Research Horizon

ISSN: 2808-0696 (p), 2807-9531 (e)

Research Horizon
Volume: 06
Issue: 03
Year: 2026
Page: 1225-1236

Citation:
Megaria, S., & Ismail, Y. C. T. (2026). Juridical review of legal protection against patient medical record data leaks in hospitals. *Research Horizon*, *6*(3), 1225-1236.

Article History:
Received: May 14, 2026
Revised: June 10, 2026
Accepted: June 23, 2026
Online since: June 25, 2026

Juridical Review of Legal Protection Against Patient Medical Record Data Leaks in Hospitals

Septiana Megaria[1*], Yana Chaeru Taufik Ismail[1]

[1] Department of Law, Faculty of Law, Universitas Islam Nusantara, Bandung, Indonesia

[*] *Corresponding author: Septiana Megaria (septinamegaria@gmail.com)*

Abstract

The rapid growth of information technology in the healthcare sector has increased the risk of patient data breaches, making legal protection increasingly important in Indonesia, where weaknesses in hospital data security systems remain evident. This study analyzes legal protections for patient data and evaluates the effectiveness of their implementation. A normative juridical literature review method was used, involving systematic analysis of books, scientific articles, research reports, and relevant legal documents. The findings show that patient data protection is normatively regulated under Law Number 44 of 2009 on Hospitals, Law Number 17 of 2023 on Health, and Law Number 27 of 2022 on Personal Data Protection. These laws emphasize hospitals' obligations to maintain patient confidentiality and restrict data access and use based on explicit consent. However, in practice, a significant gap remains between legal provisions and implementation. Weak data security infrastructure, limited awareness among healthcare personnel, and suboptimal law enforcement contribute to ongoing vulnerabilities. In conclusion, although the legal framework for patient data protection is well established, its effectiveness is still constrained by implementation challenges. Strengthening supervision, improving enforcement, and enhancing human resource capacity are essential to ensure more effective protection of patient data in Indonesia.

Keywords

Data Breach, Hospital, Legal Protection, Medical Privacy, Patient Data.

1. Introduction

In today's digital era, technological advancement has significantly transformed the healthcare sector, particularly through the adoption of Electronic Medical Record (EMR) systems (Barbieri et al., 2023). EMRs provide a more efficient and accurate method of managing patient information than conventional manual systems, enabling authorized medical personnel to access medical histories, laboratory results, and treatment plans in real time (Ayaad et al., 2019; Hidayat et al., 2025). This system greatly supports both emergency and routine healthcare services. However, alongside these benefits, the increasing use of digital health systems also raises serious concerns regarding the potential leakage and misuse of patients' personal data, which remains a critical challenge for healthcare institutions (Takaryanto & Lany, 2025).

Health information is categorized as highly sensitive personal data, and every individual has the right to ensure that their medical information is not disclosed or misused without valid consent (Temirkanova et al., 2025). Violations of this right may cause psychological distress, discrimination, financial loss, identity theft, and reputational damage. In the era of globalization and digital healthcare, patient data can easily move across institutions and national borders through telemedicine and international medical collaborations (McClelland & Harper, 2022). However, Indonesia still faces regulatory gaps regarding cross-border medical data protection, increasing the risk of privacy violations beyond the reach of national legal enforcement.

The destructive impact of medical data privacy violations does not stop at the individual level (Supriyanto et al., 2025). Structurally, the failure to maintain data confidentiality can drastically diminish public trust in the credibility and professionalism of healthcare institutions and government authorities. When the public becomes skeptical and believes that their personal data and medical records are not securely guarded by hospitals, they tend to adopt a defensive stance. Patients might conceal crucial information, hesitating to provide an honest and accurate anamnesis regarding their past medical history or infectious diseases they might carry (Alifia et al., 2024). This lack of transparency will ultimately backfire, as it can severely hinder the process of establishing an accurate diagnosis and prescribing precise therapeutic treatments, which in turn could threaten the safety and life of the patient (Prajany et al., 2025).

