Society Synergy Conference (SSC)
Volume II; Number II; Year 2025; Pages 619-629
Website:https://sinergilp.com
E-ISSN: 3048-3530

The Legal Status of the Personal Data Protection Act as a Guarantee of Patient Privacy Rights in Indonesia

Hilbertus Sumplisius M. Wau [1], Henry Aspan [2], Sumarno [3]
[123] Universitas Pembangunan Panca Budi
E-mail:sumplisiuswau@gmail.com henryaspan@dosen.pancabudi.ac.id sumarno@dosen.pancabudi.ac.id

Abstract

The rapid advancement of information technology has brought significant changes to healthcare services, particularly in the management of patients' personal data. The digitalization of healthcare not only enhances efficiency but also poses serious risks of data breaches that threaten patients' privacy rights. Law Number 27 of 2022 on Personal Data Protection has emerged as the State's effort to provide comprehensive legal protection for personal data, including health data, which is classified as specific data. This study employs a normative juridical approach by examining relevant regulations and data protection principles within the context of health law. The findings indicate that the government plays a central role in the control of personal data, both preventively and repressively, through its supervisory authority and law enforcement powers in cases of violations. The legal protection of patient privacy has been normatively strengthened; however, its implementation still faces challenges, particularly regarding institutional compliance, stakeholder awareness, and the effectiveness of supervisory authorities. Therefore, institutional reinforcement, public dissemination, and the modernization of data security systems are essential to ensure that the constitutional right to privacy is genuinely upheld in practice.

Keywords: Personal Data, Patient, Legal Protection, Personal Data Controller, Privacy

INTRODUCTION

The rapid development of information technology has had a significant impact on healthcare service systems, particularly in the management of patients' personal data. Medical records that were once stored in physical form have now been transformed into digital formats, making them more accessible, easier to store, and transferable. This transformation facilitates efficiency, but also increases the risk of personal data breaches that may harm patients psychologically, socially, and economically.

The rapid progress of technology and communication in human life has a dual effect, much like a double-edged sword. On one hand, the use of information and communication technology contributes to the advancement of human welfare and civilization. On the other hand, such technological developments may be exploited to commit unlawful acts that infringe upon legal interests, societal order, and national security. These include internet misuse, stalking, hacking, carding (credit card data theft), fraud, and defamation (Azwar et al., 2025).

In the digital era, the health sector is experiencing a significant transformation through the use of information and communication technology, where now everything can be controlled from anywhere through the internet network and interconnected devices.(Kusnadi, 2021)The application of these sophisticated technologies has had a significant impact on society at large in their daily lives, such as increasing work productivity, building socio-economic relationships, and facilitating various activities, including patient data management, electronic medical records, and telemedicine services. However, these advances also pose serious threats to the confidentiality and privacy of patients' personal data. Health data leaks not only impinge on

patients' privacy rights but can also lead to stigma, discrimination, and other personal and social harms.

In this rapidly evolving digital era, individuals' personal data is increasingly vulnerable to potential misuse and privacy violations. Indonesia, as a developing country with rapid technology adoption, has a responsibility to protect personal data as a means of privacy. In this context, the right to privacy is an urgent issue that needs to be addressed. The right to privacy is the fundamental right of every individual to maintain the confidentiality and security of their personal data. With the rise in cases of privacy violations and misuse of personal data, it is crucial for every country to have effective legislation to protect the privacy rights of its citizens.(Anggen Suari & Bachelor, 2023)

This situation has pushed the need for a legal framework capable of providing comprehensive protection for personal data, particularly health data. In response to the threat of data breaches, Indonesia passed Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law serves as a national legal instrument that comprehensively regulates the rights of data subjects, the obligations of data controllers and processors, and sanctions for privacy violations. The issue of personal data protection arises from concerns about privacy violations that individuals and/or legal entities may experience. These privacy violations can result in not only material but also moral losses, such as the damage to an individual's or organization's reputation.(Utomo et al., 2020)

Numerous data breach cases, including in the healthcare sector, highlight the weaknesses of the data protection system prior to the introduction of specific regulations. In this context, the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) marks a significant milestone in the development of the data protection system in Indonesia. This law provides a national legal framework governing the rights of data subjects, the obligations of data controllers and processors, and law enforcement mechanisms in the event of violations.

