Jurnal Iman dan Spiritualitas
eISSN: 2775-4596, Vol 6, No 3, 2026, pp. 1071-1084
https://doi.org/10.15575/jis.v6i3.56030

Analysis of Patient Data Protection in Telemedicine Services in Indonesia: A Juridical-Normative Review and Literature Study

Danny Aguswahyudy Jeremy
Universitas Islam Nusantara Bandung, Indonesia
dannyaguswahyudyjeremy@gmail.com

Suggested Citation:

Jeremy, Danny Aguswahyudy. (2026). Analysis of Patient Data Protection in Telemedicine Services in Indonesia: A Juridical-Normative Review and Literature Study. *Jurnal Iman dan Spiritualitas*, Volume 6, Number 3: 1071–1084. https://doi.org/10.15575/jis.v6i3.56030

Article's History:

Received May 2026; *Revised* August 2026; *Accepted* August 2026.

Abstract:

The digital transformation of Indonesia's healthcare sector through telemedicine presents significant challenges regarding patient data protection. Despite the existence of a legal framework—including Law No. 17 of 2023 on Health, Law No. 27 of 2022 on Personal Data Protection, and Minister of Health Regulation No. 20 of 2019—the practical implementation of patient data protection remains ineffective. This study aims to conduct a normative-juridical analysis of patient data protection in Indonesian telemedicine by examining the prevailing regulatory framework and implementation obstacles. The research methodology combines a literature review with a normative-juridical approach and a comparative analysis of international standards, such as GDPR and HIPAA. The findings indicate that while Indonesian regulations have adopted fundamental data protection principles, there are significant weaknesses in oversight, the application of technical security standards, and the enforcement of sanctions. Major data breach incidents—such as the e-HAC and BPJS data leaks—underscore the lack of effective oversight and protection. Institutional, technical, legal-cultural, and bureaucratic hurdles are the primary factors contributing to this ineffectiveness. The study recommends establishing an independent supervisory body, mandating data breach notifications, implementing minimum security standards, enhancing legal literacy, and strictly enforcing sanctions to ensure sustainable and trustworthy patient data protection in telemedicine services.

Keywords: health regulation; personal data protection; telemedicine.

INTRODUCTION

The digital transformation of the healthcare sector in Indonesia is realized through the development of telemedicine services. The use of telemedicine has grown rapidly since the government officially launched it in 2020, coinciding with the outbreak of the COVID-19 pandemic. The launch was based on the provisions of regulation HK.02.01/MENKES/303/2020, which regulates the implementation of remote healthcare services as a strategy to ensure services continue to operate amidst limited physical interaction. Through this regulation, telemedicine has become a crucial instrument in supporting safer, more efficient, and more adaptive access to healthcare services during public health emergencies (Biro Komunikasi, 2023). Based on Minister of Health Regulation Number 20 of 2019 concerning the Implementation of Telemedicine Services Between Healthcare Facilities, telemedicine is defined as a form of healthcare service provided remotely by medical personnel utilizing information and communication technology. This service includes

sharing information related to the diagnosis process, treatment procedures, and prevention efforts for disease and injury. Furthermore, telemedicine also encompasses research, evaluation, and continuing education for healthcare personnel. This entire process is carried out with the aim of supporting improved health quality for both individuals and the wider community. Through the use of digital technology, telemedicine enables the delivery of medical services without requiring face-to-face contact between patients and healthcare professionals, thereby improving access and efficiency of services to meet the needs of the development of a modern healthcare system (Peraturan Menteri Kesehatan Republik Indonesia, 2019). Telemedicine technology is useful for providing equitable access and efficiency of healthcare in Indonesia.

The use of telemedicine services in Indonesia has a clear legal basis. Its legality is affirmed in Law Number 17 of 2023 concerning Health, which recognizes the use of digital technology to support medical services. Furthermore, Minister of Health Regulation Number 20 of 2019 also explicitly states that telemedicine is a form of health care that utilizes information and communication technology. Through this regulation, health care facilities throughout Indonesia are authorized to provide remote medical services. Thus, the practice of telemedicine in Indonesia is not only officially recognized but also has a normative basis that governs its use to support more efficient and accessible health care (UUD, 2023). The development of digital transformation facilitates access to various data-based information, including sensitive health data that must be kept confidential. When data leaks occur, data owners can suffer significant losses. Various forms of cybercrime, such as hacking, fraud, wiretapping, and data manipulation, often arise as a consequence of personal information leaked via the internet. This situation indicates that risks to medical data security are increasing along with the intensity of digital technology use. Therefore, the existence of regulations governing patient data protection is crucial. Strong and comprehensive regulations are needed to ensure that health data remains secure and is not misused, thus ensuring patient privacy rights remain protected in the era of technology-based healthcare (Annan, 2024).

Amidst these technological advances, new challenges related to protecting patient privacy are becoming increasingly complex. Weaknesses in the management and security of health data in telemedicine services in Indonesia are evident in various cases of information leaks, including the leak of Electronic Health Alert Card (e-HAC) data and medical records of COVID-19 patients. These incidents demonstrate that data protection systems remain inadequate. Misuse of health data can trigger serious consequences, ranging from identity theft and financial fraud to discriminatory treatment. Furthermore, victims can experience psychological distress due to the dissemination of sensitive information that should be kept confidential. This situation demonstrates the importance of strengthening health data security mechanisms to effectively prevent risks to patients (Nadiroh et al., 2025). Health data protection is now a global issue receiving significant attention. Internationally, the European Union has classified medical information as a category of data requiring the strictest protection through the General Data Protection Regulation (GDPR). This regulation establishes important principles such as fairness, openness, and the requirement to obtain clear consent from data owners before information is processed. The GDPR also emphasizes the principle of data minimization, namely collecting only the information that is absolutely necessary. Furthermore, this regulation requires data controllers to report any breaches or breaches to regulatory authorities and to data owners within a specified timeframe. All of these provisions are designed to ensure that medical data is processed securely, responsibly, and remains under the control of the individual who owns the information (Union, 2016). Similarly, the Health Insurance Portability and Accountability Act (HIPAA) in the US establishes strict guidelines for the availability, confidentiality, and integrity of electronic protected health information (ePHI). Violations of these guidelines can result in severe penalties and the implementation of robust administrative, technical, and physical safeguards (Department & Services, 1996).

