JISS Jurnal Indonesia Sosial Sains
Vol. 7, No. 5, May 2026
E-ISSN:2723 – 6692 P-ISSN:2723– 6595
http://jiss.publikasiindonesia.id/

Legal Protection of Patient Personal Data in Telemedicine Practice: Aligning the Health Law and the Personal Data Protection Law

Agus Arya Mahottama*, I Gde Sastra Winata
Universitas Udayana, Indonesia
Email: arya.mahottamaa@gmail.com*, dr.sastrawinata@gmail.com

Keywords:
Telemedicine; Personal Data Protection; Health Law; PDP Law; Data Breach

Abstract
Digital transformation in Indonesia's health sector has accelerated the adoption of telemedicine services as an alternative to remote medical services. Although these services provide efficiency and expand healthcare access for the broader community, the practice of telemedicine raises serious juridical challenges, particularly regarding the protection of highly sensitive patient personal data. This research aims to analyze the juridical aspects of patient personal data protection in telemedicine services and examine the urgency of synchronizing the Health Law and the Personal Data Protection Law (PDP Law). Using a normative juridical legal research method with statutory and conceptual approaches, the findings indicate that a legal framework is available in Indonesia through Law No. 17 of 2023, Law No. 27 of 2022 (PDP Law), and Minister of Health Regulation No. 20 of 2019. However, there are regulatory inconsistencies, a void of technical norms, as well as weak infrastructure and human resource awareness that make patient data vulnerable to leaks. The synchronization of regulations and the adoption of international standards such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act) are urgently needed to create legal certainty, guarantee medical data confidentiality, and provide maximum protection for patients and healthcare workers.

INTRODUCTION

The development of digital technology has brought significant changes in health services, one of which is the emergence and growth of telemedicine services in Indonesia. Telemedicine is a technology-based remote health service that allows patients and healthcare professionals to connect without the need for face-to-face contact (Nadiroh & Wiraguna, 2025). These services are becoming increasingly relevant and urgent to implement, especially as Indonesia faced the COVID-19 pandemic, which limited people's mobility and demanded adaptation within conventional healthcare systems (Aisyah et al., 2023; Harapan et al., 2023; Sutrisni et al., 2023). Data shows that in 2019, the number of telemedicine service users in Indonesia was only around two million people, but during the pandemic it jumped dramatically to reach 20 million users in 2020 (Nadiroh & Wiraguna, 2025).

Post-pandemic, the public and healthcare professionals have begun to become accustomed to virtual consultations, so telemedicine is no longer considered merely an alternative solution but has become part of a sustainable and integrated healthcare system (Filkins et al., 2016; Hock et al., 2020; Rockwern et al., 2021). Telemedicine provides tangible benefits in the form of time and cost efficiency, reduced queue density in health facilities, and improved access for people living in remote areas or in underdeveloped, frontier, and outermost

(3T) regions (Widjaja et al., 2025). Platforms are also increasingly diverse, both those initiated by the government, such as Sisrute and Sehatpedia, as well as private commercial applications such as Halodoc, Alodokter, and SehatQ (Nadiroh & Wiraguna, 2025).

However, despite these significant benefits, the transformation of digital health services has given rise to serious concerns regarding information security and privacy (Filkins et al., 2016; Rockwern et al., 2021). The process of collecting, storing, and managing electronic medical data is vulnerable to data leakage and misuse if it is not regulated by a robust security framework (Widjaja et al., 2025). This is evidenced by a series of data breach incidents in recent years. One of the most striking cases occurred in early 2022, when medical record data belonging to approximately six million COVID-19 patients, containing 720 GB of data, was leaked and circulated online. The leak was also followed by an incident involving the e-HAC system, which exposed the personal data of more than one million people (Nadiroh & Wiraguna, 2025).