Beyond relying on rigid positive law and technological security, the principles of biomedical ethics play an essential and inseparable role in maintaining medical data privacy (Jaime et al., 2023; Dove, 2024). Medical ethics, particularly through the manifestation of the principle of patient autonomy and the principle of non-maleficence, demands the application of and respect for comprehensive informed consent (Varkey, 2021). This consent is not limited merely to the execution of physical medical interventions but must also encompass consent regarding the acquisition, storage, utilization, and dissemination of the patient's medical data itself. This requires that every step of the data management process be conducted purely on the basis of informed consent from the patient after they have been provided with clear, lucid, and adequate explanations.

However, empirical evaluations of medical data privacy protection policies in Indonesia reveal that, despite the formal recognition of privacy rights in various regulations, oversight mechanisms and law enforcement remain ineffective and largely reactive. Sanctions imposed on healthcare institutions or cybercriminals involved in data breaches have not created a sufficient deterrent effect, resulting in recurring violations. In recent years, incidents involving leaks of patient medical record data from hospital databases have become increasingly common, driven by weak cybersecurity infrastructure, lack of staff awareness, human error, and

sophisticated cyberattacks such as ransomware, malware, and phishing. These conditions indicate that the implementation of legal protection for patient medical record data in healthcare institutions has not yet operated optimally (Kharisma & Diakanza, 2024).

Previous studies by Putra et al. (2024) and Lakoro and Jamaludin (2025) examined legal protection against patient data leaks, mainly focusing on hospital administrative weaknesses and normative legal sanctions. However, these studies have not comprehensively addressed the effectiveness of legal protection under the newly enacted Personal Data Protection Law (PDP Law) or the emerging challenges posed by digital health services such as telemedicine. Based on these findings, this study aims to analyze the legal protection framework for patient medical record data in Indonesia, evaluate the effectiveness of its implementation in healthcare institutions, and identify the regulatory, technological, and institutional challenges that hinder the realization of optimal patient data privacy protection in the digital health era.

2. Methods

This research is designed utilizing a literature approach rooted in the framework of normative or doctrinal legal research. This juridical-normative approach was selected considering that the central object of study in this research focuses on analyzing legal principles, positive legal norms, and constitutional norms, and evaluating the synchronization of sectoral regulations related to the protection of health data privacy and the implementation of electronic medical records at the hospital level. This approach involves a logical, systematic, and structured series of activities conducted by the researcher. This step begins with the process of document collection (literature inventory), followed by intensive critical reading, noting essential points and dogmatic arguments, and concluding with an in-depth analysis to reach academic conclusions. The fundamental objective of applying this method is to build a theoretical foundation, formulate a framework of thought, and concoct a comprehensive identification of legal problems, without having to collect empirical data such as direct field interviews or questionnaires (Efendi et al., 2016).

The legal materials used to construct the reasoning in this study are classified into three complementary main stratifications. First, primary legal materials are imperative, directly binding, and serve as the central object of analysis. These primary materials include key regulations, such as Law Number 44 of 2009 concerning Hospitals, Law Number 17 of 2023 concerning Health, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), as well as various derivative rules and implementing regulations like Minister of Health Regulation Number 24 of 2022 concerning Medical Records. Second, secondary legal materials play a crucial role in providing explanations, interpretations, and theoretical foundations for the primary legal materials. These materials include literature in the form of health law textbooks, articles published in reputable scientific journals, and various research reports from credible institutions that examine the intersection between medical privacy law and cybercrime. Third, tertiary legal materials are utilized to provide guidance and clarity of meaning to technical terms, as well as medical and technological terminology, such as law dictionaries, cybersecurity glossaries, and encyclopedias.

The analysis is guided by the concepts of legal protection theory, privacy rights, and data governance principles. The framework examines the normative basis of health data protection, the consistency between health regulations and personal data protection regulations, and the legal responsibilities of hospitals as data controllers in implementing electronic medical records. This framework serves as the basis for evaluating the effectiveness and coherence of the existing regulatory regime in safeguarding patient privacy. All data collected through this documentary study

method are then processed and examined using a qualitative descriptive-analytical technique, drawing conclusions through a deductive reasoning process, starting from general legal principles toward solving specific legal facts.