Law Number 27 of 2022 concerning Personal Data Protection which was ratified on October 17, 2022 was born from considerations mandated in the 1945 Constitution of the Republic of Indonesia. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia states that, "Everyone has the right to protection of themselves, their families, their honor, their dignity and their property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a human right." This confirms that all citizens without exception have the right to protection of themselves, their families, their honor, their dignity and their property under their control. The right to personal data is a property right inherent in every individual as a subject of personal data. Personal data protection applies to every individual, both Indonesian citizens and foreign citizens in Indonesia, relating to all processing of personal data, including collection, use, storage, transmission, and deletion.(Vania et al., 2023)

Law Number 27 of 2022 concerning Personal Data Protection also classifies health data as specific or sensitive personal data, requiring stricter protection. Therefore, this law should be a tool capable of controlling and mitigating patient data leaks. However, the effectiveness of the protection provided by the state through this law remains questionable, given the significant implementation challenges, including legal awareness, infrastructure readiness, and oversight.

Regulations intended as mechanisms for protecting personal data within the framework of fulfilling the right to privacy are reflected in several regulatory models established by various parties, including international organizations, such as the European Union, the Organization for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), and the Economic Community for West African States (ECOWAS). Furthermore, the diverse models of personal data protection in several countries around the world also enrich

the treasury of regulatory models themselves. These various regulatory models demonstrate the crucial role of personal data protection for human rights. These regulatory models for personal data protection also address issues related to oversight of the management of the personal data in question. Furthermore, redress mechanisms for victims of violations of the right to privacy regarding their personal data are also an important part of data protection.(Djafar et al., 2016)

With the ratification of the Law on Personal Data Protection, it is hoped that it will protect the basic rights and freedoms of citizens regarding the protection of personal data, improve legal protection regarding personal data, provide legal certainty in the event of violations regarding the use of personal data, ensure organizational compliance, especially for the health sector which processes a lot of patient personal data.

Based on these conditions, it is important to examine the government's role, through Law Number 27 of 2022 concerning Personal Data Protection, in controlling personal data leaks, and the legal protection of patient privacy in Indonesia within the framework of human rights and state responsibility.

Based on the explanation above, the formulation of the problem raised is:

1. How does the government, through personal data protection laws, control personal data in the event of a personal data leak?
   What legal protection is provided for patient privacy in Indonesia?

METHOD

This research uses a normative legal approach, a legal research method based on the study of applicable positive legal norms. This approach was chosen because the primary focus of this research is to examine the role of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in providing legal protection for patient privacy, particularly in the context of personal data leaks in the healthcare system. This research relies on a review of statutory regulations as the primary source of law. Therefore, this study will examine various regulations governing personal data protection, patient privacy, and the right to confidentiality of health information. This approach is supported by a statute approach and a conceptual approach.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations that serve as the legal basis for personal data protection and patient privacy rights. Secondary legal materials include legal literature, scientific journals, legal expert opinions, and other relevant publications. Tertiary legal materials are used to strengthen understanding of specific legal terms or concepts that are key to the discussion. All legal materials are analyzed using qualitative descriptive analysis methods, which aim to systematically and logically describe the content of legal norms and evaluate how these norms are implemented in patient data protection practices. Through this approach, it is hoped that a comprehensive understanding of how Law Number 27 of 2022 concerning Personal Data Protection functions as a shield for patient privacy protection and its effectiveness in addressing the challenges of personal data leaks in the healthcare sector will be achieved.

RESULTS AND DISCUSSION

Control of Personal Data by the Government in the Event of a Personal Data Leak in the Light of the Personal Data Protection Act.

Information technology is now capable of collecting, storing, sharing, and analyzing data. These activities have resulted in various sectors of life utilizing information technology systems, such as the implementation of electronic commerce (e-commerce) in the trade/business sector, electronic education (e-education) in education, electronic health (e-health) in health, electronic government (e-government) in government, search engines, social networks, smartphones and mobile internet, and the development of the cloud computing industry.(Wulansari, 2020)Increasingly sophisticated technological developments pose a number of new challenges, particularly regarding the enjoyment of the right to privacy. Data-driven internet technology is increasingly being used in Indonesia to meet needs, ranging from banking and healthcare to trade transactions, even online transportation, and various other activities that require the collection of personal data. This phenomenon presents unique challenges, particularly in addressing the issue of ensuring personal data protection.

