Jurnal Multidisiplin Sahombu
Volume 5, Number 02, 2025, DOI 10.58471/jms.v5i02
ESSN 2809-8587 (Online)
https://ejournal.seaninstitute.or.id/index.php/JMS/index

Legal Analysis of Patient Privacy Violation in Electronic Medical Records and its Implications for Health Data Protection in Indonesia

Aprilia Widya Mandey
Prodi Ilmu Hukum, Fakultas Hukum, Universitas Pembangunan Nasional Manado

Article Info
Keywords:
Patient privacy,
electronic medical record, data leakage,
legal protection,
health regulation

ABSTRACT

The development of information technology has brought about major changes in the healthcare system, including through the implementation of electronic health records (EHR). While this system provides efficiency in the storage and access of patient data, it also poses serious challenges regarding the protection of patient privacy. This study analyzes the legal protection of electronic medical records in Indonesia and evaluates the effectiveness of existing regulations in addressing patient data leakage. Using a normative approach, this study examines various laws and regulations such as the Personal Data Protection Law (PDP Law), the Health Law, and the Electronic Information and Transaction Law (ITE Law). The results show that although regulations are in place, implementation and law enforcement are still major obstacles in the protection of patient data. Challenges such as lack of security standards, low awareness of medical personnel, and weak supervision are barriers to effective implementation of privacy protection. Therefore, further efforts are needed to strengthen regulations, raise awareness, and implement better security technology in the management of electronic medical records in Indonesia. Thus, it is hoped that the electronic medical record system can provide optimal protection of patient privacy and increase public confidence in the digitization of health services.

Corresponding Author:
Aprilia Widya Mandey
Prodi Ilmu Hukum, Fakultas Hukum, Universitas Pembangunan Nasional Manado
widyamandey@gmail.com

INTRODUCTION

The development of information technology has brought about major transformations in various sectors, including in the health sector. One of the important innovations in the medical world is the use of electronic health records (EHR), which replaces manual paper-based recording systems. EHR allows for more efficient storage, access and exchange of patient data, ultimately improving the quality of healthcare(Angelyn et al., 2024; Fauzi et al., 2023; Kim et al., 2019) . However, behind these benefits, serious issues arise regarding the security and privacy of patient data .(Keshta & Odeh, 2021)

Violation of patient privacy in electronic medical records has become an issue that has received increasing attention, both at the national and global levels. Cases of health data leakage often occur due to system hacking, misuse by internal health facilities, and regulatory weaknesses in ensuring patient data protection(A. M. Ibrahim et al., 2024) . In Indonesia, this challenge is even more complex given the rapid digitization of the health sector without uniform security standards (Rahman et al., 2021). Several cases in Indonesia show how patient data can be accessed without authorization or even traded on the black market(Hoffman & Podgurski, 2022; Wallis et al., 2018) . This raises serious concerns regarding the implementation of legal protection of patient privacy in EHR systems.

Patient privacy is a fundamental right that must be protected, as stipulated in various international and national regulations. At the global level, the General Data Protection Regulation (GDPR) in the European Union strictly regulates the protection of personal data, including health data(Olorunfemi et al., 2024) . Meanwhile, in the United States, the Health Insurance Portability and Accountability Act (HIPAA) has set standards for electronic health information security(Drolet et al., 2017) . In Indonesia, the protection of patient health data is regulated in several regulations, including Law No. 29 of 2004 on Medical Practices which regulates the obligation of doctors and health workers to maintain the confidentiality of medical records(Supriyatin, 2018; Tinungki, 2019) , Law No. 36 of 2009 on Health which emphasizes that patient personal information must be kept confidential, Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law)(Nomor, 11 C.E.) which includes provisions on electronic data protection, and Law No. 27 of 2022 on Personal Data Protection (PDP Law) which provides a stronger legal framework for the management of personal data, including health data .(Suryanto & Riyanto, 2024)

Despite existing regulations, the implementation and supervision of patient data protection still face various obstacles, such as the lack of data security standards in health facilities, patients' ignorance of their rights to health data, the lack of strict sanctions against patient privacy violations, and the unpreparedness of information technology infrastructure in many health facilities. With the increasing use of electronic medical record systems, an in-depth legal analysis is needed to understand the existing regulatory gaps and their implications for health data protection in Indonesia

This study aims to analyze the legal framework governing patient privacy in electronic medical records in Indonesia, identify forms of privacy violations that often occur in EHR systems in Indonesia, assess the effectiveness of the implementation of existing regulations in protecting patient health data, and develop policy recommendations to improve legal protection of patient health data in Indonesia.