Patient data protection in telemedicine services in Indonesia is still in its early stages of development. Compared to international standards, several gaps remain that need to be addressed, both in terms of regulation, technological capacity, and the legal culture of the community and healthcare providers. This research focuses on a juridical-normative analysis of patient data protection in telemedicine practices in Indonesia by examining applicable legal regulations, assessing the effectiveness of their implementation, and identifying various obstacles and challenges that arise in their implementation. The purpose of this

research is not only to provide a more comprehensive understanding of the current regulatory environment but also to strengthen public trust in digital-based healthcare services. Furthermore, this research aims to produce applicable recommendations so that the telemedicine system in Indonesia can develop sustainably, safely, and equitably. Protecting patients' personal information is a crucial part of fulfilling the right to privacy. Given the highly sensitive nature of medical data, it requires stricter security standards than other personal data. Therefore, healthcare providers are obligated to professionally maintain the confidentiality of patient data, ensuring that it is not misused and remains protected throughout every digital management and transmission process (Childress & L.Beauchamp, 2019).

The use of digital technology in healthcare delivery in Indonesia has a clear legal basis. The main framework governing this is stipulated in Law Number 17 of 2023 concerning Health, which legitimizes the use of digital systems in various forms of medical services. Furthermore, the protection of personal data processed in digital services, including medical data, is regulated in more detail in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law establishes principles and standards that must be adhered to in the management, storage, and processing of personal data, particularly sensitive data such as health information. Through these two regulations, the government emphasizes the importance of securing patient data while ensuring that the use of digital technology in healthcare continues to operate safely, in a structured manner, and in accordance with privacy principles. Therefore, this legal basis serves as a key foundation for realizing more reliable and accountable technology-based medical services (UUD, 2022).

In various international legal instruments, the protection and confidentiality of patient data are closely monitored. Health information is categorized as sensitive data requiring special protection, as stipulated in the General Data Protection Regulation (GDPR), which the European Union has implemented since 2016. In the United States, medical data protection is regulated through the Health Insurance Portability and Accountability Act (HIPAA) of 1996. This regulation establishes standards for the security, availability, and integrity of electronic health data, or electronic Protected Health Information (ePHI), requiring all health data management to meet strict technical and procedural requirements. Over the past five years, several studies have emphasized the growing urgency of data privacy issues in telemedicine in Indonesia. Murima, Sari, and Handayani, for example, demonstrated that the increased use of telemedicine services during the COVID-19 pandemic was not matched by adequate data security infrastructure (Murima et al., 2022). Although the introduction of the Personal Data Protection Law (PDP Law) represents a significant advancement in Indonesia's legal system, its implementation is still considered inadequate to meet global standards. A comparison of the Indonesian legal framework and the GDPR conducted by Jannah, Amboro, and Shahrullah revealed that Indonesia still has weaknesses, particularly regarding independent oversight mechanisms, which have not yet been optimally developed. These findings indicate the need for strengthening regulations and infrastructure to ensure more effective patient data protection in telemedicine and align with international practices (Jannah et al., 2024). Nadiroh and Wiraguna emphasized that cases of data breaches in telemedicine services in Indonesia demonstrate the weakness of internal oversight systems within healthcare facilities. They explained that many incidents occur due to poorly implemented data security procedures, coupled with a lack of understanding among medical personnel regarding the importance of maintaining patient information confidentiality. Lack of training and inconsistent operational standards also increase the risk of data breaches. These findings indicate that improving privacy literacy and strengthening internal control mechanisms are crucial steps to prevent misuse or unauthorized access to health data in telemedicine practices.

METHOD

This research combines a literature review with a juridical-normative approach and comparative analysis to examine the legal standards governing patient data confidentiality in telemedicine services in Indonesia. This study uses a normative legal research design, which places legal principles, norms, and regulations related to patient data protection as the primary object of analysis. Thus, this study seeks to understand how current legal provisions protect the confidentiality of medical information in the context of digital-based healthcare services. The scope of the legal materials used covers three categories. First, primary legal materials consist of Minister of Health Regulation Number 20 of 2019, Law Number 17 of 2023, Law Number 27 of 2022, and two international instruments: GDPR and HIPAA. Second, secondary

legal materials consist of previous research results, scientific journal articles, proceedings, books, news reports, and other publications discussing telemedicine, personal data protection, and medical data confidentiality. Third, tertiary legal materials consist of supporting literature explaining basic concepts and definitions within the legal realm (Ardiansyah et al., 2025).

All data were collected through a literature review. Primary legal materials were searched through official databases from the Indonesian government, the European Union, and the United States. Meanwhile, secondary and tertiary legal materials were drawn from various online sources, such as national and international journals available through Google Scholar, Scopus, and PubMed. The literature was selected based on its relevance to the topic of personal data protection and telemedicine, as well as its validity as a scientific and legal source. The research process was conducted through several systematic stages (Nugroho et al., 2020). First, the researchers identified the legal problem, namely the weak protection of patient data in telemedicine services in Indonesia. Second, the researchers collected relevant primary regulations, such as the PDP Law, the Health Law, Permenkes 20/2019, GDPR, and HIPAA. Third, secondary legal materials were collected through a search of various scientific publications. Fourth, legal materials were classified based on the categories of national regulations, international regulations, and data breach cases. Fifth, legal analysis was conducted using a descriptive-analytical and comparative approach to assess the compliance of Indonesian regulations with international standards. In the final stage, the study drew conclusions and formulated policy recommendations to strengthen health data protection in Indonesia. Data analysis was conducted using a qualitative descriptive-analytical method, in which all legal materials were analyzed in depth without statistical calculations. Several analytical techniques were applied, namely: (1) descriptive analysis to explain applicable legal provisions, (2) comparative analysis to compare the Indonesian legal framework with the GDPR and HIPAA, and (3) evaluative analysis to assess the extent to which national regulations align with or still have gaps compared to international data protection standards. With this approach, the study aims to provide a comprehensive overview of the actual state of patient data protection in telemedicine in Indonesia (Santoso et al., 2025).