The Indonesian government has provided legal instruments to address this issue. The ratification of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is an important milestone in safeguarding citizens' privacy rights (Nadiroh & Wiraguna, 2025). The PDP Law complements existing regulations such as Law Number 17 of 2023 concerning Health and the Regulation of the Minister of Health Number 20 of 2019 concerning the Implementation of Telemedicine Services. However, the implementation of these various regulations at the operational level still faces harmonization challenges and regulatory overlap (Challapalli, 2023; Hock et al., 2020; Pombo et al., 2016; Raut et al., 2023).

Therefore, this research aims to analyze existing weaknesses and strengths within the legal framework, as well as to formulate the urgency of synchronization between the Health Law and the PDP Law to create a safe, ethical, and comprehensive telemedicine patient data protection framework. The benefits of this research are threefold. First, theoretically, this study contributes to the development of health law and data protection scholarship by integrating normative legal analysis with comparative insights from international standards such as GDPR and HIPAA, particularly in the under-researched context of telemedicine data governance in Indonesia (Francis & Jones, 2025; Narayana, 2024). Second, practically, the findings provide strategic recommendations for policymakers, including the Ministry of Health and the Ministry of Communication and Digital Affairs, in formulating derivative regulations, technical standards, and oversight mechanisms to close regulatory gaps and prevent patient data breaches (Holl et al., 2024; Nooren et al., 2018; Zhang et al., 2025). Third, institutionally, this research offers guidance for healthcare facilities and telemedicine platform providers in designing compliant data protection systems, appointing Data Protection Officers (DPOs), and implementing cybersecurity protocols aligned with both the Health Law and the PDP Law, thereby ensuring legal certainty and maximum protection for patients and healthcare workers.

METHOD

This research used a normative legal approach, which is an approach that focuses on the study of legal norms written in laws and regulations, legal principles, and doctrines developed in legal science (Nadiroh & Wiraguna, 2025). This method used a literature review to analyze regulations governing the protection of patients' personal data in telemedicine services in Indonesia (Widjaja et al., 2025).

The approaches applied in this study included a statute approach and a conceptual approach. The statute approach was used to examine positive legal norms such as Law Number 29 of 2004 concerning Medical Practice, Law Number 36 of 2009 and its amendments in Law Number 17 of 2023 concerning Health, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), and Law Number 27 of 2022 concerning Personal Data Protection (Pradana & Silalahi, 2024; Alfarizi & Listyaningrum, 2025). Meanwhile, the conceptual approach examined the theory of patient autonomy, the principle of data privacy, and the theory of social contract in the doctor–patient relationship (Alfarizi & Listyaningrum, 2025), as well as compared international data protection principles such as the GDPR and HIPAA (Ariyanto et al., 2025).

The data used were secondary data consisting of primary legal materials (laws and regulations) and secondary legal materials (scientific journals, articles, and official documents). Data collection was carried out through a literature study, which was then analyzed using descriptive qualitative methods to describe, compare, and interpret legal provisions to identify regulatory gaps and implementation challenges in practice (Widjaja et al., 2025).

This research used qualitative normative analysis with five stages: material reduction, interpretation (grammatical, systematic, teleological, and comparative), systematization, regulatory gap analysis, and deductive conclusion drawing to examine patient data protection in telemedicine. To ensure validity, this research used source triangulation by comparing primary, secondary, and tertiary legal materials, as well as theoretical triangulation by applying multiple legal perspectives (patient autonomy, data privacy, and social contract theory) to interpret the same legal phenomenon.

RESULTS AND DISCUSSIONS

The Landscape and Dynamics of Telemedicine Practice in the Digital Era

Telemedicine is defined as the implementation of remote health services carried out by health professionals by utilizing information and communication technology (Widjaja et al., 2025). These services allow the exchange of diagnosis, treatment, disease prevention, and evaluation information without the need to be physically present in a medical facility. According to the Regulation of the Minister of Health Number 20 of 2019, telemedicine is explicitly defined as remote health services that are organized to support health services carried out by other health care facilities (Bonsapia & Jumiran, 2025).

