International Journal of Social Welfare and Family Law

E-ISSN: 3047-7727
P-ISSN: 3047-4841

# Legal Protection of Personal Health Data in Electronic Systems

**Faisal Lutfi [1*], Rahmayanti [2], Muhammad Faiz Hadi [3], Eddy [4]**

[1] Universitas Pembangunan Panca Budi, Indonesia; e-mail : faisal.lutfi.dr@gmail.com
[2] Universitas Pembangunan Panca Budi, Indonesia; e-mail : rahmayanti@dosen.pancabudi.ac.id
[3] Universitas Pembangunan Panca Budi, Indonesia; e-mail : faizhadi05@gmail.com
[4] Universitas Pembangunan Panca Budi, Indonesia; e-mail : eddyfesconsulindi@gmail.com

Alamat : Jln. Jend. Gatot Subroto Km. 4.5 Sei Sikambing 20122 Medan City, North Sumatra Province, Indonesia
* Corresponding Author : Faisal Lutfi

**Abstract:** Legal protection of personal health data amidst the rapid digitalization of health services, such as telemedicine, electronic medical records, and online consultation applications is very important. Sensitive health data requires careful management, but in fact, many digital service providers in Indonesia have not implemented adequate security standards. The case of the BPJS Kesehatan participant data leak is a real example of the weakness of the data protection system, coupled with the practice of data misuse by digital platforms without valid consent. The method used is qualitative with a normative legal approach, through a literature study of primary and secondary regulations such as Law No. 27 of 2022 concerning Personal Data Protection (UU PDP), the ITE Law, and related Government Regulations and Permenkes. The results of the study show that although regulations are comprehensively available, implementation in the field still faces serious challenges such as the lack of appointment of Data Protection Officers (DPOs), weak supervision, and low awareness of data protection. Real threats such as cyber attacks, data leaks due to negligence, and misuse by third parties are the main issues. Electronic system providers have a great responsibility in building an information security system, preparing privacy policies, and implementing the principle of "privacy by design".

**Keywords:** Data Protection, Digital Security, Electronic Systems, Health Law, Personal Health Data.

**Received: May 11, 2025**
**Revised: May 26, 2025**
**Accepted: June 25, 2025**
**Online Available: June 30, 2025**



## 1. Introduction

The development of digital technology in healthcare has accelerated the adoption of electronic-based service systems, such as telemedicine, electronic medical records (EMR), and online health consultation applications. These systems automatically rely on collecting, storing, and processing patients' personal health data in digital form. Health data is categorized as sensitive data that reflects a person's physical and mental condition, so it must be managed with the principles of prudence and high confidentiality. Unfortunately, not all digital health service providers in Indonesia have implemented adequate data protection standards.

Various cases of personal health data leakage have surfaced to the public, one of which is the leak of BPJS Health participant data, which indicates a weak cybersecurity system and weak supervision of electronic system providers in the health sector. In addition, many digital platforms such as e-commerce or online lending applications also often misuse users' personal data for business or marketing purposes without proper authorization. This not only violates individual privacy, but also poses social and psychological risks to patients as data owners.

Although Indonesia already has legal frameworks such as Law No. 27 of 2022 on Personal Data Protection, as well as the Electronic Information and Transaction Law (ITE Law), its implementation in the health sector is still not optimal. Service providers often lack a clear and accountable data protection management system. In fact, legal responsibility and accountability mechanisms for data misuse are still not regulated in detail and firmly. This causes vulnerability to leakage of sensitive and highly protected personal health data.

The urgency to review the legal protection of personal health data in electronic systems is increasing with the increasing digitization of public and private services. Leaked or misused health data can lead to discrimination, social stigma, and economic loss for individuals whose data is misused. An in-depth study is needed on how national laws regulate the responsibilities of electronic system organizers, the protection of patients' rights, and the establishment of effective supervision and sanction mechanisms.

The study on the legal protection of personal health data in electronic systems aims to identify regulatory gaps, assess the effectiveness of existing protection mechanisms, and provide normative recommendations for legislation. In addition, this study is also expected to be a reference for the formation of national policies on digital health data management based on the principles of accountability, transparency, and patient data sovereignty. In the context of information globalization, the urgency of strengthening personal data protection is an integral part of upholding human rights in the digital era.