At the global economic level, Indonesia is considered a country with a strategic position in international trade, including electronic transactions that allow for the increasingly widespread distribution of personal data.(Palupy, 2011)This situation has forced the Indonesian government to issue a legal product in the realm of personal data, which is currently mandated through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The Personal Data Protection Law is a legal consequence of the Indonesian government's ratification of four international conventions, namely the Universal Declaration on Human Rights; Article 12; the International Covenant on Civil and Political Rights: Article 17; the Convention on the Rights of the Child: Article 16; and the International Convention on the Protection of All Migrant Workers and Members of Their Families: Article 14. The importance and relevance of Law Number 27 of 2022 concerning Personal Data Protection are undoubtedly stated in the General Explanation of the Personal Data Protection Law, especially in relation to the protection of human rights, especially the right to privacy.(Puwa et al., 2023)

The concept of personal data protection initially developed from the idea of personal data protection as a fundamental human right, which was initiated by Warren and Brandeis, who formulated that privacy is the right to enjoy one's life and the right to be respected in one's feelings and thoughts, which should not be disturbed by other parties (right to be alone).(Mutiara & Maulana, 2020)This statement is confirmed in Article 17 of the International Covenant on Civil and Political Rights (hereinafter referred to as "ICCPR") in the General Comment Human Rights Committee No. 16 on the Right to Respect of Privacy, Family, Home, and Correspondence, and Protection of Honor and Reputation and Article 12 of the Universal Declaration of Human Rights which states that, "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."(Matheus & Gunadi, 2023)

The spread of information in the current digital era of information and communication technology is so fast, global, and cross-border, creating new challenges that increase the risk of personal data breaches and violations of privacy rights.(Muhajir, 2019)Personal data breaches are a serious threat to digital systems, particularly in sectors that process sensitive data, such as healthcare. The government, as the holder of the obligation to protect citizens' human rights, plays a central role in ensuring the security and integrity of personal data. This is normatively affirmed in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which provides a legal basis for controlling and responding to data breach incidents.

Law Number 27 of 2022 concerning Personal Data Protection positions the government, in this case the personal data protection supervisory authority, as an entity with strategic authority to ensure compliance with data protection principles. Article 57 paragraph (1) of the Personal Data Protection Law states that the supervisory authority is tasked with overseeing the implementation of personal data processing. When a data leak occurs, the government has an obligation to monitor, audit, investigate, and can impose administrative sanctions or recommend criminal sanctions if there are elements of a violation of the law. The government, which acts as a regulator, has two main responsibilities that must be fulfilled in terms of protecting the information and confidentiality of personal data of internet service users belonging to its citizens. The first responsibility is that the government must create a strong legal framework or legal regulations that regulate the legal protection of personal data confidentiality as a right to privacy. The second responsibility that must be carried out is that the government must supervise and enforce the regulations made.(Anakotta et al., 2024)

The frequent leaks of Indonesian citizens' personal data demonstrate that personal data protection remains highly vulnerable and could threaten the future growth of the digital economy. The National Consumer Protection Agency of the Republic of Indonesia stated that the various incidents experienced by Indonesia, particularly related to data breaches, have impacted not only the private sector but also the Indonesian government. This indicates that oversight and law enforcement regarding personal data protection, particularly in the e-commerce sector, still have weaknesses that need to be addressed. This statement indicates that the implementation of oversight and law enforcement in Indonesia regarding personal data protection has not yet reached its optimal level.(Matheus & Gunadi, 2023)

Therefore, in the event of a data breach, Article 46 of the Personal Data Protection Law requires data controllers to immediately notify the data owner and the supervisory authority of the incident, no later than 3 x 24 hours after the breach is discovered. The government can then take additional security measures, including temporarily suspending data processing or issuing corrective instructions to data controllers. The obligation

By law, the government is the controller of personal data, meaning any individual, public body, or international organization acting individually or collectively to determine the purposes and exercise control over the processing of personal data. Therefore, personal data controllers have the following obligations:

1) The personal data controller must have a basis for processing personal data;
2) The basis for processing personal data as referred to in paragraph (1) includes;

a. explicit valid consent from the Personal Data Subject for 1 (one) or several specific purposes that have been conveyed by the Personal Data Controller to the Personal Data Subject;
b. fulfillment of agreement obligations in the event that the Personal Data Subject is one of the parties or to fulfill the Personal Data Subject's request when entering into an agreement;
c. fulfillment of legal obligations of the personal data controller in accordance with the provisions of laws and regulations;
d. fulfillment of the protection of the vital interests of Personal Data Subjects;
e. carrying out duties in the public interest, public services, or carrying out the authority of the Personal Data Controller based on statutory regulations; and/or;
f. fulfillment of other legitimate interests by taking into account the objectives, needs and balance of interests of the Personal Data Controller and the rights of the Personal Data Subject.