There are complex dynamics between institutional and commercial telemedicine:

1. **Institutional Telemedicine:** Refers to the interaction between formal health service facilities (such as health centers and referral hospitals) that are under the strict supervision of the Ministry of Health. This model guarantees that services meet medical standards and professional ethics because they are managed by an officially licensed facility (Bonsapia & Jumiran, 2025).
2. **Commercial Telemedicine:** Involves direct consultation between medical personnel and patients through third-party applications such as Halodoc or Alodokter. This commercial model often operates outside the scope of the government's strict oversight, where self-practicing physicians can offer their services without directly involving formal healthcare facilities (Bonsapia & Jumiran, 2025).

This commercial telemedicine practice often carries new legal risks, because regulations such as Permenkes 20/2019 do not specifically regulate the scope of commercial applications, making them in legally "gray" territory (Bonsapia & Jumiran, 2025).

Legal Construction of Patient Personal Data Protection

The data exchanged in telemedicine services is medical information that is of very high value and confidential. Indonesia's legal framework has provided several regulatory bases to provide protection for these data entities:

1. **Law Number 27 of 2022 concerning Personal Data Protection (PDP Law):** The PDP Law is the main legal umbrella that classifies health data as sensitive personal data (specific data) that requires stricter protection treatment than ordinary data (Pradana & Silalahi, 2024). The PDP Law stipulates that service providers are obliged to protect data from unauthorized access, disclosure, alteration, and deletion. In addition, every data collection must obtain explicit *informed consent* from the patient (Nadiroh & Wiraguna, 2025).
2. **Law Number 17 of 2023 concerning Health:** This regulation reaffirms the principle of confidentiality of personal health conditions. Article 161 paragraph (1) states that health services based on information and communication technology must meet service quality standards, personal data protection, and patient safety (Bonsapia & Jumiran, 2025).
3. **Permenkes Number 24 of 2022 concerning Medical Records:** Regulates in detail the procedures for the implementation and management of electronic medical records (Nadiroh & Wiraguna, 2025). Articles 21 to 23 require the security of digital medical records, the management of access to *log* recording, and the need to store data in an encrypted manner using information system security standards (Pradana & Silalahi, 2024).

The Urgency of Synchronization of the Health Law and the PDP Law

Although the legal framework has been formed, inconsistencies between regulations are still a serious legal loophole. The Health Law provides a general framework for the obligation to comply with professional standards, while the Minister of Health Regulation 20/2019 limits jurisdiction to only registered health facilities, and the PDP Law imposes technical standards on data protection without specific health sector guidelines (Bonsapia & Jumiran, 2025).

Synchronization is crucial in the context of digital Informed Consent. Based on Article 1320 of the Civil Code and Article 11 of the ITE Law, "click agree" or electronic signature on the telemedicine system is considered valid if it meets authentication and data integrity (Alfarizi & Listyaningrum, 2025). However, without synchronization with the PDP Law that clearly requires dynamic consent, this instant "click" mechanism can hurt the principle of transparency (Alfarizi & Listyaningrum, 2025). A study from the Law Research Institute of the University of Indonesia noted that 60% of telemedicine providers have difficulty determining operational standards for data protection due to the lack of harmonization of the Health Law and the PDP Law, especially when dealing with cross-border jurisdictions (Bonsapia & Jumiran, 2025).

Implementation Challenges and Data Leak Gaps

In the practical order, the implementation of patient personal data protection regulations faces a number of complex obstacles:

1. **Unpreparedness of Technology and Cybersecurity Infrastructure:** Many healthcare institutions, especially in remote areas, do not have adequate encrypted data storage and backup systems (Pradana & Silalahi, 2024). The BSSN report states that the healthcare sector is a major target for hacking, and health applications are particularly vulnerable to leak incidents due to weak protection against cyberattacks (Bonsapia & Jumiran, 2025).
2. **Low Digital Literacy of Human Resources:** Health workers and administrative staff often ignore cybersecurity standards, such as not using two-factor authentication or using public chat applications (such as WhatsApp) for medical consultations (Widjaja et al., 2025).
3. **Legal Vacuum:** There is no special derivative regulation (such as Government Regulation) of the PDP Law that outlines technical procedures for commercial services. The absence of minimum technical standards creates inconsistencies that weaken the legal protection of patients (Ariyanto et al., 2025).
4. **Weak Supervision and Law Enforcement:** Although the PDP Law mandates massive fines and prison sentences for data leakers (Nadiroh & Wiraguna, 2025), the implementation of these sanctions has not been effective because there is no independent and functional data protection supervisory institution in Indonesia (Ariyanto et al., 2025).