Based on this description, the importance of researching the topic "Legal Protection of Personal Health Data in Electronic Systems" lies in the urgency to answer real challenges in the digital era, where highly sensitive health data is increasingly vulnerable to leakage, misuse, and exploitation by irresponsible parties. Incidents such as the leaking of BPJS participant data and weak supervision of online health service providers are strong signals that existing regulations and legal protection are not effective enough. This research is interesting to study because it is at the intersection of technology, law, and human rights, and has a major impact on the protection of individual privacy.

## 2. RESEARCH METHOD

The research method used in this study is a qualitative method with a normative juridical approach, combined with literature study as the main data collection technique. This research is conducted by examining various primary legal sources such as laws and regulations related to personal and health data protection, including Law No. 27 of 2022 on Personal Data Protection and Law No. 11 of 2008 on Electronic Information and Transactions (ITE), as well as secondary sources such as scientific journals, legal articles, academic papers, and relevant media reports. This approach aims to answer the formulation of the problem comprehensively, starting from analyzing the applicable legal norms, identifying forms of violation of personal health data, to assessing the responsibility of electronic system organizers in its implementation. The analysis technique used is descriptive-analytical, namely by interpreting legal data and literature to describe actual conditions and provide recommendations for solutions.

## 3. DISCUSSION

### Legal Provisions in Indonesia Regulating the Protection of Personal Health Data in Electronic Systems

Personal health data falls into the category of sensitive data because it contains detailed information about an individual's physical, mental, medical history, treatment, and biometric data. In the context of digitization of health services-such as *electronic* medical records, telemedicine applications, and online-based BPJS systems-the collection and processing of health data electronically is increasing. Therefore, clear and firm legal provisions are needed to protect patient privacy and security.

Indonesia already has several relevant legal bases to protect personal health data in electronic systems, including:

1. Law No. 27 of 2022 on Personal Data Protection (PDP Law) This law is the latest and most comprehensive regulation that regulates the rights of data subjects and the obligations of data controllers and processors, including health data as part of specific personal data (Article 4 paragraph 1 letter b). The PDP Law also requires explicit consent from data owners before data is collected, stored, or processed.
2. Law No. 11 of 2008 jo. Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law)
   Article 26 of the ITE Law emphasizes that every person has the right to the protection of their personal data in electronic systems. Any use of personal information must obtain valid consent from the data subject.
3. Minister of Health Regulation No. 269/MENKES/PER/III/2008 concerning Medical Records
   Regulates the storage and management of medical records including electronic forms. Article 10 mandates that hospitals must maintain the confidentiality of the contents of medical records, including from unauthorized access.
4. Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions
   Articles 14 to 17 of the Government Regulation regulate the obligation of electronic system operators (PSE), including in the health sector, to maintain the confidentiality and security of personal data managed.

One of the important aspects regulated in Law No. 27 of 2022 on Personal Data Protection (PDP Law) is the recognition of health data as part of specific personal data. Article 4 of the PDP Law states that special categories of personal data include health data, genetics, biometrics, and others. For this reason, processing health data requires special treatment, including explicit consent from the data owner. Data controllers are obliged to maintain the integrity, accuracy, and confidentiality of health data, and report leakage incidents within a maximum of 3 x 24 hours to the relevant authorities and data subjects.

Although these provisions are quite progressive, their implementation in the health sector still faces structural and technical obstacles. Many health facilities and digital service

applications have not appointed *Data Protection Officers* (DPOs) as mandated by the PDP Law. In fact, the existence of a DPO is crucial to ensure that the institution's internal policies run according to data protection principles, starting from collecting, storing, and destroying health data safely and legally. This unpreparedness shows that there is still a gap between regulations and implementation readiness in the field.

Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions also regulates the obligation of electronic system operators (PSE), including the health sector, to ensure system security and reliability. Articles 14 to 17 require PSEs to have information technology security mechanisms, encryption standards, and conduct periodic security audits. However, violations of these obligations have not been subject to strict enough sanctions, so there is still frequent misuse of personal data by digital-based health applications such as *e-commerce* and online lending services.

