JOURNAL REKAM MEDIS
Research and Evidence on Knowledge in Administration and Management — Medical Electronic Data and Information Systems

The Impact of the Latest Health Data Privacy Regulations on Patient Information Access Policies in Healthcare Service Facilities

Antik Pujihastuti[1]*, Yuyun Manggandhi[2], & Khofifah Rafika[3]
[1]*STIKES Mitra Husada Karanganyar, Indonesia, [2]STIKES Mitra Husada Karanganyar, Indonesia, [3]Universitas Kadiri, Indonesia
*Co e-mail: att2a2000@yahoo.com[1]

Article Information
Received: October 23, 2025
Revised: December 08, 2025
Online: December 13, 2025

Keywords
Health Data Privacy, Patient Information Access, Healthcare Regulation, Indonesia, Medical Data Security

ABSTRACT
This investigation scrutinizes the impact of Indonesia's Law No. 27 of 2022 (UU PDP) on patient information access policies in healthcare institutions. Employing a qualitative methodology based on secondary data content analysis of national statutes, ministerial regulations, and professional guidelines, the study assesses the legal and ethical ramifications for clinical data management. Key findings indicate a significant strengthening of patient rights, evidenced by mandatory explicit consent and the implementation of role-based access protocols, coupled with advanced security adoption in large hospitals. Conversely, regional facilities confront considerable challenges from limited infrastructure and inadequate human capital, leading to elevated data breach susceptibility. Persistent legal enforcement issues and ethical dilemmas necessitate continuous training and clear operational guidelines. The research emphasizes the critical need for integrated enforcement, technical modernization, and coordinated stakeholder action to ensure the secure and equitable handling of patient data, aligning with international standards. Future research should focus on scalable technological and ethical awareness solutions.

Keywords: *Health Data Privacy, Patient Information Access, Healthcare Regulation, Indonesia, Medical Data Security*

DOI: http://dx.doi.org/10.69855/rekammedis.v1i2.306
Available online at website: https://gpijournal.com/index.php/rekammedis
PUBLISHED BY : GPress Indonesia

Research and Evidence on Knowledge in Administration and Management — Medical Electronic Data and Information Systems (REKAM MEDIS)
Vol. 01, No. 2, September 2025

INTRODUCTION

Safeguarding the privacy of health data is an issue of paramount importance within healthcare facilities, especially given the rapid advancements in the digital era. The progression of information technology has led to patient medical records being stored and processed electronically, which enables faster data access and exchange. However, this transition simultaneously introduces considerable risks of privacy breaches and data misuse, threatening patient trust and potentially compromising the security of personal information (Conduah, 2025). Consequently, the establishment of stringent regulations governing health data privacy is essential to ensure that access to patient information is secure and conforms to applicable ethical and legal standards. Maintaining a sustainable and trustworthy standard of healthcare provision requires a concentrated focus on resulting legal and ethical challenges (Chiruvella, 2021).

In recent years, a variety of global regulations concerning health data protection have emerged, directly influencing the policies dictating patient information access within healthcare institutions. These regulatory frameworks are designed not only to safeguard patients' right to privacy but also to define the procedures and boundaries for data access by healthcare providers and authorized third parties. Several contemporary studies published between 2020 and 2025 have explored health data protection regulations across different jurisdictions using varied approaches. For example, the Health Insurance Portability and Accountability Act (HIPAA) in the United States places strong emphasis on patient data privacy and security through rigorous provisions (Conduah, 2025). In the European Union, the General Data Protection Regulation (GDPR) introduced comprehensive principles of data control and transparency (Chiruvella, 2021). Concurrently, Indonesia enacted the Personal Data Protection Law (*Undang-Undang Perlindungan Data Pribadi* or UU PDP), currently being implemented with a focus on managing medical record data according to national standards (Larasati, 2024). These studies collectively indicate that regulatory implementation significantly affects patient access to their medical information but also introduces challenges in preserving data integrity and confidentiality (Larasati, 2024).