3. Results and Discussion

3.1. Legal Protection of Patient Data in Indonesia

The implementation of regulations and the legal landscape to protect the integrity of medical data in Indonesia has shown progressive leaps and highly significant advancements in recent years. This juridical reform occurred massively, especially after the House of Representatives passed Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) (Syailendra et al., 2024; Bintarawati, 2024). The birth of this law represents a crucial step and a historical milestone to protect and safeguard personal data entities, including health data, whose position and existence are increasingly vulnerable in the digital wilderness. The PDP Law, designed with the spirit of adopting international standards like the GDPR, provides a very clear, explicit, and comprehensive legal foundation regarding the governance of the personal data lifecycle (Rahmawati, 2022). This encompasses all phases, starting from the principle of proportionality in initial data collection at the registration desk, encryption security during server database storage, validation in the use of patient medical information for diagnosis, and down to permanent data deletion protocols.

Beyond the Personal Data Protection Law, the architectural framework of law protecting health data security is also strongly supported in the hierarchy of sectoral laws, primarily in Law Number 17 of 2023, which codifies regulations specifically focusing on universal Health. At the institutional managerial operational level, this protection mandate is detailed in the Minister of Health Regulation Number 24 of 2022 concerning medical records, which obligates the transformation of conventional systems into Electronic Medical Records (EMRs). These intertwining rules establish parameters and provide highly rigid technical guidelines on how patient data storage must meet minimum cryptographic standards, determining the qualifications of healthcare personnel authorized to access such sensitive information, as well as specific exception conditions (force majeure, court orders, or outbreak prevention) where medical data can be shared with other entities or institutions. Through this integrated regulatory decree, healthcare providers such as conventional hospitals, primary clinics, clinical laboratories, and digital health application pioneers are legally obligated to guarantee that patient data privacy remains sterile from all forms of exploitation and is not misused. In this context, hospitals function as data controllers and therefore bear strict legal responsibility for any failure in personal data protection mechanisms, as discussed by Sidiq (2025).

According to the taxonomy outlined in the Personal Data Protection Law, the definition of personal data is any piece of information regarding an individual that, whether standing alone or when combined with other secondary information, can be used to recognize, identify, and reconstruct their profile. In the specific realm of healthcare, this personal information does not fall into the general data category but is qualified as "specific personal data," which is exceptionally delicate, intimate, and sensitive. This data component details comprehensively not only demographics but also genetic or congenital disease histories, psychiatric diagnosis records, comprehensive laboratory test results, lists of medication referrals, allergies, and indications of disability. Philosophically, this string of information is not just an analytical set of numbers, ICD-10 disease codes, or dry medical notes without a soul; it is a complete reflection of the deepest aspects of a person's dignity and bodily integrity that must be kept confidential and whose existence must be respected.

One fundamental principle that serves as the lifeblood in every effort to protect health data is the principle of informed consent from the patient. Every healthcare institution, from small rural clinics to type A national referral hospitals, is absolutely required by law to obtain documented permission (usually in writing and equipped with a validated electronic signature) from the patient as the data subject. This permission must be obtained before medical personnel or hospital staff can access, use, analytically process, or transfer the personal data for any purpose outside direct clinical care. Furthermore, the law manifests its protection by granting patients the power to annul or withdraw the consent they have given at any time without having to provide complicated reasons. This consent withdrawal instrument ensures that patients maintain supremacy and ultimate control over the data they own (Nugraha et al., 2026). This progressive step essentially builds a highly robust legal protection umbrella, which is simultaneously expected to reconstruct and increase public trust to transition to and support the national digital health system ecosystem.

