West Science Law and Human Rights
Vol. 3, No. 01, January 2025, pp. 1~8

Patient Data Privacy Challenges in Electronic Health Systems: A Juridical Analysis of Medical Information Protection in Indonesia

Ni Nyoman Putri Purnama Santhi
Universitas Bali Internasional

Article Info

Article history:

Received January, 2025
Revised January, 2025
Accepted January, 2025

Keywords:

health data privacy,
electronic health,
legal protection

ABSTRACT

The digital revolution has fundamentally transformed healthcare service systems, bringing complex legal issues related to patient data privacy protection. This research aims to analyze the juridical challenges of electronic medical information protection in Indonesia. Using a normative juridical method, the research examines regulatory frameworks, identifies legal gaps, and formulates responsive legal protection models. Research findings reveal that Indonesia's electronic health systems face structural weaknesses in guaranteeing data privacy. Existing regulations have not been able to accommodate digital technology developments, creating risks of medical information leakage and misuse. The complexity of challenges includes weak digital consent mechanisms, absence of cybersecurity standards, and minimal supervision. The research recommends comprehensive regulatory framework renewal, establishment of independent oversight bodies, and development of adaptive health data security protocols. This transformation requires an interdisciplinary approach that integrates legal, technological, and ethical perspectives. The research conclusion emphasizes the urgency of patient privacy rights protection in digital ecosystems while ensuring the effectiveness of modern healthcare services.

Corresponding Author:

Name: Ni Nyoman Putri Purnama Santhi
Institution: Universitas Bali Internasional
e-mail: putripurnama27@unbi.ac.id

1. INTRODUCTION

The digital revolution has fundamentally changed the healthcare system in Indonesia, with electronic health systems becoming the backbone of modern medical service transformation. The development of information technology has enabled the creation of a comprehensive electronic medical record system, facilitating the exchange of medical information between health facilities, and improving service efficiency [1]. However, behind this progress, there is a very significant complexity of legal issues, especially regarding the protection of patient data privacy.

The current digital era puts medical information in a vulnerable position. Every electronic health record contains sensitive data that includes not only medical history, but also highly personal information. The risk of data breach, information leakage, and misuse of medical data is a real threat in the electronic health system. Law No. 36/2009 on Health and the Regulation of the Minister of Health have not fully provided

comprehensive protection against the dynamics of the rapidly developing health information technology.

The legal reality in Indonesia shows the limitations of regulations in accommodating the development of digital health technology [2]. The absence of a solid protection mechanism has the potential to harm patient rights, creating legal loopholes that can be utilized by irresponsible parties. Therefore, an in-depth study of the challenges of patient data privacy in electronic health systems is urgent and critical. The development of information technology has created a new paradigm in the health care system, where patient data is no longer only stored in the form of physical documents, but integrated in a complex digital network. Electronic health systems are now capable of processing, storing and transferring medical information at an unprecedented scale and speed. However, the complexity of these systems brings with it very significant legal consequences regarding the security and privacy of personal data.

The big data phenomenon in the context of health has changed the way medical information is viewed [3]. Each electronic medical record does not simply store a history of illness, but rather becomes a strategic asset that can be utilized for research development, health policy, and even commercial interests. This raises critical questions about the ethical and juridical boundaries of utilizing patient data in the digital ecosystem. The vulnerability of electronic health systems to cyberattacks is a serious threat that requires comprehensive attention. Global reports show that the healthcare sector is a major target for cybercrime, with tens of thousands of medical data breach incidents occurring each year. Indonesia, as a developing country with a digital infrastructure that is still in its infancy, is particularly vulnerable to such risks.

Technological developments such as artificial intelligence, machine learning, and the Internet of Things (IoT) further complicate the issue of patient data privacy [4]. Advanced algorithms are now capable of analyzing health data on a massive scale, yielding insights that were previously unimaginable. However, on the other hand, this opens up great opportunities for violations of individuals' fundamental privacy rights. The international legal context shows a trend of increasingly stringent health data protection. Regulations such as the General Data Protection Regulation (GDPR) in Europe have become a global benchmark in protecting personal data, including health data. Indonesia is forced to immediately adapt and harmonize regulations in order to be in line with international standards and protect the interests of its citizens.

The juridical challenges in the protection of electronic health data do not stop at technological aspects, but include complex social, ethical, and human rights dimensions [5]. Every individual has a fundamental right to the confidentiality of their personal information, but digital systems often blur the boundaries of privacy. The balance between the need for efficient health services and the protection of individual rights is a crucial issue that requires in-depth study. The dynamic evolution of health information technology demands a responsive and adaptive legal approach. Conventional regulations that are static are no longer able to answer the complexity of data privacy issues in the digital era. A dynamic legal framework is needed, which can evolve along with technological advances, while still ensuring the fundamental protection of patient rights as the main subject in the health system.