Furthermore, the government as the controller of personal data is obliged and must inform application users (personal data subjects) regarding the processing of personal data based on consent, including:

a. legality of personal data processing;
b. purpose of processing personal data;
c. the type and relevance of personal data to be processed;
d. retention period for documents containing personal data;
e. details regarding the information collected;
f. personal data processing period; and
g. personal data subject rights.

In general, if listed in order, the controller of personal data, in this case the government, has obligations that must be carried out in the process of controlling personal data, including:

1) have a basis for processing personal data;
2) convey all information related to personal data;
3) show proof of consent given by the personal data subject;
4) carry out limited and specific, legally valid and transparent processing of personal data;
5) carry out processing of personal data in accordance with the purposes of processing personal data;
6) ensure the accuracy, completeness and consistency of personal data;
7) required to carry out verification;
8) update and/or correct errors and/or inaccuracies in personal data no later than 3 x 24 (three times twenty-four) hours from the time the personal data controller receives the request for updating and/or correcting personal data;
9) notify the results of updates and/or corrections to personal data subjects;
10) record all personal data processing activities;
11) provide access to personal data subjects to the personal data processed along with a track record of the processing of personal data in accordance with the period of storage of personal data;
12) refuse to provide access to changes to personal data to personal data subjects in the event of:
    a. endanger the security, physical health, or mental health of the personal data subject and/or other persons;
    b. impact on the disclosure of personal data belonging to;
    c. contrary to the interests of national defense and security.
13) conducting an assessment of the impact of personal data protection in cases where the processing of personal data has a high potential risk to the personal data subject;
14) protect and ensure the security of the personal data it processes;
15) maintain the confidentiality of personal data;
16) stop processing personal data in the event that the personal data subject withdraws consent to processing personal data;
17) terminate the processing of personal data;
18) delete and destroy personal data once it is no longer needed.
19) responsible for processing personal data and demonstrating accountability in fulfilling the obligation to implement the principles of personal data protection.

In the context of health data leaks, which are classified as specific personal data, the protection provided must be even stricter. The government also has a responsibility to ensure that all data controllers in the health sector, such as hospitals, clinics, laboratories, and digital health application providers, have implemented the data protection principles stipulated in the PDP Law, including the principles of data minimization, transparency, accountability, and security. Therefore, government control of personal data includes not only reactive post-leak measures but also preventive and corrective oversight mechanisms, to ensure the fulfillment of citizens' constitutional rights to personal data protection.

The Personal Data Protection Law provides legal legitimacy for the government to monitor, control, and enforce the law on personal data breaches. However, the effectiveness of these controls is largely determined by the institutional readiness of supervisory authorities, the compliance of data controllers, and the state's consistency in imposing sanctions against violations, ensuring that citizens' privacy rights, particularly in the healthcare sector, can be effectively and effectively realized.

Legal Protection of Patient Data Privacy in Indonesia

As a country based on law, the Indonesian government is obliged to guarantee the protection of personal data as a form of fundamental human right. This perspective is in line with Scheltema's view as stated in a quote by Ahmad Redi, who identified five main characteristics of a state based on law (State of Law/Rechtsstaat). One of these characteristics involves respecting, recognizing and protecting human rights that respect the dignity of each individual.(Redi, 2021)This mandate is also reaffirmed in Law No. 11 of 2008 concerning Electronic Information and Transactions (hereinafter referred to as "Law No. 11 of 2008"), where the Explanation to Article 26 of Law No. 11 of 2008 explains that the protection of personal data falls within the realm of personal rights, also known as the right to privacy. Most recently, with the enactment of Law No. 27 of 2022, the existence of personal data protection in Indonesia has been further strengthened as a guarantee of people's basic rights.