3.2. Implementation and Challenges in the Field

Theoretically and normatively, the obligation for protection has been established: all healthcare provider facilities, be it maternity hospitals, inpatient clinics, or health-tech startup developers, must ensure that patient medical record data is secure, locked, and not misused. The implementation of the regulatory mandates of the PDP Law and the Health Law requires every healthcare facility indiscriminately to put in place and build cybersecurity and privacy protection measures that comply with industry best practices. This protocol mandates the use of advanced encryption (Advanced Encryption Standard), the application of the least privilege concept, which restricts system access rights only and specifically to functionally authorized medical staff, the creation of an audit trail (access log record), as well as strict compliance to report system failures or personal data breaches to the ministry and data subjects within a maximum of 3x24 hours. These findings reinforce Nasir and Pranoto (2025), who emphasized that encryption standards and strict access control mechanisms are fundamental requirements in electronic medical record systems. However, when these noble norms collide with operational reality in Indonesia, many healthcare institutions visibly experience paralysis in facing them and grapple with various multi-layered empirical challenges.

One of the most deep-rooted problems frequently encountered is a comprehensive crisis or lack of resources, both in terms of financial funding allocation and the availability of Human Resources (HR) capacity, to design and implement a thorough data security system. For small-scale private hospitals and regional Community Health Centers in underdeveloped areas, overhauling the information system architecture from paper records to digitally certified secure servers requires an extraordinarily large injection of capital cost, which is often not budgeted. Besides financial issues, there is a syndrome of low security awareness regarding the importance of data rights protection among front-line hospital staff and healthcare workers themselves. Audit realities show that many hospital and clinic managers have not fully internalized the crucial substance of the PDP Law and view this regulation merely as a suggestion, not a strict obligation. The culture of underestimating data security aspects is still rampant. This is manifested in careless practices such as using very weak medical record system passwords ("123456" or "admin"), lacking periodic password rotation mechanisms, sharing usernames across nursing shifts, and setting up user access rights layers that are minimal and un-tiered. Furthermore, the extreme scarcity of Information Technology (IT) experts who possess specialization and licensing in health data protection serves as a massive barrier in translating these normative policies into practical security algorithms (Ogbodo et al., 2025).

Technical infrastructural challenges are equally terrifying. Quite a number of healthcare facilities, even hospitals with Regional Public Service Agency (*Badan*

Layanan Umum Daerah/BLUD) status, still rely heavily on legacy systems, pirated applications, as well as outdated hardware and software that no longer receive security patches from their original developers. This obsolete condition automatically makes the hospital's servers highly vulnerable, like an unlocked window, exceptionally easy to penetrate by cyberattack exploits and hacking infiltrations that cause data leaks. Facing this, a planned investment injection is needed to upgrade hardware servers and software firewalls, which must also be accompanied simultaneously by urgent human resource quality improvement training programs. Unfortunately, the limitations of the state/regional budget or internal revenue are often scapegoated as the main hindrance to the sluggishness of this update process (Ikawati & Haris, 2024)

The escalation of cyber threats, which become more adaptive and sophisticated day by day, is directly proportional to the increased fatal risk of medical data leaks. The transition towards the use of cutting-edge technology based on cloud computing, integration with mobile applications, and the proliferation of advanced medical devices (such as modern CT Scanners or pacemakers) directly connected to internal networks via the Internet of Things (IoT) concept, makes data security management topology incredibly complicated with a very broad attack surface. Alsubaei (2020) similarly argued that interconnected IoT-based medical devices significantly expand hospital cybersecurity vulnerabilities and complicate data protection management. Ransomware attacks targeting hospital systems are no longer mere fiction, evidenced by several major incidents in Indonesia that caused the paralysis of hospital operational services for weeks. Therefore, the preparation of preventive and comprehensive security contingency plans, rather than reactive ones, is needed to protect the integrity of data flowing freely across various platforms and endpoint devices.