This research focuses on the complexity of fundamental legal issues related to the protection of patient data privacy in the electronic health system in Indonesia. Specifically, the research intends to explore the existing legal construction, identify significant juridical challenges, and formulate an ideal legal protection model. The research questions are directed at analyzing how the current legal regulatory framework is able to accommodate the development of digital technology in the health system, while

comprehensively guaranteeing the protection of patient privacy rights.

The main objective of this research is to conduct an in-depth study of the juridical aspects of patient data protection in electronic health systems. The research aims to produce a comprehensive analysis of the applicable legal regulatory framework, with a focus on identifying legal gaps and practical challenges in ensuring the security of digital medical information. Furthermore, the research intends to formulate a responsive, adaptive and effective legal protection model, which can answer the complexity of data privacy issues in the era of Indonesia's digital health transformation.

This research is expected to make a multidimensional contribution to the development of digital health law. Theoretically, the research will enrich the academic literature and provide a new conceptual framework in understanding the dynamics of patient data protection. On a practical level, the research results are expected to be a strategic reference for policy makers, health facilitators, and stakeholders in designing more comprehensive regulations and data protection mechanisms. Socially, the research aims to increase public awareness of the importance of protecting health data privacy, encourage the creation of a safe, transparent, and dignified digital ecosystem, and protect the fundamental rights of patients in the electronic health system.

2. LITERATURE REVIEW

2.1 Concept of Health Data Privacy

Health data privacy is a fundamental concept that has undergone significant transformation in the digital era [6]. Theoretically, health data privacy goes beyond the protection of medical information and represents the protection of basic human rights. A comprehensive review shows that this concept crosses the doctrinal boundaries of health law, touching the realms of human rights, ethics, and personal data protection. This conceptual complexity presents theoretical and practical challenges in building a holistic protection framework that is responsive to the dynamics of information technology.

2.2 Development of Electronic Health Systems

Electronic health systems have undergone a complex evolution since their initial implementation [7]. Previous studies identified that the transformation from conventional to digital systems is not simply a technology shift, but a paradigmatic change in medical information governance. Systematic reviews show that the adoption of information technology in healthcare brings multidimensional consequences, ranging from increased service efficiency to increasingly complex risks of privacy violations.

2.3 Data Protection Regulatory Framework

The regulatory landscape of health data protection shows significant variation across regions and jurisdictions [8]. Comparative analysis reveals that there is no single model that can be applied universally. Each legal system has a unique approach in accommodating the development of digital technology. Previous studies emphasize the importance of an adaptive regulatory framework, able to adapt to the speed of change in health information technology.

2.4 Juridical Challenges in the Digital System

The complexity of juridical challenges in electronic health systems includes a multidimensionality of legal issues [9]. Issues such as data security, the concept of digital consent, information access restrictions, and protection mechanisms are the focus of academic studies. In-depth research shows that each stage of the electronic health system has legal loopholes that have the potential to cause violations of patient privacy rights.

2.5 Data Protection Technology and Ethics

The relationship between information technology and health data protection ethics is an increasingly complex area of study [10]. An interdisciplinary approach is needed to understand this dynamic, involving legal, technological, ethical and social perspectives. Philosophical research suggests that technological development cannot be

separated from deep ethical considerations of individual dignity and rights.

2.6 International Comparative Studies

A comparative analysis of health data protection systems in different countries yields critical findings. Developed countries such as the European Union with GDPR show a more comprehensive protection model, while developing countries still face structural challenges in implementing an effective data protection framework. This comparative study provides a global perspective in understanding the dynamics of health data protection.

2.7 Legal Theory and Digital Data Protection

The development of legal theory in the context of digital data protection shows a paradigmatic shift. Classical theories of privacy and data protection are fundamentally tested and reconstructed by the reality of contemporary information technology. Theoretical studies emphasize the need for a more flexible, responsive and anticipatory legal approach to continuous technological innovation.

3. METHODS

3.1 Research Approach

This research uses the normative juridical method, which places the law as a system of norms. This approach fundamentally examines the law through a comprehensive analysis of legislation, legal doctrine, and legal norms relating to the protection of patient data privacy in electronic health systems. Through the normative juridical method, the research is able to conduct an in-depth investigation of existing legal constructions, identify legal gaps, and formulate legal protection concepts that are responsive to the dynamics of digital technology.