Privacy and personal data protection significantly impact the development of a country's digital economy, including Indonesia. This protection is a determining factor in online trust, which is crucial in digital transactions. Privacy and personal data are crucial because online users will not conduct digital transactions if they feel their privacy and personal data are threatened. One aspect of privacy and personal data protection concerns how personal data will be processed, including sensitive user data. If distributed to irresponsible parties, it could potentially cause financial losses and even threaten the owner's security and safety. Threats arising from weak privacy and personal data protection have a direct correlation with economic growth resulting from online transactions.(Dewi Rosadi & Gumelar Pratama, 2018)

The importance of personal data protection has gained traction with the rise in mobile phone and internet users. A number of emerging cases, particularly those involving personal data leaks and resulting fraud or pornography, reinforce the need for legal regulations to protect personal data. Personal data protection is closely linked to the concept of privacy, which is the concept of maintaining personal integrity and dignity.(Djafar & Komarudin, 2014)

Legal protection is implemented as a collection of rules or legal principles implemented to protect one thing from another. Regarding personal data confidentiality, the law protects the rights of internet service users from anything that could result in the non-fulfillment of those rights, in this case the confidentiality of the internet user's personal data.(Hadjon, 2007)Personal data associated with an individual is a right that must be protected. Personal data is part of a person's privacy. Generally, there are three aspects of privacy: privacy related to the individual, privacy regarding one's data, and privacy regarding one's communications.(Makarim, 2005)The use of data by a person by the government or private sector, business entity or individual without permission is a violation of a person's privacy.(Mukhtar, 2018)

Therefore, personal data must be protected, the obligation to protect personal data is reflected in the 1945 Constitution Article 28 G paragraph 1 "Everyone has the right to protection of themselves, their families, their honor, their dignity, and their property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a human right." The provisions of this article have the same meaning as the Universal Declaration of Human Rights as stated in article 12 which was later adopted in the International Covenant on Civil and Political Rights (article 17) which applies

based on Law Number 12 of 2005 concerning the Ratification of the International Covenant on Civil and Political Rights (International Covenant on Civil and Political Rights) which provides rights or guarantees for the protection of personal data.

The provisions regarding the protection of privacy and personal data are mandated by Article 28G of the 1945 Constitution of the Republic of Indonesia, which regulates the right to protection of oneself, family, honor, dignity, and property under one's authority. To be able to view these provisions as provisions regarding privacy and personal data, Warren and Brandeis's opinion in their work entitled "The Right to Privacy" states that privacy is the right to enjoy life and the right to have one's feelings and thoughts respected.(Rosadi, 2015). One important point in the context of personal data protection is how personal data protection efforts can also be a means of protecting one's privacy.(Mardiansyah, 2018)

Forms of protection can be implemented before and after the processing of personal subject data, from the protection side before the processing of personal data, it is in the form of actions such as providing security and privacy policies, implementing data encryption, implementing access control, organizing user approval and notification, to implementing data storage policies.(Anugrah et al., 2023)Meanwhile, the form of protection that can be provided after personal data has been processed is in the form of permanent deletion of personal data if there is a leak of personal data to taking full responsibility for the processing of personal data and demonstrating responsibility in fulfilling the obligation to implement the principle of personal data protection.

Personal data protection is essential because it relates to sovereignty in political and economic aspects, both on a large scale, between countries, and to the human rights of individual citizens. This includes information such as National Identity Cards (KTP), health data, bank accounts, and even individual mobility records, which are frequently used in the context of pandemic management.(Aji, 2023)Especially in Indonesia, the COVID-19 pandemic has had various impacts, not only on public health, but also on lifestyles as a result of various policies implemented by the competent authorities in handling COVID-19, such as in the economic, social, political, educational, and psychological fields.(Aspan, 2021)

Patient data privacy is a fundamental human right that cannot be diminished under any circumstances (non-derogable rights). In the context of health law, patient privacy is closely related to the principle of confidentiality of medical information disclosed by patients to healthcare professionals. This principle forms the foundation of trust in the therapeutic relationship between patients and healthcare providers. Therefore, the state has an obligation to ensure legal guarantees for the protection of patient data privacy, particularly amidst the development of digital technology that increases the risk of data misuse.

The state's obligation to protect the right to health of all citizens aligns with the WHO's statement that the state, in this case the government, has responsibility for the health of its citizens. According to the WHO, "the government has a responsibility for the health of its people, which can be fulfilled only by the provision of adequate health and social measures."(Mardiansyah, 2018)

This protection within the health sector is insufficient to address the complexities of personal data protection in digital health systems involving third parties, such as application platform providers, cloud storage, and insurance institutions. Therefore, Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) expands the scope of legal protection by designating health data as a specific type of personal data that must be processed carefully and with higher security standards.