RESULTS AND DISCUSSION

Legal and Ethical Protection of Patient Data in Indonesian Telemedicine

In Indonesia, patient data protection in telemedicine services has a strong legal basis through several laws and regulations. *First,* Law Number 17 of 2023 concerning Health stipulates that medical records contain various information regarding a patient's condition that must be kept confidential. This obligation is inherent in every healthcare professional and healthcare facility as part of fulfilling professional ethics. Maintaining confidentiality is not only a legal obligation but also an ethical principle to respect patient privacy and dignity in all forms of healthcare services, including those delivered digitally (Langingi, 2025).

Second, specific regulations regarding telemedicine were introduced through Minister of Health Regulation Number 20 of 2019 concerning the Implementation of Telemedicine Between Healthcare Facilities. Through this regulation, the government provides a legal basis for telemedicine practices, including consultations, diagnoses, and second opinions, conducted between healthcare facilities. This regulation stipulates the obligations of facilities sending and receiving telemedicine services to ensure that all patient information transmitted via electronic devices is managed securely. Healthcare facilities are required to implement information security standards, including mechanisms to prevent data leaks, unauthorized access, and misuse. Thus, patient data confidentiality remains protected even when services are conducted without face-to-face contact (Simatupang et al., 2023).

Third, personal data protection is more comprehensively regulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law categorizes health data as sensitive personal data and therefore requires a stricter level of protection. The PDP Law adopts internationally standardized data protection principles, such as the principle of data processing validity, fairness, limitation of purposes, minimal data collection, data accuracy, limitation of storage periods, and the obligation to maintain data integrity and confidentiality (Fauzi & Radika Shandy, 2022).

Furthermore, the principle of accountability requires every data controller, including healthcare facilities and telemedicine providers, to be responsible for the processing of the personal data they manage. The PDP Law marks a significant milestone for the Indonesian legal system, as it provides the first

regulatory framework equivalent to the European Union's General Data Protection Regulation (GDPR). This regulation provides a clearer, more structured, and more comprehensive legal framework for the protection of personal data, including medical data in telemedicine services. With the combination of health regulations and the PDP Law, Indonesia has a strong normative foundation to ensure the security, confidentiality, and ethical and responsible use of patient data in the digital age.

Challenges in Implementing Patient Data Protection in Indonesian Telemedicine

Although the legal framework governing patient data protection in telemedicine is generally considered quite comprehensive, the most prominent weakness lies in the lack of technical guidelines and operational derivative regulations. To date, telemedicine service providers are not required to meet specific standards regarding the use of encryption technology, system activity recording mechanisms (audit logs), or reporting procedures for data breach incidents. This lack of established standards leads to diverse and inconsistent data protection practices across service providers. In reality, protecting patient data privacy in telemedicine services in Indonesia still faces various obstacles. Although the legal basis has been established through Law Number 17 of 2023 concerning Health, Law Number 27 of 2022 concerning Personal Data Protection, and Minister of Health Regulation Number 20 of 2019, its implementation has not been optimal. Various factors such as limited digital infrastructure, low levels of compliance among healthcare facilities, and a weak legal culture are major obstacles to achieving ideal data protection standards. Uneven technological infrastructure, particularly in areas with limited resources, directly impacts the security of medical data transmission and storage. Furthermore, not all healthcare facilities understand or correctly implement data protection principles due to minimal oversight and a lack of clear technical guidelines. Furthermore, the evolving legal culture, including awareness among healthcare providers and personnel about the importance of patient privacy, also contributes to the uneven implementation of regulations. This situation demonstrates that, although the normative framework is quite robust, more concrete implementation steps are still needed to ensure truly effective patient data protection in telemedicine (Mannas et al., 2023).

The digital infrastructure of healthcare facilities in Indonesia remains patchy. Many hospitals and community health centers still rely on manual or semi-digital record-keeping systems, such as paper files or simple, unintegrated software. This puts patient medical records at greater risk of misuse, loss, or unauthorized access. Even in institutions that have begun adopting digital systems, security standards remain suboptimal. Critical measures such as data encryption, access rights management with dual authentication mechanisms, and user activity recording through audit logs have not been fully implemented. As a result, electronic medical records (EMD) systems, which should improve security and efficiency, continue to face significant vulnerabilities. This situation highlights the need for improved technological infrastructure and the implementation of stricter security protocols to ensure adequate protection of patient health data across all healthcare facilities (Rusman & Suwardoyo, 2022). The Ministry of Health often fails to fully monitor the deployment of private telemedicine applications. Although some applications are active, they may not always comply with patient data protection regulations, and some are not officially registered. Data breaches are more likely to occur when security certification procedures or routine audits are not implemented. From lab test results and medical photos to online discussions between patients and doctors, telemedicine apps collect a wealth of personal health information.

Cases of patient data leaks demonstrate that efforts to secure health information remain far from adequate. A major incident occurred in 2021 when approximately 1.3 million users' data was leaked and spread publicly due to a security flaw in the Electronic Health Alert Card (e-HAC) system managed by the Ministry of Health. This incident underscored the importance of digital systems that should support healthcare services, but can actually become a source of risk if they are not equipped with robust security safeguards. This leak revealed weaknesses in data management, including a lack of security verification mechanisms, minimal system monitoring, and the failure to implement security standards in accordance with international best practices. The impact not only harms users but also erodes public trust in digital healthcare services. Therefore, the e-HAC incident serves as a clear example of the importance of strengthening cybersecurity systems, increasing oversight, and implementing stricter data protection technology in the provision of telemedicine services and healthcare applications in Indonesia (BBC, 2025). Medical records of patients infected with the coronavirus were also allegedly leaked to the public shortly thereafter, raising significant concerns regarding health data protection (Kompas, 2025).

The series of data breach incidents indicates that the problem lies not only in technical weaknesses but also in the ineffectiveness of regulatory oversight mechanisms. Although legal provisions require telemedicine service providers to maintain the confidentiality of medical information, these provisions are almost never enforced when violations occur. The Personal Data Protection Law provides for fines of up to 2% of annual revenue and a maximum prison sentence of six years. However, in practice, administrative and criminal sanctions of significant severity have never been effectively enforced. This situation has led the public to believe that personal data protection remains merely an ideal norm without strong certainty of implementation. Another problem arises from weak coordination between institutions with authority in this sector. The National Agency for the Protection of National Data, the Ministry of Health, and the Ministry of Communication and Informatics are among the institutions responsible for maintaining health data security. However, to date, there has been no structured coordination mechanism to handle data breach incidents in an integrated manner. As a result, each time a breach occurs, responses between institutions tend to be siloed, often shifting responsibility. This results in cases being handled without concrete corrective measures (Pomantow et al., 2024).