The health sector is actually also regulated through Minister of Health Regulation (Permenkes) No. 24 Year 2022 on Medical Records which replaces Permenkes 269/2008. In this new regulation, electronic medical records are legally recognized and must be equipped with an information security system that includes authentication, authorization, and audit trail. However, not all health facilities have followed this digital transformation, resulting in an imbalance in data protection between large hospitals and primary care facilities. To bridge this gap, synergy between the Ministry of Health, Ministry of Communication and Information, and the private sector is needed to establish technical standards and integrated supervision policies.

Legal provisions in Indonesia that regulate the protection of personal health data in electronic systems have actually undergone significant development, especially with the enactment of Law No. 27 of 2022 on Personal Data Protection which explicitly classifies health data as personal data that is specific and must be strictly protected. However, in practice, the implementation of this regulation still faces various obstacles, such as the low compliance of electronic system providers, the lack of cybersecurity infrastructure in the health sector, and the suboptimal role of supervision by the government. Further efforts are needed to strengthen law enforcement, clarify sanctions for violations, and build synergies between institutions to ensure more effective and comprehensive health data protection in the digital era.

**Threats and Violations of Personal Health Data in the Implementation of Electronic Systems**

In the current era of healthcare digitization, patient data is no longer only stored in physical files in hospitals, but has shifted to electronic form stored on local servers or *cloud-based* systems. While this system is efficient, the security risks to personal health data are becoming increasingly complex. Information such as medical history, genetic data, allergies, laboratory results, and psychiatric status can be accessed, transferred, or even misused if the system is not equipped with adequate security. This shows that health data security is not only a technical issue, but also involves ethics, legal protection, and public trust.

There are various forms of threats to personal health data in electronic systems, including:

1. *Cyber attacks* such as *phishing, ransomware,* and *malware* targeting hospital systems and online health applications. Global cases show that the healthcare sector is one of the main targets as the data is highly valuable in the black market.
2. Data leakage is due to internal system negligence, such as the use of unencrypted networks, weak passwords, or open access without layered authentication. This is exacerbated by the lack of cybersecurity training for healthcare workers.
3. Data misuse by third parties, such as health app developers who divert user data for commercial purposes, advertising, or even online lending without explicit consent.

Legal violations of health data usually occur when data controllers or electronic system operators (PSEs) do not comply with statutory provisions, such as:

1. The absence of explicit consent from the data subject when the data is collected or processed. This violates Article 20 of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which requires the principles of *lawfulness, fairness, and transparency*.
2. The failure of electronic system providers to report data leakage incidents to the authority and data subjects within 72 hours after they become known, as stipulated in Article 46 paragraph (1) of the PDP Law.
3. The absence of internal protection and supervision mechanisms such as the presence of a *Data Protection Officer* (DPO) in health service institutions. In fact, the presence of a DPO is a must to ensure that data governance is carried out according to the principles of privacy and security.

One concrete example is the case of data leakage of 279 million BPJS Health participants which was revealed in 2021. The leaked data included full names, NIKs, addresses, and medical histories, and were traded illegally on online forums. This case shows the weakness of the national data protection system, especially in the health sector, and the slow response of related institutions. The case has also sparked widespread concerns in the community regarding the privacy and security of personal data, and highlighted the need for stricter regulations and effective oversight of sensitive data management. In addition, the incident has become a momentum for the government and relevant agencies to immediately revise and strengthen data protection systems to prevent similar incidents in the future.

The threats and violations of personal health data in electronic systems reflect the health system's lack of readiness to adopt the principle of data *privacy by design*. Many health facilities have not implemented data encryption, double authentication, or continuous information auditing systems. In addition, awareness of privacy rights is still minimal, both among organizers and the general public. Violations that occur are often not followed by strict administrative or criminal sanctions, so they do not have a deterrent effect. In fact, health data is a much more sensitive asset than financial data or basic identity. Therefore, in addition to strengthening regulations, a multidisciplinary approach involving law, technology, and public education is needed so that health data protection is not only formal, but also substantive.