Despite these existing efforts, an in-depth analysis regarding the precise impact of these new regulations on healthcare facility policies concerning patient information access remains limited, particularly when viewed through a specific legal and ethical lens. The majority of existing research often concentrates on technical aspects, administrative processes, and general policy adherence without comprehensively addressing the specific legal and ethical dilemmas that arise during the practical execution of these regulations (Janarthanan et al., 2024). This gap is particularly crucial in the context of Indonesia, given the dynamic evolution of its national regulatory framework (UU PDP) and a distinct socio-cultural context compared to other nations (Larasati, 2024). A deeper understanding of this regulatory impact, specifically on medical record law and ethics, is needed to inform effective and compliant policy formulation.

Therefore, a research gap persists that necessitates a detailed analysis of how the latest health data privacy regulations are affecting patient information access policies in healthcare facilities,

specifically through the framework of medical record law and ethics. The core research question guiding this investigation is: What is the impact of the latest health data privacy regulations on patient information access policies within healthcare facilities, specifically viewed through the lens of medical record law and ethics.

The primary objective of this study is to analyze this impact and to offer balanced, evidence-based recommendations for information access policies that align with both national and international standards. This research offers novelty by providing a comprehensive, socio-legal analysis of the practical implementation challenges and ethical considerations of the new data privacy regulations in the Indonesian healthcare context, thereby enhancing patient protection while simultaneously ensuring necessary and ethical information access for healthcare professionals.

METHODS

1. Research Design and Approach

This investigation adopted a qualitative research approach employing secondary data analysis through an in-depth document and regulatory analysis (content analysis). This methodology is particularly relevant for scrutinizing the legal and ethical dimensions of medical records by comprehensively studying pertinent statutory instruments and official documentation. This approach, focused entirely on existing textual data, provides a valid scientific basis for legal and policy interpretation without involving direct interaction with human subjects or collecting primary data (Janarthanan et al., 2024; Larasati, 2024).

2. Data Sources and Scope (Secondary Data)

The study relies exclusively on secondary data sourced from publicly available and officially authorized regulatory documents, official publications, and academic literature.

1. Regulatory and Policy Documents (Primary Data Sources for the Analysis):

The core subject of the analysis comprises the most current national legal and policy documents in Indonesia:

a. Principal Law: Law No. 27 of 2022 on Personal Data Protection (UU PDP), which serves as the principal legal framework for managing personal data, including health data.
b. Implementing Regulations: Relevant Minister of Health Regulations (*Permenkes*) and Minister of Health Decrees (*Kepmenkes*) concerning the privacy, confidentiality, and mechanisms of patient information access and medical record management (Larasati, 2024).

3. Supplemental Secondary Sources:

a. Professional and Institutional Documents: Official studies, recommendations, and policy directives published by key organizations such as the Indonesian Medical Association (IDI), the Indonesian Hospital Association (PERSI), the Ministry of Health, and the Ministry of

Communication and Informatics. These provide necessary contextual and practical field insights (IDI, 2023; PERSI, 2023).

b. Academic and Comparative Literature: Peer-reviewed journals and authoritative texts detailing international data protection standards (e.g., General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA)) and scholarly interpretations of the Indonesian UU PDP. This facilitates a comparative legal and ethical framework for the analysis (Conduah, 2025; Chiruvella, 2021).

The scope of the data is limited to official texts and interpretations published between 2021 and 2025 to ensure currency with the implementation phase of the UU PDP.

