases, including Google Scholar, PubMed, and arXiv, with a focus on works published between 2020 and 2025. The selection of current literature aims to ensure that the sources used reflect the latest developments in the field of health law and information technology, as well as align with current issues affecting the regulation of personal data protection in the context of the digitization of health services (Rohman, 2020).

The analysis method employed in this study is qualitative, conducted in three main stages. The first stage involves identifying legal norms, which is achieved by reviewing the regulations in force in Indonesia and international principles relevant to the protection of patients' personal data. In the second stage, a comparison was made between national regulations and international principles to identify any gaps or inconsistencies that might arise, as well as to assess the extent to which Indonesian regulations align with international standards. The third stage involved

constructing a compliance model based on the interpretation of the legal norms identified and analyzed in the previous stage. This model is designed to help healthcare facilities comply with applicable legal obligations and protect patients' personal data more effectively in their operational practices.

To maintain the validity of this study, document triangulation techniques were used to compare and confirm information obtained from various relevant sources. In addition, this study also maintained logical consistency between sources to ensure that the conclusions drawn were valid and accountable. This analysis process involves an in-depth evaluation of legal interpretations and their application in the field to produce a compliance model that is not only theoretical but also applicable and in line with the practical needs of healthcare facilities in Indonesia (Marzuki, 2019; Darmadi, 2023).

3. Results and Discussion

Results

This study identified several important findings related to personal data management in Electronic Medical Records (EMR) in Indonesia, based on an analysis of applicable regulations and their comparison with international principles. The main findings of this study are presented in three stages of analysis: the identification of legal norms, the comparison of national and international regulations, and the development of a compliance model.

Identification of Legal Norms

The first stage of this study involved identifying the legal norms applicable in Indonesia, particularly in terms of patient personal data protection. Based on an analysis of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), Minister of Health Regulation No. 24 of 2022 concerning Electronic Medical Records, and Law No. 36 of 2009 concerning Health, it was found that Indonesia already has a relatively strong legal framework for regulating the protection of patients' personal data. The PDP Law provides a clear legal basis regarding individuals' rights to their personal data, and Minister of Health Regulation No. 24 of 2022 regulates in detail the mechanism for managing Electronic Medical Records (EMR) in health facilities.

However, despite these regulations, their implementation in practice still faces various challenges. One of these is the secure management of data in accordance with the principles of transparency, data security, and lawful access. For example, although there is an obligation to protect patients' personal data, the regulations do not contain sufficiently detailed provisions on audit trails, which are a key principle of the General Data Protection Regulation (GDPR) and other international

standards. Audit trails are an important mechanism for monitoring every interaction with personal data, including who accessed the data, when, and for what purpose, to ensure transparency and accountability.

Comparison of National and International Regulations

The second stage of this study was a comparison between national regulations and international principles related to personal data protection. Based on a comparison between the PDP Law, Minister of Health Regulation No. 24 of 2022, and the GDPR, several significant discrepancies were found in the management of patients' personal data.

The GDPR clearly stipulates that every organisation that manages personal data must maintain an audit trail that records every transaction involving access to data, including who accessed it and for what purpose. This is important to ensure transparency and accountability in data management. In contrast, Minister of Health Regulation No. 24 of 2022, although it covers data security management, does not provide explicit provisions regarding the obligation of an audit trail for each data access. This shows a gap between national and international regulations in terms of data access tracking and monitoring mechanisms.

A further comparison with the Health Insurance Portability and Accountability Act (HIPAA), implemented in the United States, also reveals substantial differences in terms of access control and data security. HIPAA requires healthcare facilities to use encryption systems and provide limited access to authorised parties. However, even though the PDP Law in Indonesia regulates data protection, the implementation of data security in many healthcare facilities still depends heavily on the technical capabilities of each facility, resulting in inconsistencies in the management of patient medical data.