3.2 Types and Sources of Legal Materials

The research is based on comprehensive and tiered legal materials. Primary legal materials include laws and regulations that directly regulate electronic health systems, including the Health Law, Electronic Information and Transaction Law, and relevant Ministry of Health regulations. Secondary legal materials consist of academic literature, scientific journals, previous research results, and international documents that provide theoretical and practical perspectives. Tertiary legal materials include supporting reference sources such as legal dictionaries, encyclopedias, and additional sources of information that can enrich the research analysis.

3.3 Legal Material Collection Technique

The process of collecting legal materials was carried out through a comprehensive literature study. Researchers conducted a systematic search of various legal sources, both in physical and digital formats. Documentation studies were conducted in depth, focusing on critical analysis of official documents, academic publications, and relevant written sources. Digital searches through electronic databases and academic platforms were used to access current and up-to-date sources relating to health data protection.

3.4 Legal Material Analysis Technique

Analysis of legal materials is carried out in a multidimensional manner. An analytical descriptive approach was used to describe and systematically analyze legal regulations, concepts, and practices of patient data protection. Legal interpretation techniques include grammatical interpretation that pays attention to the language of the regulation, systematic interpretation that looks at the interrelationship between regulations, and teleological interpretation that considers the purpose and context of the law. Legal construction is carried out to build a new conceptual framework in understanding the protection of patient data privacy in the digital era.

3.5 Specific Research Approach

The research integrated several specialized approaches to ensure a comprehensive analysis. A statutory approach was used to review the applicable regulations. The conceptual approach enabled the development of a new theoretical framework. A comparative approach was

utilized to compare health data protection practices across different jurisdictions, providing a broader and deeper perspective.

3.6 Conceptual Limitation

The research limits the scope of the study to electronic health systems in Indonesia, with a particular focus on patient data privacy in a digital context. The study focuses on analyzing national and international legal frameworks, as well as the challenges of information technology in health services. This limitation is intended to provide depth of analysis and sharpness of research focus.

3.7 Systematization of Discussion

The research will be built systematically, starting from the identification of complex legal issues, followed by an in-depth analysis of the existing regulatory framework. The next stage is a critical evaluation of the juridical challenges faced by the electronic health system. The conclusion of the research will lead to the formulation of a legal protection model that is comprehensive, responsive, and adaptive to the development of health information technology.

4. RESULTS AND DISCUSSION

4.1 Regulatory Framework and Structural Challenges

The legal construction of electronic health data protection in Indonesia faces significant complexities that require a thorough transformation [11]. Existing laws, such as Law No. 36/2009 on Health, reveal fundamental limitations in accommodating the development of digital technology. The fundamental weakness lies in the inability of existing regulations to define data protection mechanisms, the scope of medical information confidentiality, and electronic system security protocols. Technological developments such as cloud computing and big data analytics in the health system create new challenges that have not been accommodated in the existing legal construction.

Overlapping authorities and legal interpretations between government agencies further complicate efforts to protect electronic health data, pointing to the need for comprehensive and integrated regulatory harmonization. The legal construction of electronic health data protection in Indonesia faces significant complexities that require a comprehensive transformation. Existing laws, such as Law No. 36/2009 on Health, reveal fundamental limitations in accommodating the development of digital technology. The fundamental weakness lies in the inability of existing regulations to define data protection mechanisms, the scope of medical information confidentiality, and electronic system security protocols

Technological developments such as cloud computing and big data analytics in the health system create new challenges that have not been accommodated in existing legal constructions. Overlapping authorities and legal interpretations between government agencies further complicate efforts to protect electronic health data, pointing to the need for comprehensive and integrated regulatory harmonization.

4.2 Privacy Complexity and Data Security Risks

Electronic health systems in Indonesia are highly vulnerable to data breaches [12]. The health information technology infrastructure spread across various health facilities does not have uniform security standards, creating security gaps that could potentially be misused. The integration of Internet of Medical Things (IoMT) technologies further complicates privacy protection challenges, generating real-time health data that requires layered security protocols and more sophisticated verification systems. Cybersecurity threats are becoming a serious challenge, with the development of increasingly sophisticated attacks [13].

Methods such as ransomware, social engineering attacks, and the use of artificial intelligence for cyber-attacks create a very high risk of data leakage. The absence of standardized security protocols that healthcare facilities are required to implement

further exacerbates the situation, leaving Indonesia's eHealth system in a highly vulnerable state. The electronic health system in Indonesia is highly vulnerable to data breaches. The health information technology infrastructure spread across various health facilities does not have uniform security standards, creating security gaps that could potentially be abused. The integration of Internet of Medical Things (IoMT) technology further complicates the privacy protection challenge, generating real-time health data that requires layered security protocols and more sophisticated verification systems. Cybersecurity threats are becoming a serious challenge, with the development of increasingly sophisticated attacks. Methods such as ransomware, social engineering attacks, and the use of artificial intelligence for cyber-attacks create a very high risk of data leakage. The absence of standardized security protocols that health facilities are required to implement further exacerbates the situation, leaving Indonesia's eHealth system in a highly vulnerable state.