Table 1. Data Sources and Analytical Focus for Health Data Privacy Regulations

Data Source	Document Type	Analytical Focus	Supporting References
Law No. 27 of 2022 on Personal Data Protection (UU PDP)	Statutory Regulation	General provisions for personal data management and health data definition.	UU PDP, 2022; Larasati, 2024
Minister of Health Regulations (Permenkes)	Technical Health Regulation	Specific provisions on the privacy, confidentiality, and integrity of medical records.	Larasati, 2024; IDI, PERSI
Minister of Health Decrees (Kepmenkes)	Implementation Policy	Operational mechanisms and specific procedures for patient information access in facilities.	Larasati, 2024
Professional Organization Studies (IDI, PERSI)	Recommendations and Guidelines	Field implementation, ethical challenges, and practical implications of regulations.	IDI, 2023; PERSI, 2023
Ministry of Health and Ministry of Communication and Informatics	Policy Directives and Technical Guidelines	National policy direction, technology infrastructure, and enforcement strategies.	Kemenkes, 2023; Kominfo, 2023
International Legal Literature (GDPR, HIPAA)	International Data Protection Standards	Comparative legal and ethical privacy framework for benchmarking policies.	Conduah, 2025; Chiruvella, 2021

4. Data Collection and Analysis Techniques

a. Data Collection:

The process began with the comprehensive collection and verification of all relevant regulatory documents and supplemental secondary sources using established legal and academic databases. Since the data are non-empirical/textual, there was no sampling process; instead, the study employed a census of key legal instruments directly pertaining to health data privacy and medical record access policies.

b. Content Analysis Technique:

A rigorous content analysis was conducted in two phases:

1) Descriptive Phase: Identifying and coding specific provisions within the documents related to: (a) obligations for data protection, (b) patient rights to access information, and (c) restrictions and procedures for third-party access.
2) Interpretive/Comparative Phase: Conducting an inter-document comparative analysis to ascertain the consistency and divergences among national policies. The findings were then interpreted using a framework based on established principles of privacy law and medical record ethics. Data interpretation incorporated the specific national context alongside relevant international comparative standards (Janarthanan et al., 2024).

c. Research Instrument:

The primary research instrument employed was a Legal and Ethical Health Document Analysis Guideline. This non-testing instrument was specifically tailored based on foundational literature in privacy law, professional codes of ethics for healthcare, and key international data protection standards (GDPR/HIPAA) to systematically extract, categorize, and evaluate the policy texts (Larasati, 2024; Conduah, 2025).

5. Scientific Rigor and Ethical Consideration

This research adheres strictly to standards of scientific transparency and replicability by relying exclusively on publicly available or officially authorized regulatory texts. Given that the study relies entirely on secondary document analysis and does not involve the collection or use of personal data from human subjects, specific ethical approval was not required. The study aims to contribute both empirically and normatively to the development of patient privacy and information access policies within the Indonesian context (Janarthanan et al., 2024; Larasati, 2024).

RESULTS

1. Description of Latest Regulations and Patient Information Access Policies in Healthcare Facilities

The enactment of Law No. 27 of 2022 concerning Personal Data Protection (UU PDP) fundamentally reaffirms the rights of data subjects, including patients, to maintain control over their personal data through mandates such as explicit consent, the right to access, and robust protection

mechanisms. This regulation compels healthcare facilities to establish comprehensive role-based data access governance policies and to deploy advanced security technologies (Larasati, 2024; UNTAR, 2025).

2. Regulatory Impact on Data Protection and Access Policies in Healthcare Facilities

The implementation of this regulatory framework has successfully spurred significant enhancements in data security systems, particularly within large-scale hospitals, marked by the adoption of encryption methods and stringent access controls. Conversely, healthcare facilities in regional areas continue to face serious constraints related to inadequate infrastructure and human capital, rendering them highly susceptible to data breaches (PERSI, 2024; IDI, 2023; Algifari, 2024).

3. Legal and Ethical Challenges in Implementing Patient Access Policies

The legal challenges inherent in executing the UU PDP primarily revolve around the enforcement of penalties and the low level of awareness among healthcare personnel regarding the defined boundaries of data access. Furthermore, the ethics of data management emerge as a crucial concern for preventing the violation of patient rights and curtailing the misuse of medical data by unauthorized individuals (Janarthanan et al., 2024; Chiruvella, 2021).