In practice, a significant gap remains between legal provisions and the implementation of health data protection. Although various regulations mandate the confidentiality of patient information, their effectiveness has been limited due to weak oversight mechanisms, low cybersecurity standards in many institutions, and minimal coordination between relevant agencies. Consequently, data protection, which should be a fundamental principle of modern healthcare, often falls short of expectations. Globally, the European Union has set the highest standards through the General Data Protection Regulation (GDPR), which came into effect in May 2018. This regulation classifies health data as a special category of personal data, a type of personal data deemed highly sensitive and therefore requiring the strictest protection. Under Article 9 of the GDPR, processing of health data may only occur if there is a valid legal basis. One of the most important bases is the explicit consent of the data subject, namely the patient. Furthermore, processing may still be carried out for medical purposes, legitimate research activities, public health interests, or situations concerning the safety of individuals. This provision shows that although data processing is permitted, the GDPR ensures that any access or use of health data must be within strict legal limits and accompanied by strong accountability mechanisms, thereby preventing misuse that could harm patients (Huda et al., 2024).

The GDPR mandates that organizations managing large-scale data appoint a Data Protection Officer (DPO). This officer is responsible for acting as the official liaison between the data processing institution and the data protection authority, ensuring that all information processing activities are carried out in accordance with applicable law. The DPO also monitors internal compliance and provides advice on data protection measures. Furthermore, the GDPR requires each European Union member state to have an independent supervisory authority. This supervisory body operates within the coordination structure of the European Data Protection Board (EDPB), which serves to harmonize the implementation of the GDPR across the EU. This national authority has broad powers, including investigating suspected violations, issuing warnings or instructions for improvement, and imposing administrative sanctions. These sanctions can range from warnings to substantial fines for organizations found to be non-compliant with data protection provisions. With a strict oversight mechanism and a robust institutional structure, the GDPR is designed to ensure consistent and effective personal data protection across the EU (Faiqy et al., 2022).

The obligation to report data security incidents is a key element of the GDPR. Under Article 33, every organization or service provider is required to notify a supervisory authority of a data breach within a maximum of 72 hours of the incident being detected. Furthermore, if the breach has the potential to pose a significant risk to the rights and freedoms of individuals, affected parties must also be informed directly. This provision aims to provide the public with the opportunity to take preventative measures, increase the accountability of service providers, and encourage public transparency regarding the management of personal data (Kholis, 2025). In the United States, health data protection is more specifically regulated through the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which has a different scope than the more general GDPR. HIPAA consists of two main rules, the Privacy Rule and the Security Rule, which together form the framework for protecting health information. The Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164) establishes provisions regarding the use and disclosure of patients' Protected Health Information (PHI). This rule also gives patients the right to know, access, and control their

health data. In addition to regulating data confidentiality, the Privacy Rule emphasizes the importance of accountability for healthcare providers and all entities that manage patient information. Therefore, HIPAA strives to ensure that all parties handling PHI are subject to strict data protection standards so that the security, confidentiality, and integrity of patient health information can be consistently maintained. The Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) emphasizes electronic protected health information (ePHI) in more detail. This rule mandates healthcare providers to implement administrative (such as staff training and internal policies), technical (such as encryption, user authentication, and audit trails), and physical (such as server room access controls) safeguards to ensure the availability, confidentiality, and integrity of data (OCR HIPAA, 2025).

HIPAA also mandates the implementation of strict oversight mechanisms, including audit procedures and access control systems, that must be adhered to by all entities handling health information. These regulations ensure that all activities related to patient data are traceable and accessible only to authorized parties. In the event of a violation, HIPAA imposes significant penalties. Intentional violations can result in criminal penalties in the form of substantial fines or imprisonment, while administrative violations can incur fines of up to US$1.5 million per year, particularly if the violation occurs repeatedly or is caused by serious negligence. Compared to these international standards, Indonesia has adopted several important principles similar to the provisions of the GDPR. This is reflected in Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), which serves as the primary legal basis for the management, processing, and protection of personal data in Indonesia. The Law PDP contains fundamental principles such as the need for valid consent, limitation of processing purposes, transparency, and the right of data owners to access and correct their information. However, the implementation of the Law PDP still faces several challenges and has not yet fully met the enforcement standards set by the GDPR or HIPAA. These principles cover the need to obtain consent, the data subject's right to access and erase their data, and the data provider's obligation to protect personal data. However, there are a number of important differences:

a. Institutional: Unlike the OCR under HHS in the United States or regulatory authorities in the European Union, Indonesia does not yet have an independent regulatory authority. As a result, oversight and enforcement systems remain inadequate.
b. Data Breach Notification: The PDP Act does not specifically stipulate a mandatory notification process for data breaches within a specific timeframe, unlike the GDPR and HIPAA. As a result, instead of hearing directly from the responsible organization, the public often only learns about data breaches through the media or open forums.
c. Technology Standards: While Indonesia currently does not have any derivative regulations that establish minimum technology standards for cybersecurity in healthcare institutions, HIPAA explicitly requires technical, administrative, and physical standards to protect electronic health data;
d. Sanction Enforcement: While the PDP Law stipulates administrative fines of up to 2% of annual revenue and criminal penalties of up to IDR 6 billion, no sanctions have been implemented in cases involving significant health data breaches, such as e-HAC or BPJS. This contrasts with HIPAA, which routinely prosecutes violators annually, and GDPR, which has resulted in hundreds of fines totaling billions of euros.

Comparison with global standards shows that Indonesia is still in the early stages of adopting data protection practices consistent with international regulations. Although several regulations have been issued, their implementation is not yet supported by a mature institutional structure, strong oversight mechanisms, and consistent sanctions. Given this situation, even though a formal legal basis is in place, patient data protection in telemedicine services still faces serious vulnerabilities and has the potential to create recurring risks in the future. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is indeed a significant milestone in reforming Indonesia's legal system regarding the protection of personal information, including health data. However, its implementation in the telemedicine sector still faces various obstacles. These challenges arise from several key aspects, both structural and practical. From an institutional perspective, the lack of an independent supervisory authority has resulted in suboptimal coordination and law enforcement. Technical infrastructure remains weak, as evidenced by the lack of adequate cybersecurity standards in many healthcare facilities. Furthermore, legal awareness among

service managers and healthcare workers remains low, resulting in many data protection procedures not being properly implemented. A slow bureaucratic culture and unstandardized operational practices have also undermined the effectiveness of the PDP Law's implementation in telemedicine services. Given these conditions, improving the quality of regulation and implementation is an urgent need to ensure stronger patient data protection (Harefa et al., 2024).