4.3 Consent Mechanism and Patient Autonomy

The concept of digital consent in Indonesia's electronic health system is still very weak, which is contrary to the fundamental principle of individual autonomy [14]. The majority of healthcare facilities do not provide a transparent mechanism to inform patients about the use of their medical data, so patients often lose full control over their personal information. Innovative solutions are emerging, such as the development of blockchain-based consent management systems that offer transparent and controlled mechanisms. The implementation of dynamic consent allows patients to modify their privacy preferences over time, while the integration of artificial intelligence can help patients understand the implications of each data sharing decision. The concept of digital consent in Indonesia's eHealth system is still very weak, which goes against the fundamental principle of individual autonomy. The majority of healthcare facilities do not provide transparent mechanisms to inform patients about the use of their medical data, so patients often lose complete control over their personal information. Innovative solutions are emerging, such as the development of blockchain-based consent management systems that offer transparent and controlled mechanisms. The implementation of dynamic consent allows patients to modify their privacy preferences over time, while the integration of artificial intelligence can help patients understand the implications of each data sharing decision.

4.4 International Comparisons and Recommendations for Transformation

A comparison with international regulatory frameworks such as GDPR, CCPA, and HIPAA shows significant gaps in health data protection in Indonesia [8]. Developed countries have developed much more comprehensive protection systems, with strict oversight mechanisms, clear sanctions, and stronger protection of individual rights. Comprehensive transformation requires a multidimensional approach, including updating the regulatory framework, establishing independent oversight bodies, developing national security standards, and public education programs.

A risk-based approach and the adoption of privacy by design are key in building an effective health data protection system [15]. A comparison with international regulatory frameworks such as GDPR, CCPA, and HIPAA shows significant gaps in health data protection in Indonesia. Developed countries have developed much more comprehensive protection systems, with strict oversight mechanisms, clear sanctions, and stronger protection of individual rights. A comprehensive transformation requires a multidimensional approach, including updating the regulatory framework, establishing an independent oversight body, developing national security standards, and public education programs. A risk-based approach and the adoption of privacy by design are key in building an effective health data protection system.

4.5 Ethical and Social Implications

Digital transformation in the health system cannot be separated from deep ethical considerations. The democratization of health data access creates new dilemmas related to digital justice, where disparities between community groups have the potential to create discrimination in access to and control over personal health data. The commercialization of health data by large technology corporations creates new power dynamics that have the potential to threaten patient autonomy. The balance between the utilization of data for the public interest and the protection of individual privacy is a crucial ethical issue in the context of the development of digital health technology

Digital transformation in the health system cannot be separated from deep ethical considerations. The democratization of health data access creates new dilemmas related to digital justice, where disparities between community groups have the potential to create discrimination in access to and control over personal health data. The commercialization of health data by large technology corporations creates new power dynamics that have the potential to threaten patient autonomy. The balance between the utilization of data for the public interest and the protection of individual privacy is a crucial ethical issue in the context of the development of digital health technology.

5. CONCLUSION

A comprehensive study of patient data privacy challenges in Indonesia's eHealth system reveals a significant complexity of legal issues. The current eHealth system faces structural vulnerabilities in protecting sensitive patient data, due to the limitations of the existing regulatory framework. Existing laws and regulations have not been able to fully accommodate the development of digital technology, creating legal loopholes that could potentially harm the privacy rights of individuals. The research identified that the main challenges lie in the absence of comprehensive protection mechanisms, weak cybersecurity protocols, and the absence of standardization of electronic health systems. Digital transformation in healthcare demands a legal approach that is responsive, adaptive, and able to ensure a balance between technological efficiency and human rights protection.

SUGGESTIONS

1) The government needs to immediately conduct a comprehensive revision of laws and regulations related to electronic health systems, by adopting international standards such as GDPR and taking into account the latest developments in information technology.
2) The Ministry of Health should establish a specialized independent body responsible for overseeing the protection of electronic health data, with the authority to conduct security audits, set standards, and impose strict sanctions against violations.
3) Facilitate the development of health information technology infrastructure that has high security standards, by integrating the latest encryption protocols, cyber threat detection systems, and strict data protection mechanisms.
4) The Ministry of Communication and Informatics together with the Ministry of Health need to design a special regulation that regulates a transparent digital consent mechanism and gives patients full control over the use of their personal data.
5) Universities and health research institutions are encouraged to develop interdisciplinary research that brings together legal, technological, ethical, and social perspectives in order to develop a comprehensive health data protection model.
6) Continuous implementation of public education and socialization programs to increase public awareness on the

importance of health data privacy protection, digital rights, and potential risks in electronic systems.