Compliance Model Construction

The third stage of this research involves constructing a compliance model, which aims to formulate an operational framework that enables healthcare facilities in Indonesia to comply with applicable legal obligations and protect patients' personal data more effectively. Based on the findings from the first and second stages, the proposed compliance model consists of several important elements, as follows:

1. **Audit Trail:** This compliance model proposes that every healthcare facility implement a system that can record every access to patient personal data. This will ensure that every data transaction can be tracked and accounted for, as stipulated in the GDPR and HIPAA. The implementation of a strict audit trail will enable authorities to identify suspicious activity or unauthorised access to

patient personal data, as well as provide a clear legal basis in the event of data leaks or misuse.

2. **Data Security:** This model emphasises the need for healthcare facilities to implement data encryption systems and stricter access controls. All access to Electronic Medical Records (EMRs) must be restricted to authorised parties, with access rights clearly defined according to the duties and responsibilities of each party within the healthcare facility. This measure will enhance the protection of patients' personal data and prevent unauthorised access.
3. **Education and Training:** Healthcare facilities must have regular training programs for medical and administrative staff on the secure management of patient personal data. These training programmes aim to increase medical staff's awareness and knowledge of the importance of data confidentiality and the security protocols that must be followed. This training will also reduce operational errors and ensure that security procedures are consistently implemented throughout the healthcare facility.
4. **Law Enforcement and Sanctions:** This model also proposes stricter law enforcement against healthcare facilities that violate provisions related to the protection of personal data. Administrative sanctions and substantial fines should be imposed on facilities that fail to implement personal data protection regulations properly. Clear and firm law enforcement will increase accountability and transparency in the management of patient personal data, as well as strengthen public trust in Indonesia's digital healthcare system.

This study reveals that, although Indonesia has fairly strong regulations in place for patient personal data protection through the PDP Law and Minister of Health Regulation No. 24 of 2022, several significant gaps remain in relation to international standards, particularly in terms of audit trails, data security, and law enforcement. Therefore, this study develops a compliance model that integrates international principles, such as the GDPR and HIPAA, to ensure the effective and safe implementation of Electronic Medical Records in Indonesia. This model incorporates concrete steps, including audit trails, data security measures, training for medical personnel, and stricter law enforcement, which are expected to enhance the protection of patients' personal data and foster public trust in Indonesia's digital health system.

Discussion

Limitations of Infrastructure and Human Resources (HR)

This study found that limitations in infrastructure and human resources in most Indonesian healthcare facilities are a significant obstacle to the implementation of Electronic Medical Records (EMR). Many hospitals, especially small ones and those

in remote areas, find it challenging to provide adequate hardware and networks to support the optimal implementation of EMR. Furthermore, the lack of training for medical personnel in managing electronic medical data exacerbates this situation.

This finding aligns with research by Lestari et al. (2024), which indicates that limitations in digital infrastructure and inadequate human resource training are significant obstacles to the adoption of digital health technology in Indonesia. Hossain et al. (2025) also note that the lack of training for medical personnel on data security protocols causes uncertainty in the management of patient personal data, which ultimately increases the risk of data leaks. In developed countries, the implementation of Electronic Medical Records is supported by adequate technological infrastructure and continuous training for medical personnel, which makes medical data management more efficient and secure. Therefore, strengthening infrastructure and training medical personnel in Indonesia is a crucial step to improve the protection of patients' personal data.

Non-compliance with International Standards

This study found that although the PDP Law and Minister of Health Regulation No. 24 of 2022 regulate the protection of patients' personal data, Indonesian regulations are still not fully aligned with international standards, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). One of the main differences found is in terms of audit trails, where the GDPR requires every organisation that manages personal data to record every interaction with the data, including who accessed it and for what purpose, with complete transparency.

This finding confirms a significant gap between Indonesian regulations and international standards, as noted by Indra, Dewi, and Wibowo (2024), who point out that although Indonesia has a clear legal framework through the PDP Law, regulations related to audit trails are still lacking in detail. The GDPR outlines detailed obligations regarding audit trails, which not only document access to data but also ensure that every data transaction can be monitored and accounted for. In Indonesia, although Minister of Health Regulation No. 24 of 2022 addresses personal data management, implementing adequate audit trails and supervising data access remain significant challenges. Therefore, harmonization with international standards, such as the GDPR, is essential to strengthen transparency and security in the management of RME in Indonesia.