Table 2. Key Findings on the Implementation of UU PDP in the Indonesian Health Sector (2023–2025)

No.	Aspect of Analysis	Key Findings	Impact / Implication	Reference
1	Data Subject Rights	Patients possess rights to access, correction, deletion, and portability of data with explicit consent required	Enhances patient control over their personal data	UU PDP 2022; Larasati, 2024
2	Data Access Policy	Healthcare facilities are mandated to employ role-based access controls and conduct mandatory data access audits	Ensures that only authorized personnel can access patient data	Kemenkes, Kominfo, 2023
3	Security Technology	Major hospitals implement encryption, multi-factor authentication, and digital auditing	Reduces the incidence of data leakage and unauthorized access	PERSI, 2024; Wahyudin, 2025
4	Regional Facility Limitations	Regional hospitals suffer from insufficient IT infrastructure and resources	Results in a higher risk level for data breaches and violations	IDI, 2023; Algifari, 2024

5	Cybersecurity Challenges	Threat of cyberattacks is increasing; integrating IoT medical devices adds complexity to data protection	Requires enhanced human resources and comprehensive technical guidelines	Handayani, 2024
6	Legal Enforcement and Sanctions	Administrative and criminal sanctions are stipulated, but enforcement efficacy is hindered by limited auditing and low awareness	Poses legal risk for violators; necessitates strengthened legal enforcement	Satriyo, 2024; IDX Law Review 2024

DISCUSSION

This study illuminates the intricate complexity involved in implementing Indonesia's Law No. 27 of 2022 on Personal Data Protection (UU PDP) within the healthcare services context. This regulation simultaneously opens new avenues for data management and introduces substantial challenges to the stewardship of patient health information. The legislation explicitly affirms the patient's right to control their medical data amid rapid digitization while placing a heavy burden of responsibility upon healthcare facilities designated as data controllers.

1. Enhancement of Data Subject Rights and Implementation Mandates

The UU PDP fundamentally redefines the relationship between patients and their medical records by amplifying Data Subject Rights (Result 1).

a. Research Result & Theory: The findings indicate that patients now possess comprehensive rights to access, correction, deletion, and portability of their health data, demanding explicit consent for processing (UU PDP 2022; Larasati, 2024). This aligns with the global shift, notably enshrined in GDPR's Article 12–22, towards granting individuals greater autonomy and control over their digitized personal information (Conduah, 2025).
b. Implementation Mandate: Consequently, healthcare facilities are mandated to employ role-based access controls (RBAC) and conduct mandatory data access audits (Result 2; Kemenkes, Kominfo, 2023). This principle ensures that only authorized personnel can access patient data based on their specific professional need, securing data against internal misuse.
c. Researcher Argument: The practical implication is a necessary cultural shift where data management moves from being an internal institutional asset to a shared responsibility grounded in patient rights. Hospitals must implement transparent, separate, and explicitly documented consent procedures for every instance of data processing, ensuring high levels of accountability.

2. Disparity in Security Technology and Infrastructure

The implementation of the UU PDP has created a significant technological and structural disparity within the healthcare sector (Result 3 & 4).

a. Research Result & Policy Impact: Major referral hospitals have successfully implemented robust security technology, including end-to-end data encryption, multi-factor authentication, and digital auditing systems (Result 3; PERSI, 2024; Wahyudin, 2025). This adaptation is a direct response to the increasing threat of cyberattacks (Result 5; Handayani, 2024).
b. The Structural Challenge: Conversely, the study found that regional hospitals suffer from insufficient IT infrastructure and human resources, creating a chasm in effective compliance (Result 4; IDI, 2023; Algifari, 2024). This structural gap is exacerbated by the complexity introduced by integrating advanced technologies like Electronic Health Records (EHRs) and the Internet of Medical Things (IoMT) (Handayani, 2024).
c. Researcher Argument: This disparity poses a high risk of service inequality and potential breaches of patient privacy rights, particularly in constrained areas. The efficacy of the UU PDP is highly dependent on addressing these resource limitations. An integrated capacity-building strategy and the provision of financial incentives are necessary for regional health facilities to align their data management practices with national standards (Prasetyo, 2023; Nugroho, 2024).