From the repressive instrument of law enforcement, although the body of the PDP Law has valiantly established a stratification of exceptionally strict sanctions for any form of data protection violation or negligence, ranging from administrative sanctions in the form of written warnings, proportional fines up to a percentage of annual revenue, system access closures, to criminal imprisonment sanctions for individuals selling data, the fact remains that the effectiveness of this system is still far from ideal. Existing law enforcement faces a dead end due to the dullness of proactive supervisory functions from the ministry, the slow formation of an independent data protection authority supervisory body, and the extremely low initiative of incident reporting from hospital management to the public due to the looming fear of business reputation damage. Wulandari and Ilmih (2024) further noted that transnational cybercrime and dark web data trading create serious obstacles for cross-border enforcement and patient rights recovery mechanisms. Massive cross-ministerial collaboration, cyber incident response teamwork, and technological support must be realized immediately to strengthen the oversight system and restore the dignity of data protection law enforcement in the country.

3.3. Effectiveness of Patient Data Privacy Policies

Analyzing and calibrating the effectiveness of the foundational policies for patient medical record data privacy in Indonesia fundamentally depends heavily on three pillars of equilibrium: the authoritative strength of the regulation itself, the quality of implementative execution in the operational field, and the maturation of the readiness of human resources (brainware) and supporting technical infrastructure. Doctrinally, the presence of the Personal Data Protection Law takes over the position as the guiding star in protecting the flow of personal data, no exception being the whirlpool of health data in hospitals (Syailendra et al., 2024). This regulation dismantles the old paradigm by delegating far more veto rights and full control to patients over their genetic and medical information. The law imperatively requires healthcare institutions, as managing parties, to implement the principles of

integrity, information openness (transparency), the principle of data collection minimization (only collecting data that is truly essential for medical treatment), the fulfillment of the right to request data access, and strict and persistent layers of cyber protection security. Alongside the umbrella instrument of the PDP Law, these patient data security procedures are tightly stitched and locked in the technical specifications of the Health Law and the Minister of Health Regulations regarding EMRs. These technical rules reiterate the importance of the validity of explicit consent from patients, stringent interdepartmental database access restriction mechanisms, and the imposition of a proactive obligation to report honestly to authorities and patients immediately if the catastrophe of a data breach truly occurs.

In normative and theoretical review, the orchestration of this policy has succeeded in composing a legal foundation framework that is quite comprehensive, progressive, and considered capable of adapting (future-proof) in response to the accelerating pace of digital technology advancements disrupting the healthcare field. Patients as data subjects have been explicitly guaranteed their constitutional rights: the right to access their electronic medical records independently, the right to request corrections (revisions) to inaccurate medical history information, and the exclusive right to request permanent deletion (right to erasure or right to be forgotten) for data that is no longer relevant or when the retention period has legally expired. Patients are also armed with the absolute right to unilaterally revoke consent for the use of their data at any time (Temirkanova et al., 2025). With the availability of this protection ammunition, conceptually, the policy should provide a tangible contribution to efforts for the total protection of patients' clinical privacy rights and be able to build pillars of public trust regarding the security of electronic health service penetration (such as state or private e-health applications).

However, practical implementation remains hindered by various challenges that reduce the effectiveness of electronic medical record policies. Evidence from simulation studies and security audits in regional and private hospitals indicates that many healthcare institutions have not fully complied with personal data protection standards. Common deficiencies include unclear informed consent procedures, limited transparency regarding patient privacy rights, weak data deletion mechanisms, and insufficient training for healthcare personnel on privacy regulations. Consequently, despite a relatively comprehensive legal framework (law in books), the effectiveness of its implementation in hospital practice (law in action) remains fragile (Takaryanto & Lany, 2025).

Another trigger factor for challenges that greatly influences policy effectiveness is the porous foundation of technological security infrastructure behind the scenes of many healthcare institutions, a critical condition that is increasingly severe in regional facilities or Community Health Centers outside Java. Quite a lot of electronic medical record software currently in use has never been upgraded to be equipped with cutting-edge cybersecurity technology suitable for the demands of the times. These facilities do not apply encryption security algorithms for their databases, do not equip their networks with adequate firewall protection configurations against web application attacks, and entirely neglect the use of automated technologies such as Intrusion Detection/Prevention Systems. This dark reality nakedly makes piles of millions of rows of sensitive patient medical record data extremely vulnerable (Ikawati & Haris, 2024). The risk of threat is not only in the form of breaches and hacks by cybercrime syndicates out there (external), but also vulnerable to deliberate exploitation, theft, or manipulation by irresponsible internal parties, such as rogue employees (insider threats).