**Responsibilities and Roles of Electronic System Providers in Ensuring Security and Confidentiality of Personal Health Data**

Electronic System Providers (PSEs) play a central role in the management of personal health data because they function as data collectors, processors, storage, and managers in digital-based systems. PSEs in the context of health services can be hospitals, clinics, laboratories, *telemedicine platforms*, and health-based *mobile* applications. Given the high sensitivity of health data, the responsibilities of PSEs are not only limited to technical operations, but also include legal, ethical, and comprehensive information security aspects.

According to Law No. 27 of 2022 on Personal Data Protection (PDP Law), PSEs that act as data controllers and processors have inherent legal responsibilities. Articles 39 to 48 stipulate the obligation of data controllers to maintain the integrity, accuracy, and security of personal data, including taking appropriate technical and organizational measures to prevent leakage or unauthorized access. In addition, PSEs are required to appoint a *Data Protection Officer* (DPO) if the scale and risk of data processing is high. The DPO is tasked with ensuring internal compliance with data protection principles and liaising between the institution and the supervisory authority.

In Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions, PSEs are required to develop and implement an information security system, including physical, technical, and procedural safeguards. PSEs are also responsible for keeping access logs, conducting periodic system audits, and drafting privacy policies that are transparent and easily accessible to users.

PSE's responsibility is not only passive as a data protector, but also includes an active role in encouraging a culture of cybersecurity within its institution. PSEs need to conduct:

1. Regular education and training for health workers and IT staff on personal data management.
2. Apply the principles of *privacy by design* and *security by default* in the development of health information applications or systems.
3. Establish an incident response *system* that enables early detection and rapid response to data leakage threats.

Unfortunately, many health institutions-especially at the medium and small level-do not have adequate infrastructure and technical capacity. A study mentioned that only a small percentage of electronic system providers in the health sector have appointed DPOs and have standardized privacy policies.

The responsibility and role of PSEs in ensuring the security and confidentiality of personal health data needs to be strengthened through a combination of strict regulations, active government oversight, and internal institutional awareness. Many PSEs still consider data security as a purely technical issue, rather than a legal and ethical obligation. In fact, even the slightest negligence can have serious social and legal repercussions for patients. There is a need to reform the integrated supervision system in the future involving the Ministry of Health, Ministry of Communication and Information, and independent supervisory institutions to ensure that all electronic system providers implement equal, measurable, and sustainable data protection standards.

## 4. Conclusions

Based on the description described above, it is concluded that:

1. Indonesia has a comprehensive regulation to protect personal health data as sensitive data, especially in electronic systems. Law No. 27 of 2022 on Personal Data Protection (PDP Law) is the main legal umbrella that regulates explicit consent, security, and data integrity. Accompanied by the ITE Law, PP No. 71 of 2019, and Permenkes No. 24 of 2022, this regulation requires electronic system providers to maintain data confidentiality and security. However, its implementation still faces serious obstacles, such as unprepared infrastructure, lack of DPOs, and weak law enforcement.
2. Threats to personal health data are increasingly complex with increasing digitization. Common risks include cyberattacks (phishing, ransomware), internal system negligence, and misuse of data by third parties. Breaches include collection without explicit consent and non-reporting of data leakage incidents, such as the leak of 279 million BPJS data in 2021. Many health facilities have not implemented the security principle of *"privacy by design"*, and weak legal sanctions lead to a lack of deterrent effect against violations.
3. Electronic System Providers (PSEs) have legal and ethical responsibilities in managing health data. They must maintain data accuracy, security, and confidentiality in accordance with the PDP Law and PP No. 71/2019. PSEs must also appoint a *Data Protection Officer* (DPO), implement transparent privacy policies, and build strong digital security systems. However, many health institutions still do not meet these standards, especially small-scale ones. Collaboration between regulatory agencies as well as technical capacity building and education are needed to ensure equitable and sustainable data protection.