7) Promote international collaboration and knowledge exchange with developed countries in developing legal and technological frameworks for electronic health data protection that are responsive and adaptive to global developments.

REFERENCES

[1] Utami, Y. T., Dharma, R. A., Sari, D., Br, N., Amanda, D., Nabila, Y. A., Wahyudi, S., Ms, P., & Mauliyand, S. (2024). *The Role of Technology in Planning and Evaluation of Hospital Medical Records Health*. *7*(8), 3236-3241. https://doi.org/10.56338/jks.v2i1.695

[2] Heriani, I., & Adlina, N. A. (2024). Legal Aspects of Telemedicine in Indonesia: Challenges and Opportunities in the Digital Era. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, *2*(3), 1398–1405.

[3] Saudjhana, A., Budiman, A., Fernando, H., Juliantio, J., Junianto, K., Venessa, K., Salim, S., & Tomy, T. (2024). Implementation of Big Data for Medical Checking and Health Consultation in Indonesia. *Journal of Information System and Technology*,*5* (1), 1-6. https://doi.org/10.37253/joint.v5i1.4323

[4] Andika, & M. Soemarno. (2023). Privacy and Personal Data Security Issues in the Application of Artificial Intelligence. *INNOVATIVE: Journal Of Social Science Research*, *3*, 4917– 4929.

[5] Primasatya, S. (2024). Protection Against the Development of Artificial Intelligence-Based Health Services in Indonesia. *Journal of Legal Globalization*,*1* (1), 78-93. https://doi.org/10.25105/jgh.v1i1.19833

[6] Hanaya, E. (2023). Personal Data Protection in the Digital Age in a Comparative Legal Perspective. *Bevinding Journal*, *1*(9), 11–22.

[7] Ristivani, A., Fitri, A., & Aknuranda, I. (2022). *ANALYSIS OF THE SUCCESSFUL IMPLEMENTATION OF ELECTRONIC MEDICAL RECORDS (EMR) IN PRIVATE CLINICS USING THE HUMAN ORGANIZATION TECHNOLOGY-FIT MODEL*. *1*(1), 1–7.

[8] Heriyanto, H. (2023). Comparative Analysis of Regulations and Legal Protection of Patient Data Privacy in Three Southeast Asian Countries (Indonesia, Singapore, and Laos). Ners Journal,7 (2), 1247-1259. https://doi.org/10.31004/jn.v7i2.16760

[9] Pantow, A. W., Gabriela, J., & Gunawan, C. (2024). *PROVING THE CRIME OF SELLING IMPORTED MEDICAL DRUGS*. *1*(5), 177–190.

[10] Budiyanti, R. T., Herlambang, P. M., & Nandini, N. (2019). Ethical and Legal Challenges of Using Electronic Medical Records in the Era of Personalized Medicine. *Journal of Vocational Health*,*4* (1), 49. https://doi.org/10.22146/jkesvo.41994

[11] Cahya, A. N., Maksum, M. A., & Primadana, T. A. S. (2024). Transformation of Legal Culture in the Digital Era (Implications of the Use of AI in the Development of Law in Indonesia). *IKRA-ITH HUMANITIES: Journal of Social and Humanities*, *8*(2), 361–373.

[12] Siti Ashira Salvina Day, & Rahayu Subekti. (2024). Liability of System Provider Electronic Medical Records from Partner System Against Data Leakage. *Democracy: Journal of Legal, Social and Political Science Research*,*1* (3), 92-101. https://doi.org/10.62383/demokrasi.v1i3.253

[13] Widya, D., Simatangkir, E., Semarang, U. N., Semarang, U. N., Faliha, N. S., & Semarang, U.N. (2025). *CYBERSECURITY IN BANKING AND CHALLENGES*. *2*(1), 33–42.

[14] Salsabila, M. (2024). Contemporary Challenges of Human Rights in Indonesia: Cases of Discrimination and Violence that Raise Awareness. *Socius: Journal of Social Sciences Research*,*1* (6), 89-96. https://zenodo.org/records/10476843

[15] Sunaryono. (2023). Optimal Portfolio of Bumn Sharia Shares with Single Index. *STIEP Economic Journal*,*8* (1), 72-81. https://doi.org/10.54526/jes.v8i1.138