International Comparison and Efforts to Strengthen Solutions

Comparative evaluation of international regulations such as the European Union's General Data Protection Regulation (GDPR) and the United States' Health Insurance Portability and Accountability Act (HIPAA) provides perspective for strengthening the national legal system (Ariyanto et al., 2025).

1. **Technical and Administrative Standards (HIPAA):** HIPAA has Security Rules that detail the absolute use of end-to-end encryption technologies, multifactor authentication, and system log monitoring. Indonesia must develop similar guidelines through the Ministry of Health (Ariyanto et al., 2025).
2. **Law Enforcement and Fines (GDPR):** GDPR can provide a deterrent effect with sanctions of up to €20 million or 4% of global turnover. In addition, the GDPR requires the appointment of an explicit Data Protection Officer (DPO) (Ariyanto et al., 2025).
3. **Institutional Solutions:** Hospitals and telemedicine platforms are required to appoint Data Protection Officers (DPOs) to oversee data compliance governance. This supervision must be combined with the preparation of Standard Operating Procedures (SOPs) and the implementation of regular cybersecurity audits (Pradana & Silalahi, 2024).
4. **Technology Solutions:** Technological adaptations such as encryption and blockchain will ensure transparent data log accountability (Ariyanto et al., 2025).

CONCLUSION

Based on the normative juridical analysis, the protection of patients' personal data in telemedicine practice in Indonesia remains in a transitional phase and requires systemic strengthening. Although a solid legal framework has been established through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), Law Number 17 of 2023 concerning Health, and related Minister of Health regulations, their implementation is still not optimal. Key challenges include regulatory gaps in commercial telemedicine platforms, overlapping institutional authority, weak cybersecurity infrastructure, and low digital literacy among healthcare workers. In addition, inconsistencies between the Health Law, which emphasizes clinical service delivery, and the PDP Law, which imposes strict privacy standards, have created legal loopholes that contribute to recurring medical data breaches. Therefore, stronger regulatory harmonization is urgently needed through comprehensive derivative regulations, stricter sanctions and operational standards aligned with international benchmarks such as GDPR and HIPAA, the establishment of an independent data protection supervisory authority, mandatory appointment of Data Protection Officers (DPOs) in telemedicine providers, and routine cybersecurity compliance audits. Future research is suggested to empirically examine the effectiveness of these legal frameworks in practice, particularly through case studies of telemedicine platforms and user experiences, as well as to assess the readiness of Indonesia's digital health infrastructure in implementing full-scale personal data protection compliance.

REFERENCE

Aisyah, D. N., Lokopessy, A. F., Naman, M., Diva, H., Manikam, L., Adisasmito, W., & Kozlakidis, Z. (2023). The use of digital technology for COVID-19 detection and response management in Indonesia: Mixed methods study. *Interactive Journal of Medical Research, 12*(1), e41308.

Alfarizi, L. M., & Listyaningrum, N. (2025). Analisis hukum terhadap informed consent dalam tindakan medis di era digital. *Ganec Swara, 19*(4), 1557–1560.

Ariyanto, A., Rezi, & Maryono. (2025). Analisis kelemahan dan kekuatan UU No. 27 Tahun 2022 dalam melindungi data pribadi pasien telemedicine. *Prosiding Nasional LABEL: Law, Accounting, Business, Economics, and Language, 2*(1), 15–26.

Bonsapia, M., & Jumiran. (2025). Aspek hukum telemedicine di Indonesia. *Jurnal Ilmu Hukum The Juris, 9*(1), 259–268.

Challapalli, S. (2023). Benefits and constraints associated with the harmonization of financial regulations: An overview. *Asian Journal of Economics, Business and Accounting, 23*(15), 49–56.