Law Number 27 of 2022 concerning Personal Data Protection grants data subjects (in this case, patients) a number of rights, including the right to access, the right to rectify data, the right to delete data, and the right to obtain information regarding the processing of their personal data. Data controllers (such as hospitals or healthcare applications) are obligated to

securely manage and store patient data and prevent unauthorized access. In the event of a violation of these rights, Law Number 27 of 2022 concerning Personal Data Protection provides a complaint mechanism and opens up opportunities for claims for compensation, whether administrative, civil, or criminal.

In several International Conventions and international legal documents, provisions regarding the right to health are stipulated as one of the basic rights (fundamental rights) that every individual has. The provisions on the right to health, which are fundamental rights that every individual has, are stated in the preamble to the World Health Organization (WHO) Constitution, which states: The enjoyment of the highest attainable standard of health is one of the fundamental rights of every human being without distinction of race, religion, political belief, economic or social conditions.(Leary, 1994). It is understood that health, as a basic right of every individual, must be respected and fulfilled by the state without distinction of ethnicity, religion, political background, economic status, or social status. In addition to national instruments, legal protection of patient privacy is also reinforced by international principles, such as General Comment No. 14 of the UN Committee on Economic, Social, and Cultural Rights, which states that the right to health includes guarantees of confidentiality of patient medical data.

With the regulation of health data as a specific form of personal data under Law Number 27 of 2022 concerning Personal Data Protection, legal protection of patient privacy is no longer a sectoral issue but has become part of a comprehensive national data protection system. This reflects the state's recognition that medical data is not merely technical but also concerns aspects of an individual's dignity, honor, and personal confidentiality, which must be safeguarded.

Although the available legal instruments have shown significant progress in terms of normative aspects, challenges remain in implementation. Low compliance by healthcare institutions with data security standards, weak oversight, and the suboptimal function of data protection supervisory authorities are obstacles to ensuring effective protection. Therefore, legal protection of patient privacy must be supported by increased technical and institutional capacity, education for data controllers, and awareness of the importance of the right to privacy as a fundamental human right.

In this context, Law Number 27 of 2022 concerning Personal Data Protection must be understood not merely as an administrative regulation, but as a constitutional protection instrument that positions patients as legal subjects entitled to full control over their personal data. Therefore, legal responsibility for protecting patient privacy lies not only with healthcare providers but also with the state, which is obliged to guarantee the fulfillment, respect, and protection of this right through effective regulation and strict oversight. Thus, the legal protection system for patient privacy in Indonesia has been strengthened through the cross-sectoral enactment of Law Number 27 of 2022 concerning Personal Data Protection, although its effectiveness depends heavily on implementation, legal awareness of stakeholders, and the functioning of state-provided oversight mechanisms.

CONCLUSION

Law Number 27 of 2022 concerning Personal Data Protection provides a crucial legal basis for controlling and protecting citizens' personal data, including patient health data. This law affirms the state's commitment to guaranteeing the right to privacy as a constitutionally protected human right. The government, through its supervisory authorities, holds primary responsibility for ensuring data processing complies with legal principles and for imposing sanctions for any violations, particularly in cases of personal data breaches.

In the context of legal protection for patient privacy, the PDP Law expands and strengthens the legal framework, including recognition of data subject rights and the obligations of data controllers to maintain the security and confidentiality of medical information. However, implementation in the field still faces various obstacles, ranging from weak oversight infrastructure, low compliance among healthcare institutions, to a suboptimal understanding of the importance of data protection. Therefore, strategic steps are needed, including increasing legal awareness, building institutional capacity, and updating data security systems to ensure effective and sustainable protection of patient privacy.