From an institutional perspective, one of the main obstacles is the lack of an independent personal data supervisory authority as stipulated in the PDP Law. As of 2024, this agency still lacks a clear organizational structure, working mechanisms, or operational authority. This situation has resulted in data protection oversight functions being carried out fragmented by several agencies, such as the Ministry of Communication and Information Technology, the Ministry of Health, and the National Cyber and Crypto Agency (BSSN). Without a single agency with a single and clear mandate, inter-agency coordination often overlaps and is ineffective in addressing personal data breaches, including those involving telemedicine services. This situation stands in stark contrast to international models that have strong, centralized oversight structures. In the United States, oversight of health data falls entirely under the Office for Civil Rights (OCR), part of the Department of Health and Human Services (HHS). Meanwhile, the European Union has independent data protection authorities in each member state that operate within the GDPR framework. Both operate with clear mandates, strong investigative powers, and consistent enforcement mechanisms. The absence of a similar institution in Indonesia means that personal data protection still lacks a solid institutional basis (Matheus & Gunadi, 2023).

Technical Infrastructure: Technically, many healthcare facilities in Indonesia still lack adequate digital security systems. These systems generally lack basic security features such as firewalls, intrusion detection systems (IDS), data encryption, and multi-factor authentication, and are still manual or semi-digital. Even hospitals that have implemented electronic medical records (EMDs) sometimes lack audit logs or backup systems to monitor access. According to a 2022 assessment by the National Cyber and Cyber Security Agency (BSSN), the healthcare industry is one of the ten most vulnerable industries to cyberattacks, and attacks have increased significantly since the COVID-19 pandemic (Judijanto et al., 2025). Legal Awareness: Patients and healthcare workers' legal knowledge regarding personal data protection remains lacking. The majority of healthcare workers are aware of the ethical considerations surrounding patient confidentiality, but they are not fully aware of the legal responsibilities arising from the PDP Law. Furthermore, more than 60% of patient respondents in a 2022 survey conducted by the Institute for Policy Research and Advocacy (ELSAM) were unaware that the PDP Law protects their medical data. The public is less skeptical of health workers who violate data confidentiality due to the low level of legal knowledge (Hardisman, 2025).

From a bureaucratic cultural perspective, one of the main obstacles hampering patient data protection is the persistently strong sectoral work pattern. Within the digital health ecosystem, several institutions play roles related to personal data protection, including the National Cyber and Crypto Agency (BSSN), the Ministry of Health, and the Ministry of Communication and Informatics. However, coordination among these institutions has not been effective. When data leaks or breaches occur, the response often involves shifting responsibility without producing concrete solutions or firm legal action. This lack of a centralized coordination mechanism means that patient data protection is not viewed as a strategic national agenda, but rather as an issue handled separately by each sector. This situation ultimately weakens the consistency of oversight and reduces the effectiveness of enforcing established regulations. Without a shift in bureaucratic culture toward more integrated collaboration, digital health data protection in Indonesia will continue to face serious obstacles and will struggle to achieve expected security standards (Katharina, 2021). In practice, a number of major incidents demonstrate the weakness of health data protection in Indonesia. First, in 2021, data on approximately 1.3 million COVID-19 patients was leaked due to a security flaw in the Ministry of Health's e-HAC application. This incident demonstrated that the digital security system in place did not meet standards for protecting sensitive information. Second, in the same year, data on approximately 279 million Indonesians, including BPJS Kesehatan participants, was revealed. Despite the massive scale and widespread impact, no significant legal action or strict sanctions were imposed. These two cases illustrate that oversight and law enforcement mechanisms for data breaches are still far from adequate (Menpanrb, 2025). In 2022, a leak of COVID-19 patient medical records sparked public concern. This incident highlighted the vulnerability of health information, which should be kept confidential, to

unauthorized access, raising public concern and demonstrating the weaknesses of the medical data protection system.

The lack of firm action against a number of major violations indicates that the threat of sanctions in the PDP Law remains lex imperfecta, meaning that the regulations are in effect but have not been effectively implemented. This situation demonstrates that data protection in telemedicine services faces not only technical issues but also institutional challenges and suboptimal law enforcement. These various obstacles demonstrate the complexity of patient data privacy issues in the Indonesian telemedicine ecosystem. Problems arise from various dimensions, ranging from weak inter-institutional coordination, limited information technology capabilities, a low culture of compliance, and a lack of legal understanding among service providers. Without institutional reform, improved digital security standards, improved regulatory literacy, and consistent enforcement of sanctions, the telemedicine sector will remain one of the industries most vulnerable to data breaches. The impact of health information leaks is also extensive and goes beyond technical ones. These violations carry legal, social, economic, and even psychological consequences for patients. Considering that medical data is a very sensitive category of personal data, its misuse can trigger various serious risks, both for individuals and society at large, such as discrimination, identity fraud, mental stress, and loss of public trust in digital health services (Saraya et al., 2025).

Highly sensitive medical data, such as mental health history, HIV/AIDS status, or chronic disease conditions, can be exposed to unauthorized parties when health information is leaked. If this information is shared without the owner's consent, the impact can be very serious. Individuals whose data is leaked are at risk of unfair treatment, both in the workplace and in everyday social activities. Furthermore, exposure to such sensitive information can trigger negative stereotypes and long-lasting social stigma. This situation is not only personally detrimental but can also hinder patients' access to healthcare due to fear or shame. Thus, medical data leaks pose a real threat to the dignity, right to privacy, and social well-being of patients, highlighting the importance of stronger protection of health information in digital healthcare systems (WHO, 2021). Maintaining the confidentiality of patient information is a crucial part of respecting human rights and protecting individual dignity in the realm of health law. Therefore, any violation of patient data confidentiality is not only considered a violation of the right to privacy but also an act that undermines human dignity and worth. When a person's medical data is accessed or disseminated without permission, the impact can touch fundamental aspects of their personal lives, thus disrupting their sense of security, trust, and integrity. In other words, a breach of patient confidentiality is not simply an administrative or technical issue, but a violation of the fundamental principle of respect for human beings. Leaks of medical information can also lead to discrimination in the workplace and when applying for health insurance. For example, if a patient's medical history is disclosed, insurance companies may deny claims or increase premiums. Similarly, people with certain medical conditions may be denied promotions or even unfairly dismissed at work. The vulnerability of vulnerable groups, such as those with infectious diseases, uncommon illnesses, or mental disorders, is further increased by the structural injustices caused by these incidents (Heryana, 2021).