## References

[1] Alder, Steve. "Healthcare Data Breach Statistics." The HIPAA Journal, 2025..
[2] Ayereby, Manouan Pierre-Marius. "Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems." College of Management and Technology Walden University, 2018.
[3] Chaterine, Rahel Narda, and Dani Prabowo. "Kemenkominfo Suspects 279 Million Leaked Population Data Identical to BPJS Health Data." kompas.com, 2021. https://nasional.kompas.com/read/2021/05/21/15192491/kemenkominfo-duga-279-juta-data-penduduk-yang-bocor-identik-dengan-data-bpjs.
[4] CIPL. Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation. Pennsylvania: Center For Information Policy Leadership, 2016.
[5] Cyble. "5 Steps To Master Data Incident Response | Cyble," 2025. https://cyble.com/knowledge-hub/5-data-incident-response/.
[6] EDPS. "Data Protection Officer (DPO) | European Data Protection Supervisor," 2025. 2025.
[7] Faiqy, Muhammad Raihan, Muhammad Izzar Damargara, Muhammad Alhidayah, and Jatnika Maulana. "The Urgency of Realizing the Role of Data Protection Officer (DPO) in the Health Sector in View of Personal Data Protection Law." Padjadjaran Law Review 10, no. 1 (2022): 1–15. https://doi.org/10.56895/plr.v10i1.838.
[8] Fatmawati, Arum. "Legal Protection of User Data by Cloud Computing Service Providers in View of Law Number 11 of 2008 concerning Electronic Information and Transactions." Faculty of Social Sciences and Law, Surabaya State University, 2022.
[9] Fauzi, Elfian, and Nabila Alif Radika Shandy. "The Right to Privacy and Legal Politics of Law Number 27 of 2022 on Personal Data Protection." Journal of Lex Renaissance 7, no. 3 (2022): 445–61. https://doi.org/10.20885/JLR.vol7.iss3.art1.
[10] Haapalainen, Aleksi. "Data Privacy and Security in Healthcare Systems." Lappeenranta, Finland: Unpublished, 2024. https://doi.org/10.13140/RG.2.2.35998.55363.
[11] Hansen, Johan, Petra Wilson, Eline Verhoeven, Madelon Kroneman, and Mary Kirwan. Assessment of the EU Member States' Rules on Health Data in the Light of GDPR. Luxembourg: Publications Office of the European Union, 2021.

[12] Ministry of State Secretary RI. Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions. Jakarta: Ministry of State Secretariat of the Republic of Indonesia, 2019.
[13 Maharani, Rista, and Andria Luhur Prakoso. "Protection of Consumer Personal Data by Electronic System Operators in Digital Transactions." Journal of USM Law Review 7, no. 1 (2024): 333–47. https://doi.org/10.26623/julr.v7i1.8705.
[14] Mayasafira, Sarrah Dwiananda, and Mohammed Almansoob. "Electronic Medical Records as Digital Transformation in Indonesian Health Services 4.0." International Journal Of Nursing And Midwifery Science (IJNMS) 8, no. 2 (2024): 229-39.
[15] Indonesian Minister of Health. Minister of Health Regulation No. 269/MENKES/PER/III/2008 concerning Medical Records. Jakarta: Ministry of Health of the Republic of Indonesia, 2008.
[16] Seh, Adil Hussain, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. "Healthcare Data Breaches: Insights and Implications." Healthcare 8, no. 2 (2020): 133. https://doi.org/10.3390/healthcare8020133.
[17] RI State Secretariat. Law No. 19 of 2016 on Electronic Information and Transactions (UU ITE). Jakarta: State Secretariat of the Republic of Indonesia, 2016.
[18] ---. Law No. 27 of 2022 on Personal Data Protection. Jakarta: State Secretariat of the Republic of Indonesia, 2022.
[19] Singh, Suruchi, Bhatt Pankaj, K. Nagarajan, Neha P. Singh, and Veer Bala. "Blockchain with Cloud for Handling Healthcare Data: A Privacy-Friendly Platform." Materials Today: Proceedings 62, no. 7 (2022): 5021–26. https://doi.org/10.1016/j.matpr.2022.04.910.
[20] Utomo, Handryas Prasetyo, Elisatris Gultom, and Anita Afriana. "The Urgency of Legal Protection of Patient Personal Data in Technology-Based Health Services in Indonesia." Galuh Justisi Scientific Journal 8, no. 2 (September 13, 2020): 168–85. https://doi.org/10.25157/justisi.v8i2.3479.