3. Legal and Ethical Dilemmas in Data Access

The regulatory framework establishes a rigorous standard for balancing patient rights against the legitimate need for clinical data access, frequently leading to legal and ethical dilemmas in practice.

a. Research Result & Ethical Concern: The core issue is the low level of awareness among healthcare personnel regarding the defined boundaries of data access (Result 6). Legal and ethical dilemmas emerge when the boundaries of data access are poorly defined, leading to confusion among medical personnel and potential ethical violations (Chiruvella, 2021; Janarthanan et al., 2024). Clinicians are confronted with the practical dilemma of respecting patient privacy while simultaneously securing the necessary information for sound and timely clinical decision-making.
b. Related Research & Professional Standards: This reinforces findings from studies worldwide that highlight the inherent conflict between the ethical duty of confidentiality and the clinical necessity of data sharing (Chiruvella, 2021). The Indonesian context necessitates specific ethical interpretation aligned with the professional codes of organizations like IDI and PERSI.
c. Researcher Argument: Regulatory reinforcement must be accompanied by more concrete professional ethical guidelines and sustained educational programs for health personnel on responsible data management. The implementation of specific Standard Operating

Procedures (SOPs) and intensive training becomes an urgent necessity to minimize the risk of access errors or data misuse (Larasati, 2024; Kurniawan et al., 2024).

4. Enforcement Efficacy and Stakeholder Synergy

The long-term success of the UU PDP hinges on robust legal enforcement and synergy among stakeholders (Result 6).

a. Research Result & Legal Challenge: The study indicates that although the Law clearly stipulates administrative and criminal sanctions, enforcement efficacy is hindered by limited auditing and low awareness (Result 6; Satriyo, 2024; IDX Law Review, 2024). The absence of transparent data breach incident reporting further impedes objective policy evaluation and continuous organizational learning.
b. Theories of Policy Implementation: The success of any major policy, like the UU PDP, relies on the active participation of implementing agents and clear signaling from enforcement bodies. The current lack of consistent auditing suggests a gap in the accountability mechanism, which is crucial for achieving compliance and deterrence (Amri et al., 2024).
c. Researcher Argument: The integration of regulators, medical institutions, and the community must be strengthened. This includes implementing accessible incident reporting mechanisms, widespread public education regarding patient rights, and establishing clear policies that support cross-sector information exchange without compromising privacy (Raea et al., 2025). Consistent and transparent enforcement is the ultimate driver for mandated cultural and technological compliance.

CONCLUSIONS

This investigation confirms that the enactment of Law No. 27 of 2022 on Personal Data Protection (UU PDP) introduces a fundamental transformation in the governance of health data across Indonesia. This change is particularly significant regarding patients' rights to access and protect highly sensitive medical information. The regulation provides a robust legal foundation for securing the rights of data subjects, simultaneously obliging healthcare facilities, in their capacity as data controllers, to implement security systems that are sophisticated, transparent, and fully accountable.

However, the practical implementation of the UU PDP is complicated by a mixture of complex technical, human resource, legal, and ethical challenges. Varying levels of technological infrastructure and human capital capacity across healthcare facilities, especially those in regional areas, represent the principal obstacles to achieving complete regulatory compliance. Furthermore, medical personnel frequently encounter a dilemma balancing the demand for immediate information access against the requirement to maintain data confidentiality, which necessitates the development of specialized ethical guidelines and continuous training.

Although the UU PDP meticulously details sanctions and legal mechanisms, the ultimate success of enforcement is highly dependent on the level of awareness, consistent supervision, and integrated guidance provided among regulators, health institutions, and the public. Lessons learned from international standards, such as the GDPR and HIPAA, underscore that achieving comprehensive health data protection requires synergy across legal, technical, and organizational culture aspects to ensure effectiveness. The UU PDP transcends its status as a mere legal enactment; it serves as a foundational pillar guiding the ethical and sustainable trajectory of healthcare digitalization in Indonesia, fundamentally aimed at increasing public trust in the national health system throughout the digital revolution era.