From the perspective of government authorities, the mandate for supervision and the implementation of law enforcement instruments continue to be the weakest link in the structure of patient data privacy effectiveness in Indonesia (Judijanto et al., 2024). Even though the state has formally produced the PDP Law, complete with a

range of massive administrative fine penalty instruments and criminal imprisonment sanctions against perpetrators of data misuse and theft, the culture of transparency and willingness to report and handle incidents professionally is often still paralyzed (Satwiko, 2021). Dozens of incidents of hospital data breaches or leaked health insurance credentials fail to be detected by security radars early on, and even if detected, these cases frequently stall halfway or are not precisely followed up by special cyber police or authorized agencies. This lack of decisiveness blatantly fails to create and has not yet provided the crucial and educational shock or deterrent effect for the data management ecosystem in hospitals, as well as for criminal hackers (Wulandari & Ilmih, 2024).

To inject life into efforts to increase the effectiveness of this protection policy, structural prevention innovations are recommended to start being implemented by adopting the mandatory mechanism of Privacy Impact Assessment (PIA). This PIA analysis procedure has the rationale as an initial identification method to map vulnerabilities, forecast hazard probabilities, and manage privacy rights risk management, which must be executed prior to the launch of any new module in the hospital health technology information system (Binns, 2017; Vemou & Karyda, 2020). PIA essentially functions to support healthcare institutions in measuring their absolute compliance with regulatory parameters, documenting risk catalogs administratively, and compiling mitigation and prevention controls before patient data leaks to the internet. Unfortunately, the use of crucial instruments like PIA in the map of the Indonesian healthcare industry still moves like a highly uneven pilot project, only applied in a handful of international standard hospitals, and requires a massive injection of political will and commitment from the top ranks of healthcare institution boards of directors and the relevant ministry regulatory guards.

Beyond regulatory frameworks and technological infrastructure, the effectiveness of patient data protection ultimately depends on organizational culture and the level of privacy literacy among healthcare professionals (Lakoro & Jamaludin, 2025). Effective implementation requires strong leadership commitment, continuous cybersecurity and privacy training for hospital staff, and enhanced patient awareness regarding confidentiality and autonomy rights. Although Indonesia has established a relatively comprehensive legal and administrative framework for protecting health data, its practical effectiveness remains limited. Therefore, strengthening regulatory enforcement, improving cyber oversight mechanisms, modernizing hospital information technology infrastructure, and enhancing human resource capabilities are essential. Sustainable collaboration among government institutions, hospital administrators, and technology providers is also crucial to developing a secure, transparent, and trusted healthcare data governance ecosystem.

4. Conclusion

Based on the findings of this normative legal research, Indonesia has established a relatively comprehensive legal framework for protecting patient medical record data through Law Number 44 of 2009 concerning Hospitals, Law Number 17 of 2023 concerning Health, and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). These regulations position healthcare institutions as data controllers that are legally obligated to maintain confidentiality, implement cybersecurity safeguards, and ensure informed consent mechanisms in electronic medical record systems. Nevertheless, this study identifies a substantial gap between normative legal provisions and their practical implementation in healthcare institutions. The findings reveal persistent challenges, including weak cybersecurity infrastructure, limited digital literacy among healthcare workers, inadequate supervisory mechanisms, and the growing complexity of cyber threats in digital health services and telemedicine systems.

The implications of this study emphasize the urgency of strengthening institutional compliance, improving cybersecurity governance, and enhancing coordination between healthcare providers and regulatory authorities to ensure effective patient data protection. However, this study is limited by its doctrinal and literature-based approach, which relies exclusively on secondary legal materials without direct empirical observation in hospitals or healthcare institutions. Consequently, the study cannot fully capture the operational realities and technical readiness of healthcare facilities in practice. Future research is therefore recommended to adopt empirical or socio-legal approaches through field studies, interviews, or case analyses involving hospitals, regulators, healthcare workers, and patients in order to evaluate the actual effectiveness of patient data privacy protection policies and cybersecurity implementation in Indonesia's digital healthcare ecosystem.