To overcome the problem of health data protection in electronic medical record systems, this study offers several solutions that can be applied, including improving regulations and security standards by encouraging the adoption of international standards in health data protection, such as ISO 27799 (Information Security Management in Health) to ensure the security of EHR systems, and strengthening legal sanctions against those who violate patient privacy (Lestari et al., 2023). In addition, increasing the awareness and digital literacy of patients and medical personnel is important, by conducting socialization regarding patients' rights to their personal data and developing training for medical personnel and hospital administration regarding data security policies (Prasetyo, 2021). In terms of technology, the implementation of data encryption and multi-factor authentication can improve the security of access to electronic medical records, while the use of blockchain systems as a more secure and transparent data storage alternative can also be considered (Santoso, 2022). Supervision and auditing of health data management needs to be improved by establishing an independent supervisory institution tasked with overseeing the protection of health data on a regular basis and requiring hospitals and clinics to implement data security audits on a regular basis (Budiarto & Wicaksono, 2023).

The research aims to serve as an academic and practical reference for health and legal stakeholders, including regulators, healthcare providers, and academics interested in data protection issues. By understanding and addressing the existing problems, it is hoped that the electronic medical record system in Indonesia can become more secure, reliable, and able to provide optimal protection of patient privacy rights.

METHODS

This research uses normative legal research methods with a statute approach, conceptual approach, and case approach(Ali, 2021; M. B. Ibrahim et al., 2023) . The normative legal method is used to examine legal rules relating to the protection of patient privacy in electronic medical records(Efendi & Ibrahim, 2021) . The statutory approach is carried out by examining relevant national and international regulations, such as Law Number 29 of 2004 concerning Medical Practice, Law Number 36 of 2009 concerning Health, Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law), and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).

The conceptual approach is used to analyze the legal principles underlying patient privacy protection, including the right to personal data protection, the concept of consent in health data processing, and the principle of accountability in electronic data management. Meanwhile, the case approach is used to examine various cases of patient privacy violations that have occurred in Indonesia and abroad. This case study aims to understand the patterns of violations, regulatory loopholes that are utilized, and how existing regulations and policies are implemented in practice.

The data used in this research consists of primary legal sources in the form of laws and regulations, court decisions, and related policy documents. Secondary legal sources include academic literature, legal journals, and previous research relevant to this topic (Hidayat & Setiawan, 2022). Data analysis was conducted using a qualitative analysis method, which examines and interprets legal norms and applicable practices in order to develop policy recommendations that are more effective in protecting patient privacy in the electronic medical record system.

RESULTS AND DISCUSSION

Legal protection of patient privacy in electronic medical records in Indonesia is regulated in various regulations, such as Law No. 36/2009 on Health which states that every individual has the right to confidentiality of their medical information. In addition, Law No. 27 of 2022 on Personal Data Protection (PDP Law) provides a more specific legal basis regarding the governance of personal data, including patient health data. Article 4 of the PDP Law emphasizes that specific personal data, such as health information, must receive extra protection in its processing. However, in practice, there are still many health facilities that have not implemented adequate data security standards, so patient data remains vulnerable to leakage and misuse.

Although regulations are in place, the main challenge in their implementation is weak supervision and law enforcement. Law No. 19/2016 on Electronic Information and Transactions (UU ITE) has actually provided a legal framework for electronic data breaches, but many cases of patient data leakage are not taken seriously by the relevant authorities. The lack of socialization and education to medical personnel regarding their obligations in maintaining the confidentiality of patient data is also a factor that exacerbates this situation. In addition, Article 79 of Law No. 29/2004 on Medical Practices requires doctors and health workers to maintain the confidentiality of patients' medical records, but there is no effective supervisory mechanism to ensure compliance with this provision.

Patient data leakage has far-reaching implications, both for individuals and for the healthcare system as a whole. From an individual perspective, leaked medical data can be used for harmful purposes, such as discrimination in health insurance services or misuse of medical information for illegal purposes. From an institutional perspective, leaked patient data can reduce the level of public trust in digital-based health services. A study conducted by Nugroho et al. (2023) showed that more than 60% of patients who experienced health data leakage became reluctant to use digital services in the future.

To overcome this problem, several steps can be taken. First, the government needs to tighten supervision of the implementation of the PDP Law by establishing an independent institution responsible for the protection of patient data. Second, capacity building of medical personnel and hospital administrative staff should be carried out through periodic training on patient data governance in accordance with legal provisions. Third, health facilities should be required to adopt more sophisticated security technologies, such as data encryption systems and layered authentication, to prevent unauthorized access to electronic medical records. Fourth, it is necessary to apply stricter sanctions against patient data breaches, as stipulated in Article 58 of the PDP Law, which stipulates administrative and criminal fines for perpetrators of personal data breaches.

It is also important to give patients greater rights to control their own medical data, as guaranteed in Article 26 of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which states that data owners have the right to know how their data is used and have the right to request the deletion of data that is no longer relevant. With these steps, it is hoped that the electronic medical record system in Indonesia can be more secure, reliable, and able to provide optimal protection for patient privacy.