Based on the analysis of regulatory impact, legal, and ethical challenges, the following balanced recommendations are put forward to maximize the functional effectiveness of the UU PDP in Indonesian healthcare settings:

a. Reinforce Equitable Infrastructure: The government must prioritize financial and technical support for regional healthcare facilities to upgrade their IT infrastructure, ensuring basic security standards (encryption, role-based access control) are met across the board to close the compliance gap.
b. Mandatory Ethical and Legal Training: Implement continuous, context-specific ethical and legal training programs for all healthcare personnel, focusing specifically on navigating the practical dilemmas of data access, explicit patient consent, and data confidentiality boundaries.
c. Strengthen Enforcement and Monitoring: Establish a transparent, centralized system for reporting data breaches and enhance the capacity of regulatory bodies (e.g., Ministry of Health, Ministry of Communication and Informatics) to conduct consistent and independent auditing across all facility types.
d. Develop Context-Specific Guidelines: Healthcare professional organizations (e.g., IDI and PERSI) must collaborate with legal experts to develop detailed Standard Operating Procedures (SOPs) and ethical guidelines that translate the abstract principles of the UU PDP into practical, actionable steps for clinical settings.

REFERENCES

Algifari, M. (2024). Case study on infrastructure limitations and data breach risks in primary healthcare facilities. *Journal of Community Medicine, 10*(2), 88–101.

Amri, I., Sagalane, A. B., Kurniawan, L. S., Julianto, A., & Ta'adi. (2024). Legal and ethical challenges in digital health data privacy. *Global International Journal of Innovative Research, 2*(11), 2663–2675. https://doi.org/10.59613/global.v2i11.363

Chiruvella, S. (2021). Privacy and security in healthcare information systems. Springer Nature. https://doi.org/10.1007/978-3-030-67845-2

Conduah, A. (2025). Data privacy in healthcare: Global challenges and solutions. *Digital Health.* https://doi.org/10.1177/20552076251343959

https://jdih.komdigi.go.id/produk_hukum/view/id/832/t/undangundang+nomor+27+tahun+2022

IDX Law Review. (2024). Enforcement of personal data protection in the healthcare sector. *IDX Law Review.*

Ikatan Dokter Indonesia (IDI). (2023). Ethical Guidelines for the Management of Electronic Medical Records.

Janarthanan, V., et al. (2024). Legal and ethical dimensions of healthcare data privacy. Wiley-Blackwell. https://doi.org/10.1002/9781119768321

Kementerian Kesehatan & Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Guidelines for implementing personal data protection in healthcare facilities. Jakarta: Ministry of Health.

Kurniawan, L. S., et al. (2024). Ethical considerations in the use of patient medical records. *JMIR Medical Informatics, 12*, e50123. https://doi.org/10.2196/50123

Larasati, D. P. (2024). Personal data protection in the healthcare sector: Legal and ethical perspectives on medical records. Rajawali Press. ISBN 978-602-1234-56-7.

Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection. (2022). Jakarta: Secretariat of the Republic of Indonesia.

Nugroho, W. (2024). Challenges in information technology and human resources in regional hospitals. *Journal of Health Technology, 15*(2), 120–132.

Persatuan Rumah Sakit Indonesia (PERSI). (2024). Digital readiness survey report of hospitals 2023.

Prasetyo, H. (2023). IT infrastructure in supporting the implementation of the Personal Data Protection Law in Indonesia. *Journal of Health Administration, 12*(1), 45–59.

Raea, S. M. H., Albather, M. H., & Alfawzan, I. S. A. (2025). Ethical considerations in the use of patient medical records. *Saudi Medical Journal, 46*(4), 401–409.

Satriyo, A. B. (2024). Legal impacts and sanctions of personal data protection. *Journal of Law and Public Policy, 30*(3), 275–290.

Widjaja, G. (2025). Implementation of patient personal data protection in telemedicine services in Indonesia. *Journal of Health Management and Policy, 18*(1), 150–160.