References

Alifia, J., Benny, D., & Maman, S. (2024). Tanggung jawab notaris dalam perlindungan data pribadi klien berdasarkan UU No. 27 Tahun 2022 tentang perlindungan data pribadi. *Jurnal Ilmu Hukum, Humaniora dan Politik*, *5*(1), 653–662. https://doi.org/10.38035/jihhp.v5i1.3204.

Alsubaei, F. S. (2020). *Security assessment framework for the Internet of medical things solutions.* Memphis: The University of Memphis.

Ayaad, O., Alloubani, A., Alhajaa, E. A., Farhan, M., Abuseif, S., Al Hroub, A., & Akhu-Zaheya, L. (2019). The role of electronic medical records in improving the quality of health care services: Comparative study. *International Journal of Medical Informatics*, *127*(9), 63–67. https://doi.org/10.1016/j.ijmedinf.2019.04.014.

Barbieri, C., Neri, L., Stuard, S., Mari, F., & Martín-Guerrero, J. D. (2023). From electronic health records to clinical management systems: How the digital transformation can support healthcare services. *Clinical Kidney Journal*, *16*(11), 1878–1884. https://doi.org/10.1093/ckj/sfad168.

Binns, R. (2017). Data protection impact assessments: A meta-regulatory approach. *International Data Privacy Law*, *7*(1), 22–35. https://doi.org/10.1093/idpl/ipw027.

Bintarawati, F. (2024). The influence of the personal data protection law (UU PDP) on law enforcement in the digital era. *Anayasa: Journal of Legal Studies*, *1*(2), 135–143. https://doi.org/10.61397/ays.v1i2.92.

Dove, E. S. (Ed.). (2024). *Confidentiality, privacy, and data protection in biomedicine: International concepts and issues.* Oxfordshire: Taylor & Francis.

Efendi, J., Ibrahim, J., & Rijadi, P. (2016). *Metode penelitian hukum: Normatif dan empiris.* Jakarta: Prenada Media Group.

Hidayat, N., Subekti, S., Astutik, S., & Widodo, E. (2025). Penegakan hukum terhadap penyalahgunaan data pribadi pengguna e-commerce menurut Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi. *Journal of Innovation Research and Knowledge*, *5*(2), 1221–1230.

Ikawati, F. R., & Haris, M. S. (2024). Challenges in implementing digital medical records in Indonesian hospitals: Perspectives on technology, regulation, and data security. In *Proceedings of the International Conference of Innovation Science, Technology, Education, Children and Health* (Vol. 4, No. 2, pp. 1–25). Malang: Institute Technology of Science and Health Dr. Soepraoen Hospital.

Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors*, *23*(21), 8944-8960. https://doi.org/10.3390/s23218944.

Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in Indonesia. *The Eastasouth Journal of Law and Human Rights*, *3*(1), 20–29. https://doi.org/10.58812/eslhr.v3i01.351.

Kharisma, D. B., & Diakanza, A. (2024). Patient personal data protection: comparing the health-care regulations in Indonesia, Singapore and the European Union. *International*

Journal of Human Rights in Healthcare, *17*(2), 157-169. https://doi.org/10.1108/IJHRH-04-2022-0035.

Lakoro, D. D. K., & Jamaludin, A. (2025). Legal responsibility of health professionals in protecting patient data. *Research Horizon*, *5*(3), 869–878. https://doi.org/10.54518/rh.5.3.2025.657.

McClelland, R., & Harper, C. M. (2022). Information privacy in healthcare the vital role of informed consent. *European Journal of Health Law*, *30*(4), 469–480. https://doi.org/10.1163/15718093-bja10097.

Nasir, A. F., & Pranoto, E. (2025). Analisis hukum terhadap pelaksanaan perlindungan data pribadi pasien dalam sistem rekam medis elektronik. *Fiat Iustitia: Jurnal Hukum*, *1*(1), 94–104. https://ejournal.ust.ac.id/index.php/FIAT/article/view/5490.