Identity theft is another potentially devastating consequence. Bank account registrations, loan applications, or illegal transactions in the victim's name are possible using compromised patient data. According to a 2021 Interpol study, because medical data includes comprehensive information, including names, addresses, ID numbers, insurance numbers, and medical records, its value on the black market is higher than credit card data. In addition to experiencing direct financial losses, data breach victims often face legal challenges to prove their authenticity in these illegal transactions. Medical data leaks can cause psychological impacts in addition to physical harm. Patients often feel anxious, restless, and lose trust in medical institutions and telemedicine providers. Some people are reluctant to use digital healthcare services due to the trauma of fears that their data could be exploited in the future. The goal of telemedicine, which is to increase patient accessibility and convenience, clearly conflicts with this situation (Lestari & Lestari, 2025).

In general, public trust in digital health systems can be weakened by data breaches. People tend to reject government-owned health apps, electronic medical records (EMDs), and telemedicine if they are unsure about the security of their data. Consequently, initiatives to implement digital transformation in the healthcare industry may face obstacles. This can make it more difficult for people to access healthcare services, especially in rural areas where telemedicine is most needed (Anjani & Abiyasa, 2023). Several

strategic actions can be implemented to improve patient data protection in telemedicine services in Indonesia, based on research findings and comparisons with international standards:

a. Establish an autonomous oversight body. As mandated by the PDP Law, the first step is to establish an independent oversight body for personal data protection. This body must have full authority to conduct oversight, issue permits, investigate violations, and punish violators. Oversight remains fragmented and ineffective without an independent body. Examples include the OCR within the HHS in the United States and the EDPB in the European Union (Fitrian et al., 2025).
b. Mandatory Data Breach Notification. Following the GDPR model, which requires reporting within 72 hours of discovery of a breach, Indonesia should implement mandatory data breach notification with a specified timeframe. In addition to encouraging more responsible behavior from healthcare providers, this method is crucial for protecting patients and empowering them to take preventative action. The PDP Law does not yet have a specific deadline or comprehensive procedures; it only outlines data breach notification (Raib et al., 2025).
c. Implement Minimum Security Standards. Implementing ISO/IEC 27001 (Information Security Management System) certification, governments must establish baseline security requirements for all medical institutions and telemedicine applications. IDSs, firewalls, encryption, multi-factor authentication, and audit logs are all covered by this standard. Service providers will have a robust security system that can be regularly audited if certification is required (Alam et al., 2025).
d. Digital and Legal Literacy. Improving legal and digital literacy is crucial, in addition to regulatory considerations. The public needs to be informed of their rights under the PDP Law, and healthcare workers need to be aware of their legal responsibilities regarding patient data confidentiality in the digital age (ELSAM, 2025). Hospital training, integration into medical curricula, and government public campaigns are some ways to achieve outreach programs.
e. Proportional and Firm Sanctions. Firm sanctions for data protection violations are necessary for the regulations to be effective. Although the PDP Law stipulates potential prison sentences and fines of up to IDR 6 billion (approximately US$400,000) under Article 67 paragraphs 1, 2, and 3, as well as Article 68, its implementation remains inadequate. Consistent enforcement of sanctions is needed, including the potential revocation of the operating licenses of healthcare organizations or telemedicine programs deemed negligent. Firm law enforcement will increase public trust and serve as a deterrent (Sianturi et al., 2024).
f. Regular Government Audits. Furthermore, the government must implement a regular audit system for telemedicine service providers. With an emphasis on assessing system security, regulatory compliance, and protecting patient rights, audits can be conducted by the Ministry of Communication and Information Technology, the National Agency for the Protection of National Services (BSSN), or an independent agency. To enable the public to evaluate the level of compliance of digital healthcare providers, audit results must be made public (Sari & SH, 2024).

CONCLUSION

The digital transformation of Indonesia's healthcare sector has driven the use of telemedicine as an adaptive and efficient medical service innovation. Since its legalization through Ministerial Regulation 20/2019 and its official launch during the COVID-19 pandemic in 2020, telemedicine has become a crucial instrument in maintaining the continuity of healthcare services amidst limited physical interaction. The national legal framework, particularly Health Law 17/2023 and Personal Data Protection Law 27/2022, provides legitimacy and legal principles governing the processing of health data as sensitive information that must be protected. These regulations emphasize the importance of maintaining the confidentiality, integrity, and security of patient data throughout the digital service process. Analysis shows that health data protection in telemedicine still faces significant challenges. Various data breach incidents, such as the e-HAC and COVID-19 medical record cases, have exposed systemic weaknesses in digital infrastructure, non-compliance with security standards, and minimal regulatory oversight. The absence of derivative regulations governing technical security standards, audit mechanisms, and incident reporting procedures also increases the risk of privacy breaches. This situation highlights a gap between legal norms and their implementation on the ground. Compared to international standards such as the European Union's GDPR and HIPAA in the United States, Indonesia has adopted several important

principles but lacks an independent oversight body, a mandatory incident notification mechanism, or detailed technical security standards. Therefore, patient data protection in telemedicine is still in its infancy and requires strengthening regulations, infrastructure, and a culture of compliance. The success of telemedicine depends not only on technological advancements but also on legal certainty, data security, and public trust. Comprehensive implementation measures are needed to ensure digital health services in Indonesia can develop safely, sustainably, and meet global standards.

REFERENCES

Alam, R. G. G., Hidayah, A. K., Gunawan, G., Wijaya, A., & Abdullah, D. (2025). *Manajemen Risiko Keamanan Informasi [Information Security Risk Management]*. PT. Sonpedia Publishing Indonesia.