Filkins, B. L., Kim, J. Y., Roberts, B., Armstrong, W., Miller, M. A., Hultner, M. L., Castillo, A. P., Ducom, J.-C., Topol, E. J., & Steinhubl, S. R. (2016). Privacy and security in the era of digital health: What should translational researchers know and do about it? *American Journal of Translational Research, 8*(3), 1560–1580.

Francis, O. H. U., & Jones, L. A. (2025). Predictive behavioral risk intelligence: An AI framework for insider threat detection based on cognitive and psychological indicators. *RAIS Journal for Social Sciences, 9*(2), 108–132.

Harapan, B. N., Harapan, T., Theodora, L., & Anantama, N. A. (2023). From archipelago to pandemic battleground: Unveiling Indonesia's COVID-19 crisis. *Journal of Epidemiology and Global Health, 13*(4), 591–603.

Hock, S. C., Kian, S. M., & Wah, C. L. (2020). Global challenges in the manufacture, regulation and international harmonization of GMP and quality standards for biopharmaceuticals.

Generics and Biosimilars Initiative Journal, 9(2), 52–64.
Holl, F., Kircher, J., Hertelendy, A. J., Sukums, F., & Swoboda, W. (2024). Tanzania's and Germany's digital health strategies and their consistency with the World Health Organization's global strategy on digital health 2020–2025: Comparative policy analysis. *Journal of Medical Internet Research, 26*, e52150.
Nadiroh, A., & Wiraguna, S. A. (2025). Analisis yuridis kebocoran data di layanan kesehatan digital: Studi kasus aplikasi telemedicine di Indonesia. *Media Hukum Indonesia (MHI), 2*(6), 313–320.
Narayana, S. (2024). *Myresearchgo, October issue 7, 2025*. Myresearchgo.
Nooren, P., Van Gorp, N., van Eijk, N., & Fathaigh, R. Ó. (2018). Should we regulate digital platforms? A new framework for evaluating policy options. *Policy & Internet, 10*(3), 264–301.
Pombo, M. L., Porrás, A., Saidon, P. C., & Cascio, S. M. (2016). Regulatory convergence and harmonization: Barriers to effective use and adoption of common standards. *Revista Panamericana de Salud Pública, 39*, 217–225.
Pradana, Y. A., & Silalahi, W. (2024). Implementasi dan tantangan regulasi perlindungan data pribadi pasien di era digital pada rumah sakit. *Rewang Rencang: Jurnal Hukum Lex Generalis, 5*(12).
Raut, N., Bajaj, K., Matte, P., Vhora, M., Kale, V., Umekar, M., & Harane, S. (2023). Building bridges: Harmonization efforts for enhanced collaboration between developed and developing countries. *International Journal of Drug Regulatory Affairs, 11*(3), 68–79.
Rockwern, B., Johnson, D., Snyder Sulmasy, L., & Medical Informatics Committee and Ethics, Professionalism and Human Rights Committee of the American College of Physicians. (2021). Health information privacy, protection, and use in the expanding digital health ecosystem: A position paper of the American College of Physicians. *Annals of Internal Medicine, 174*(7), 994–998.
Sutrisni, I. A., Kekalih, A., Friska, D., Timoria, D., Limato, R., Dien, R., Bogh, C., Chambers, M., Lewycka, S., & Van Nuil, J. I. (2023). Indonesian healthcare professionals' experiences in rural and urban settings during the first wave of COVID-19: A qualitative study. *PLoS ONE, 18*(7), e0288256.
Widjaja, G., Wagiman, Yustanti, D. E., Sijabat, H. H., & Dhanudibroto, H. (2025). Implementasi perlindungan data pribadi pasien dalam layanan telemedicine di Indonesia: Analisis regulasi dan tantangan praktis. *JK: Jurnal Kesehatan, 3*(2), 148–158.
Zhang, R., Liu, L., & Wang, G. (2025). Medical policy reform in the digital age: Responding to health crises shaped by internet public opinion. *Risk Management and Healthcare Policy*, 3387–3396.