BIBLIOGRAPHY

Aji, MP (2023). Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective (Case Study of Personal Data Protection). Journal of Politica: Dynamics of Domestic Political Problems and International Relations, 13(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Anakotta, F., Haliwela, NS, & Pariela, MVG (2024). Legal Protection for Internet Service Users Regarding Personal Data Confidentiality. PATTIMURA Legal Journal, 3(3), 205–220. https://doi.org/10.47268/pela.v3i3.17348

Anggen Suari, KR, & Sarjana, IM (2023). Maintaining Privacy in the Digital Age: Personal Data Protection in Indonesia. Journal of Legal Analysis, 6(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Anugrah, M., Syahid, MN, Sahri, Azka, FM, & Anwar, MS (2023). Legal Challenges and the Role of Government in E-Commerce Development in Indonesia. Wara Sains Journal of Law and Human Rights, 2(05), 421–438. https://doi.org/10.58812/jhhws.v2i05.354

Aspan, H. (2021). Legal Basis for the Implementation of Work from Home Amid The COVID-19 Pandemic in Indonesia. Saudi Journal of Humanities and Social Sciences, 6(4), 116–121. https://doi.org/10.36348/sjhss.2021.v06i04.002

Azwar, TKD, Barus, UM, Meher, M., & Wau, HSM (2025). Limitations on the Use of Social Media in Health Services in Terms of Legislation. Pena Justisia: Media Komunikasi Dan Kajian Hukum, 23(3), 2940–2955.

Dewi Rosadi, S., & Gumelar Pratama, G. (2018). The Urgency of Data Privacy Protection in the Digital Economy Era in Indonesia. Veritas et Justitia, 4(1), 88–110. https://doi.org/10.25123/vej.2916

Djafar, W., & Komarudin, A. (2014). Protecting the Right to Privacy on the Internet - Some Key Explanations. Elsam.

Djafar, W., Sumigar, BRF, & Setianti, BL (2016). Personal Data Protection: Proposed Policy Institutionalization from a Human Rights Perspective. Institute for Policy Research and Advocacy (ELSAM).

Hadjon, PM (2007). Legal Protection for the Indonesian People: A Study of Its Principles, Its Handling by the Courts in the General Court Environment and the Formation of Administrative Courts. Civilization.

Kusnadi, SA (2021). Legal Protection of Personal Data as a Privacy Right. AL WASATH Journal of Legal Studies, 2(1), 9–16. https://doi.org/10.47776/alwasath.v2i1.127

Leary, V. (1994). The Right to Health in International Human Rights Law, Health and Human Rights. Health and Human Rights, 1(1), 32. https://doi.org/https://doi.org/10.2307/4065261

Makarim, E. (2005). Introduction to Telematics Law. Raja Grafindo Persada.

Mardiansyah, R. (2018). Dynamics of Legal Politics in Fulfilling the Right to Health in Indonesia. Veritas et Justitia, 4(1), 227–251. https://doi.org/10.25123/vej.2918

Matheus, J., & Gunadi, A. (2023). Establishment of a Personal Data Protection Supervisory Agency in the Digital Economy Era: Comparative Study with KPPU. Justisi, 10(1), 20–35. https://doi.org/10.33506/jurnaljustisi.v10i1.2757

Muhajir, I. (2019). World Scientific Journal. World Scientific Journal of Law, 4(2528–6137), 25–36.

Mukhtar, H. (2018). Cryptography for Data Security. Deepublish.

Mutiara, U., & Maulana, R. (2020). Personal Data Protection as Part of the Human Right to Personal Protection. Indonesian Journal of Law and Policy Studies, 1(1), 42. https://doi.org/10.31000/ijlp.v1i1.2648

Palupy, HE (2011). Privacy and Data Protection: Indonesia Legal Framework. Van Tilburg University.

Puwa, SIP, Puluhulawa, FU, & Rahim, EI (2023). The Ideal Idea of Personal Data Protection Regulation as a Form of Privacy Rights in Indonesia. PALAR (Pakuan Law Review), 9(2), 25–37.

Redi, A. (2021). Law on the Formation of Legislation. Sinar Grafika.

Rosadi, SD (2015). Aspects of Personal Data Protection According to International, Regional, and National Law. Refika Aditama.

Utomo, HP, Gultom, E., & Afriana, A. (2020). The Urgency of Legal Protection of Patient Personal Data in Technology-Based Healthcare Services in Indonesia. Galuh Justisi Scientific Journal, 8(2), 168. https://doi.org/10.25157/justisi.v8i2.3479

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). A Legal Review of Personal Data Protection from the Aspects of Data Security and Cybersecurity. Indonesian Multidisciplinary Journal, 2(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157

Wulansari, EM (2020). The Concept of Personal Data Protection as a Fundamental Aspect of Norms in Protecting a Person's Right to Privacy in Indonesia. Surya Kencana Dua Journal: Dynamics of Legal and Justice Issues, 7(2), 265–289.