Anjani, S., & Abiyasa, M. T. (2023). *Disrupsi Digital dan Masa Depan Rekam Medis (Kajian Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 Tentang Rekam Medis Elektronik) [Digital Disruption and the Future of Medical Records (A Review of Minister of Health Regulation Number 24 of 2022 Concerni*. Selat Media.

Annan, A. (2024). Tinjauan Yuridis Perlindungan Data Pribadi pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022 [Legal Review of Personal Data Protection in the Health Sector Based on Law No. 27 of 2022]. *Synergy: Jurnal Ilmiah Multidisiplin*, *1*(4), 247–254.

Ardiansyah, M. R., Buaton, T., & Sutrisno, S. (2025). Kewenangan Klinis dan Tanggung Jawab Hukum Dokter dalam Pelaksanaan Telemedisin ICU di Indonesia [Clinical Authority and Legal Responsibilities of Doctors in the Implementation of ICU Telemedicine in Indonesia]. *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, *8*(11), 12635–12641. https://doi.org/10.54371/jiip.v8i11.9722 [In Indonesian]

BBC, I. (2025). *Kebocoran Data 279 Juta Warga [Data Leak Affects 279 Million Citizens]*. https://www.bbc.com/indonesia/indonesia-5839334,

Biro Komunikasi, P. P. K. K. R. I. (2023). *Transformasi Kesehatan Mewujudkan Masyarakat Indonesia Sehat dan Unggul [Health Transformation: Creating a Healthy and Superior Indonesian Society]*. Kementerian Kesehatan RI.

Childress, J. F., & L.Beauchamp, T. (2019). *Principles of Biomedical Ethics* (8th ed.). Oxford University Press.

Department, U. S., & Services, H. and H. (1996). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. HHS.

ELSAM. (2025). *Rendahnya Kesadaran Privasi dan Pentingnya Regulasi Pelindungan Data Pribadi [Low Privacy Awareness and the Importance of Personal Data Protection Regulations]*. https://www.elsam.or.id/bisnis-dan-ham/rendahnya-kesadaran-privasi-dan-pentingnya-regulasi-pelindungan-data-pribadi.

Faiqy, M. R., Damargara, M. I., Alhidayah, M., & Maulana, J. (2022). Urgensi Realisasi Peran Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi [The Urgency of Realizing the Role of Data Protection Officers (DPOs) in the Health Sector in the Light of Personal Data Protection La. *Padjadjaran Law Review*, *10*(1). https://doi.org/10.56895/plr.v10i1.838 [In Indonesian]

Fauzi, E., & Radika Shandy, N. A. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi [The Right to Privacy and Legal Politics Law Number 27 of 2022 concerning the Protection of Personal Data]. *Jurnal Lex Renaissance*, *7*(3), 445–461. https://doi.org/10.20885/JLR.vol7.iss3.art1 [In Indonesian]

Fitrian, A., Akhyar, C. F., Ibrahim, M., Yuliana, T., Riancana, R., Pakarti, M. H. A., & Herniati. (2025). *Hukum Perdata Dan Hak Asasi Manusia: Menjamin Keadilan Individu [Civil Law and Human Rights: Ensuring Individual Justice]*. PT. Nawala Gama Education.

Hardisman. (2025). *Pendekatan Kontemporer Etika dan Hukum Kesehatan [Contemporary Approaches to Health Ethics and Law]*. wawasan Ilmu.

Harefa, J. E., Pandia, E. V. A. P., Situmorang, A. S., & Rumapea, M. S. (2024). Analisis Perbandingan Penegakan Hukum Pidana Korupsi Di Indonesia Dengan Singapura: Pendekatan Normatif Terhadap Kriteria Keberhasilan Penindakan Korupsi [Comparative Analysis of Corruption Criminal Law Enforcement in Indonesia and Singapore: A Normative . *Ilmu Hukum Prima (IHP)*, *7*(1), 97–109. https://doi.org/10.34012/jihp.v7i1.5135 [In Indonesian]

Heryana, A. (2021). Asuransi Kesehatan & Managed Care [Health Insurance & Managed Care]. In *Universitas Esa Unggul*.

Huda, H. U. N., Astaruddin, H. T., Nasution, M. I., Haddad, A. Al, & Gumelar, D. R. (2024). *Data Pribadi, Hak Warga, dan Negara Hukum: Menjaga Privasi di Tengah Ancaman Digital [Personal Data, Citizen Rights, and the Rule of Law: Maintaining Privacy Amidst Digital Threats]*. Penerbit Widina.

Jannah, M., Amboro, F. Y. P., & Shahrullah, R. (2024). Personal Data Protection in Telemedicine: Comparison of Indonesian and European Union Law. *Journal of Law and Policy Transformation*, *8*(2), 145. https://doi.org/10.37253/jlpt.v8i2.8827

Judijanto, L., Pasrun, Y. P., Rohman, T. B., Sudipa, I. G. I., Selviana, R., Pandawana, I. D. G. A., Listartha, I. M. E., Rusdianto, D., Salsabila, Z., & Nirsal, N. (2025). *Sistem Informasi: Teori dan Penerapannya di Berbagai Bidang [Information Systems: Theory and Its Application in Various Fields]*. PT. Sonpedia Publishing Indonesia.

Katharina, R. (2021). *Pelayanan Publik & Pemerintahan Digital Indonesia [Public Services & Digital Government of Indonesia]*. Yayasan Pustaka Obor Indonesia.

Kholis, I. M. (2025). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia [Personal Data Protection and Cybersecurity in the Banking Sector: A Critical Study of the Implementation of the PDP Law and the I. *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, *4*(2), 275–299. https://doi.org/10.14421/t5sfe747 [In Indonesian]

Kompas. (2025). *Data Rekam Medis Pasien Covid-19 Diduga Bocor, Segera Tuntaskan RUU Perlindungan Data Pribadi [COVID-19 Patient Medical Records Allegedly Leaked, Urgent Finalization of Personal Data Protection Bill]*. https://www.kompas.id/artikel/data-rekam-medis-pasien-covid-19-diduga-bocor-segera-tuntaskan-ruu-perlindungan-data-pribadi,

Langingi, A. R. C. (2025). *Manajemen Informasi Kesehatan: Fondasi, Strategi, dan Inovasi Digital dalam Dunia Akademik dan Klinik [Health Information Management: Foundations, Strategies, and Digital Innovations in Academic and Clinical Practices]*. Goresan Pena.