CONCLUSION

From the results of this study, it can be concluded that the violation of patient privacy in electronic medical records is an increasing problem that requires serious attention. Existing regulations, such as Law Number 36 of 2009 on Health, Law Number 19 of 2016 on Electronic Information and Transactions (ITE Law), and Law Number 27 of 2022 on Personal

Data Protection (PDP Law), have provided a legal basis for the protection of patient data. However, weak implementation and lack of law enforcement mean that these regulations have not been fully effective in protecting patient health data from leakage and misuse. The biggest challenges in patient data protection in Indonesia include weak oversight, lack of awareness among medical personnel about the importance of data protection, and low security standards implemented by health facilities. Patient data leakage can have serious impacts on both individuals and institutions, including identity theft, misuse of medical information, and loss of public trust in digital-based healthcare systems. To overcome this problem, strategic steps are needed, such as increased supervision of the implementation of regulations, training for medical personnel and hospital administrative staff, adoption of better data security technology, and the application of stricter sanctions for violations of patient privacy. In addition, the role of patients in controlling and accessing their own data also needs to be strengthened so that they are more aware of their rights in personal data protection. With improved regulations and increased awareness as well as security technology, it is hoped that the electronic medical record system in Indonesia can become more secure, reliable, and able to provide optimal protection of patient privacy.

REFERENCE

Ali, Z. (2021). *Metode penelitian hukum*. Sinar Grafika.

Angelyn, M. C., Iswara, I. B. A. I., Putra, D. M. D. U., & Sastaparamitha, N. N. A. J. (2024). Towards Improved Heart Disease Detection: Evaluating Naïve Bayes and K-Nearest Neighbors in Medical Data Classification. *Jurnal Galaksi*, *1*(3), 190–197. https://doi.org/10.70103/galaksi.v1i3.45

Drolet, B. C., Marwaha, J. S., Hyatt, B., Blazar, P. E., & Lifchez, S. D. (2017). Electronic communication of protected health information: privacy, security, and HIPAA compliance. *The Journal of Hand Surgery*, *42*(6), 411–416.

Efendi, J., & Ibrahim, J. (2021). *Metode Penelitian Hukum Normatif dan Empiris*.

Fauzi, A. A., Kom, S., Kom, M., Budi Harto, S. E., MM, P. I. A., Mulyanto, M. E., Dulame, I. M., Pramuditha, P., Sudipa, I. G. I., & Kom, S. (2023). *PEMANFAATAN TEKNOLOGI INFORMASI DI BERBAGAI SEKTOR PADA MASA SOCIETY 5.0*. PT. Sonpedia Publishing Indonesia.

Hoffman, S., & Podgurski, A. (2022). Balancing privacy, autonomy, and scientific needs in electronic health records research. *SMUL Rev.*, *65*, 85.

Ibrahim, A. M., Abdel-Aziz, H. R., Mohamed, H. A. H., Zaghamir, D. E. F., Wahba, N. M. I., Hassan, G. A., Shaban, M., El-Nablaway, M., Aldughmi, O. N., & Aboelola, T. H. (2024). Balancing confidentiality and care coordination: challenges in patient privacy. *BMC Nursing*, *23*(1), 564.

Ibrahim, M. B., Sari, F. P., Kharisma, L. P. I., Kertati, I., Artawan, P., Sudipa, I. G. I., Simanihuruk, P., Rusmayadi, G., Nursanty, E., & Lolang, E. (2023). *METODE PENELITIAN BERBAGAI BIDANG KEILMUAN (Panduan & Referensi)*. PT. Sonpedia Publishing Indonesia.

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177–183.

Kim, E., Rubinstein, S. M., Nead, K. T., Wojcieszynski, A. P., Gabriel, P. E., & Warner, J. L. (2019). The evolving use of electronic health records (EHR) for research. *Seminars in Radiation Oncology*, *29*(4), 354–361.

Nomor, U.-U. (11 C.E.). *tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Olorunfemi, O., Oyegoke, E. O., Abiodun, O. O., Kunle-Abioye, F. B., & Ayeni, B. A. (2024). Achieving a balance between ethical and legal obligations with regard to confidentiality and patient privacy. *Amrita Journal of Medicine*, *20*(3), 90–93.

Supriyatin, U. (2018). Aspek Hukum Dalam Penyelenggaraan Praktik Kedokteran Dihubungkan Dengan Undang-Undang Nomor 29 Tahun 2004 Tentang Praktik Kedokteran. *Jurnal Ilmiah Galuh Justisi*, *6*(1), 117–124.

Suryanto, D., & Riyanto, S. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Industri Ritel Tinjauan terhadap Kepatuhan dan Dampaknya pada Konsumen. *VERITAS*, *10*(1), 121–135.

Tinungki, J. P. (2019). Kewajiban Dokter dalam Membuat Rekam Medis Menurut Undang-Undang No 29 Tahun 2004. *Lex Et Societatis*, *7*(5).

Wallis, K. A., Eggleton, K. S., Dovey, S. M., Leitch, S., Cunningham, W. K., & Williamson, M. I. (2018). Research using electronic health records: Balancing confidentiality and public good. *Journal of Primary Health Care*, *10*(4), 288–291.