Nugraha, L. A., Zamroni, M., & Romadhon, A. H. (2026). Perlindungan data pribadi pasien atas penggunaan data rekam medis. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(2), 2901–2919. https://doi.org/10.61104/alz.v4i2.4726.

Ogbodo, D. C., Awan, I. U., Cullen, A., & Zahrah, F. (2025). From regulation to reality: A framework to bridge the gap in digital health data protection. *Electronics*, *14*(13), 2629-2640. https://doi.org/10.3390/electronics14132629.

Prajany, J. J., Silitonga, L., & Sapsudin, A. (2025). Regulation of ethical aspects of electronic medical records in Indonesia's positive law and implementation in hospitals. *Research Horizon*, *5*(4), 1477–1488. https://doi.org/10.54518/rh.5.4.2025.706.

Putra, N. I. K. U., Kuswardhani, T., & Purwani, S. P. M. (2024). Analysis of patient rights protection through medical record confidentiality and information disclosure system in Indonesian hospitals. *Journal La Sociale*, *5*(2), 539–549.

Rahmawati, N. A. (2022). Kebijakan-kebijakan pemerintah di masa pandemi dalam perspektif hukum kesehatan. *Jurnal Hukum, Politik dan Ilmu Sosial*, *1*(1), 43–57. https://doi.org/10.55606/jhpis.v1i1.1708.

Satwiko, B. S. (2021). Privacy and data protection: Indonesian legal framework. *Corporate and Trade Law Review*, *1*(2), 106–108.

Sidiq, M. A. (2025). Perlindungan hukum terhadap rumah sakit atas kebocoran data rekam medik elektronik yang dilakukan oleh peretas. *Akademik: Jurnal Mahasiswa Humanis*, *5*(2), 605–620. https://doi.org/10.37481/jmh.v5i2.1336.

Supriyanto, Rahardjo, T. M. S., Sumiyati, Noerdjaja, H., Pambudi, G. E., & Prabowo, M. S. (2025). Consumer protection legal frameworks in Indonesia: The challenges of e-commerce and data privacy. *Research Horizon*, *5*(2), 119- 128. https://doi.org/10.54518/rh.5.2.2025.491.

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: Challenges and opportunities. *Indonesia Law Review*, *14*(4), 175–190.

Takaryanto, D., & Lany, A. (2025). Legal protection of personal data in the exchange of electronic medical record in healthcare services. *Research Horizon*, *5*(6), 2817–2830. https://doi.org/10.54518/rh.5.6.2025.897.

Temirkanova, D., Nakisheva, M., Akimzhanov, Y., Karzhassova, G., & Khanov, T. (2025). International legal regulation of access to health information and the right to privacy. *Jurídicas CUC*, *21*(1), 173–187. https://doi.org/10.17981/juridcuc.21.1.2025.09.

Varkey, B. (2021). Principles of clinical ethics and their application to practice. *Medical Principles and Practice*, *30*(1), 17–28.https://doi.org/10.1159/000509119.

Vemou, K., & Karyda, M. (2020). Evaluating privacy impact assessment methods: Guidelines and best practice. *Information & Computer Security*, *28*(1), 35–53. https://doi.org/10.1108/ICS-04-2019-0047.

Wulandari, F. P., & Ilmih, A. A. (2024). Perlindungan data pribadi dalam kejahatan transnasional lintas-negara. *Aladalah: Jurnal Politik, Sosial, Hukum dan Humaniora*, *2*(4), 8–15. https://doi.org/10.59246/aladalah.v2i4.925.

Acknowledgment
We gratefully acknowledge the contributions of individuals who supported the completion of this article.

Funding Information
This research did not receive any funding.

Conflict of Interest Statement
The authors declare that there is no conflict of interest.

Ethical Approval and Originality Statement
Ethical approval was obtained for this study. The manuscript represents original work and has not been previously published, nor is it under consideration by another journal.

Data Disclosure Statement
The data that support the findings of this study are available from the corresponding author upon reasonable request.