Weak Law Enforcement

Law enforcement in the personal data protection sector in Indonesia remains relatively weak. Although the PDP Law regulates administrative sanctions for

violations in personal data management, their implementation in the field remains limited. Security systems in many health facilities are also inadequate, and data breach reporting procedures are minimal.

This aligns with Rohman's (2020) findings, which state that law enforcement against violations related to patient personal data in Indonesia remains inadequate. The GDPR and HIPAA, on the other hand, impose more stringent sanctions, including substantial fines and even criminal penalties, which provide stronger protection for patients. In Indonesia, despite a strong legal basis, the implementation of supervision and enforcement of sanctions remains weak, leading to potential data leaks and undetected misuse of personal information. Therefore, stricter law enforcement and tighter supervision of RME implementation are necessary to increase public trust in Indonesia's digital health system.

Dependence on Internal Policies of Healthcare Facilities

This study reveals that one of the primary challenges in implementing Electronic Medical Records (EMR) in Indonesia is the reliance on internal policies of each health facility. Each hospital or clinic has different policies regarding the management of patients' personal data, resulting in inconsistencies in the management of medical data across healthcare facilities.

This inconsistency was also highlighted by Budiyaniti et al. (2023), who noted that reliance on these non-uniform internal policies exacerbates the challenges of managing patient personal data in Indonesia. Non-standard internal policies result in inconsistent data management, which often fails to comply with standard operating procedures (SOPs). Komalasari and Mustafa (2024) also emphasise that standardisation of policies at the national level is essential so that every healthcare facility can follow standard procedures in managing Electronic Medical Records. Therefore, there is a need for policy standardisation across all healthcare facilities to improve data accountability and security.

The Importance of Collaboration between the Government and the Private Sector

The findings of this study underline the importance of collaboration between the government and the private sector in overcoming the challenges of managing Electronic Medical Records (EMR). The government needs to strengthen supervision and law enforcement, as well as ensure that personal data protection regulations are consistently implemented in all health facilities. The private sector, especially healthcare technology providers, must also ensure that the EMR systems used meet high data security standards and that medical personnel receive ongoing training.

Collaboration between the public and private sectors is also emphasized by

Komalasari and Mustafa (2024), who state that the private sector plays a crucial role in providing safe and proven technology, as well as strengthening human resource capacity in healthcare facilities. The government, on the other hand, must be more active in providing funding, technical guidance, and support for healthcare facilities, especially those in areas with limited budgets. Siregar and Astuti (2025) also suggest that this effective collaboration will improve the management of patients' personal data and ensure that Electronic Medical Records (EMR) are implemented optimally, securely, and in accordance with applicable regulations.

Based on the results and discussions presented, although Indonesia has enacted fairly strong personal data protection regulations through the PDP Law and Minister of Health Regulation No. 24 of 2022, several obstacles remain to their practical implementation. Limited infrastructure, limited human resources, non-compliance with international standards, and weak law enforcement are the main challenges that must be addressed immediately. Collaboration among the government, the private sector, and healthcare facilities is crucial to ensure that patients' personal data is well-protected and that RME management can be implemented effectively and in accordance with applicable regulations. More vigorous law enforcement and stricter monitoring will increase public confidence in Indonesia's digital healthcare system.

4. Conclusion

This study analysed the implementation of Electronic Medical Records (EMR) in Indonesia, particularly in terms of protecting patients' personal data. The main findings of this study indicate that, despite Indonesia having strong regulations, such as the PDP Law and Minister of Health Regulation No. 24 of 2022, several significant challenges remain in their practical implementation. Limitations in technological infrastructure and human resources (HR) in health facilities are significant obstacles to the safe and effective implementation of EMR. Additionally, a gap exists between national regulations and international standards, such as the GDPR and HIPAA, which necessitate more detailed audit trail management and stringent access control for patient personal data. Weak law enforcement and reliance on the internal policies of each health facility also exacerbate the implementation of patient personal data protection.

The importance of collaboration between the government and the private sector is also a key finding of this study. The government must strengthen supervision and law enforcement, and ensure clear policy standardization across all healthcare facilities in Indonesia. The private sector, particularly healthcare technology providers, must ensure that the EHR systems implemented meet high data security standards and provide ongoing training for medical

personnel. This study suggests that to increase public trust in Indonesia's digital healthcare system, infrastructure needs to be strengthened, human resources need to be adequately trained, and law enforcement needs to be more rigorous and consistent.

Overall, this study demonstrates that although Indonesia has enacted robust personal data protection regulations, their implementation in the field still faces numerous challenges. Therefore, joint efforts from the government, private sector, and health facilities are needed to ensure that Electronic Medical Records can be implemented effectively, safely, and in accordance with applicable personal data protection regulations. This will not only strengthen patient data protection but also increase accountability and transparency in the management of digital health systems in Indonesia.

References

- Budiyanti, R. T., Herlambang, P. M., Fuad, A., & Kusumastuti, W. (2023). Integration of electronic medical record and SATUSEHAT's platform: Patient's legal protection perspective. *International Journal of Health Literacy and Science*, 1(2). <https://doi.org/10.60074/ihelis.v1i2.18>
- Darmadi, A. (2023). *Theory and Practice of Normative Legal Research*. Jakarta: Erlangga.
- Hossain, K., Sutanto, J., Handayani, P. W., Haryanto, A., Bhowmik, J., & Frings-Hessami, V. (2025). An exploratory study of electronic medical record implementation and record-keeping culture: The case of hospitals in Indonesia. *BMC Health Services Research*, 25, Article 249. <https://doi.org/10.1186/s12913-025-12399-0>
- Indonesia. (2022). Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection. LN 2022/No.196.
- Indonesia. (2009). Law of the Republic of Indonesia Number 36 of 2009 concerning Health. LN 2009/No.144.
- Indonesia. (2022). Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Electronic Medical Records. BN 2022/No.829.
- Indra, A., Dewi, S., & Wibowo, A. (2024). The legal implications of patient privacy violations in electronic medical records in Indonesia. *Journal of Health Policy and Legal Studies*, 8(1), 113-127.
- Izza, A., & Lailiyah, S. (2024). Literature review: Overview of the implementation of electronic medical records in Indonesian hospitals based on Minister of Health Regulation (Permenkes) No. 24/2022 concerning Medical Records. *Media Gizi Kesmas*, 13(1), 549-562.
- Juliansyah, R., Aqid, B. M., Salsabila, A. P., & Nurfiyanti, K. (2024). Implementation of EMR system in Indonesian health facilities: Benefits and constraints. ArXiv

- Preprint. <https://arxiv.org/abs/2410.12226>
- Lestari, A. Y., Misran, M., Raharjo, T., Annas, M., Riskanita, D., & Prabandari, A. P. (2024). Improving healthcare patient data security: An integrated framework model for electronic health records from a legal perspective. *Law Reform: Journal of Law and Policy*, 20(2). <https://doi.org/10.14710/lr.v20i2.56986>
- Komalasari, R., & Mustafa, C. (2024). Electronic health records in Indonesia: A law-, and policy analysis. *Jurnal Mahkamah Keadilan*, 2(1). <https://doi.org/10.15366/jmk.v2i1.311>
- Kusumah, H. (2021). *Legal Research Methodology*. Jakarta: Rajawali Pers.
- Marzuki, P. M. (2019). *Legal Research (Revised Edition)*. Jakarta: Kencana.
- Mishra, V., Gupta, K., Saxena, D., & Singh, A. K. (2024). A global medical data security and privacy-preserving standards identification framework for electronic healthcare consumers. *ArXiv Preprint*. <https://arxiv.org/abs/2410.03621>
- Rohman, R. (2020). Legal implications of patient data privacy in electronic health records: Challenges and opportunities in Indonesia. *Journal of Health Law*, 12(3), 67-84.
- Siregar, R. A., & Astuti, N. K. (2025). Assessing legal and institutional readiness for patient data protection in the age of big health data: An empirical study of health facilities in Indonesia. *International Journal of Law, Policy and Social Review*, 7(3), 15-21.