Lestari, R. A., & Lestari, N. M. (2025). Fraud Dalam Implementasi Kartu Pembiayaan Bank Syariah: Tantangan Dan Konstruksi Perlindungan Hukum Bagi Nasabah [Fraud in the Implementation of Islamic Bank Financing Cards: Challenges and the Construction of Legal Protection for Customers]. *ISTIKHLAF: Jurnal Ekonomi, Perbankan Dan Manajemen Syariah*, *7*(1), 44–66. https://doi.org/10.51311/istikhlaf.v7i1.746 [In Indonesian]

Mannas, Y. A., Elvandari, S., & Elvandari., S. (2023). *Aspek Hukum Telemedicine di Indonesia [Legal Aspects of Telemedicine in Indonesia]* (Vol. 9, Issue 1). PT. RajaGrafindo Persada-Rajawali Pers. http://ejournal.stih-awanglong.ac.id/index.php/juris

Matheus, J., & Gunadi, A. (2023). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU [Establishment of a Personal Data Protection Supervisory Agency in the Digital Economy Era: A Comparative Study with the KPPU]. *JUSTISI*, *10*(1), 20–35. https://doi.org/10.33506/jurnaljustisi.v10i1.2757 [In Indonesian]

Menpanrb. (2025). *Data BPJS Kesehatan Diduga Bocor, Menteri Tjahjo Dukung Kemkominfo Usut Tuntas [Minister Tjahjo Supports the Ministry of Communication and Information's Thorough Investigation into Alleged BPJS Health Data Leak]*. https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas,

Murima, W. H., Prayogi, A. R. Y., Rahvy, A. P., Djunaedi, N., & Dhamanti, I. (2022). Telemedicine Use in Health Facility During Covid-19 Pandemic: Literature Review. *Jurnal Administrasi Kesehatan Indonesia*, *10*(2), 251–260. https://doi.org/10.20473/jaki.v10i2.2022.251-260

Nadiroh, A., Wiraguna, S. A., & Nadiroh, A. (2025). Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia [Legal Analysis of Data Leaks in Digital Healthcare Services: A Case Study of Telemedicine Applications in Indonesia]. *Media Hukum Indonesia*, *2*(6), 313–320. https://doi.org/10.5281/zenodo.15520536 [In Indonesian]

Nugroho, S. S., Haryani, A. T., & Farkhani, F. (2020). Metodologi Riset Hukum [Legal Research Methodology]. *Oase Pustaka, Surakarta*.

OCR HIPAA, P. (2025). *Standards For Privacy of Individually Identifiable Health Information [45 CFR Parts 160 and 164*. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html.

Peraturan Menteri Kesehatan Republik Indonesia. (2019). Peraturan Menteri Kesehatan Republik Indonesia Nomor 20 Tahun 2019 tentang Penyelenggaraan Pelayanan Telemedicine Antar Fasilitas Pelayanan Kesehatan [Regulation of the Minister of Health of the Republic of Indonesia Number 20 of 2019 concerning the Provi. In *Lembaga Negara Republik Indonesia Tahun 2019 Nomor 890*.

Pomantow, M. P., Rokhmat, R., & Retnowati, A. (2024). Perlindungan Hukum Kepada Klinik dan Dokter Terhadap Informasi Data Pasien yang Tidak Lengkap [Legal Protection for Clinics and Doctors Against Incomplete Patient Data Information]. *Jurnal Cahaya Mandalika ISSN 2721-4796 (Online)*, *3*(1), 667–680. https://doi.org/10.36312/jcm.v3i1.3667 [In Indonesian]

Raib, M. I. E., Rosadi, S. D., & Cahyadini, A. (2025). Perbandingan Penerapan Prinsip Transparansi Antara Indonesia dengan Irlandia dalam Hal Terjadinya Kegagalan Pelindungan Data Pribadi [Comparison of the Implementation of Transparency Principles between Indonesia and Ireland in Cases of Failure to Protect . *Eksekusi : Jurnal Ilmu Hukum Dan Administrasi Negara*, *3*(2), 51–71. https://doi.org/10.55606/eksekusi.v3i2.1815 [In Indonesian]

Rusman, A. D. P., & Suwardoyo, U. (2022). *Penerapan Sistem Informasi Berbasis IT Pengolahan Data Rekam Medis untuk Peningkatan Pelayanan di Rumah Sakit [Implementation of IT-Based Information Systems for Medical Record Data Processing to Improve Hospital Services]*. Penerbit Nem.

Santoso, S., Setiadi, A., Kom, S., Kom, M., Asikin, A. M., Pi, S., Radian Ilmaskal, S. K. M., Sadat, L. A., Dewi Nashrulloh, S. K. M., & Putra, E. S. (2025). *Sistem Informasi Kesehatan [Health Information System]*. CV Rey Media Grafika.

Saraya, S., Lubis, A. F., Juansa, A., Layungasri, G. R., & Rianty, E. (2025). *Dinamika Hukum di Indonesia: Perkembangan & Tantangan [Legal Dynamics in Indonesia: Developments & Challenges]*. PT. Star Digital Publishing, Yogyakarta-Indonesia.

Sari, A. R., & SH, M. S. (2024). *Reformasi Pelayanan Publik*. PT Indonesia Delapan Kreasi Nusa.

Sianturi, C. G. S., Nababan, R., & Siregar, R. J. (2024). Peran Hukum dalam Melindungi Data Pribadi [The Role of Law in Protecting Personal Data]. *Journal Of Social Science Research Volume*, *4*, 1–18. https://doi.org/10.31004/innovative.v4i5.15192 [In Indonesian]

Simatupang, J. R., Ardiansah, & Sudi Fahmi. (2023). Efektivitas Penggunaan Media Telemedicine Berdasarkan Hukum Indonesia dan Malaysia [Effectiveness of Telemedicine Media Use Based on Indonesian and Malaysian Law]. *Jurnal Hukum Samudra Keadilan*, *18*(1), 15–32. https://doi.org/10.33059/jhsk.v18i1.7183 [In Indonesian]

Union, E. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation. *Official Journal of the European Union*.

UUD. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi [Law Number 27 of 2022 concerning Personal Data Protection]. In *Lembaran Negara Republik Indonesia Tahun 2022*.

UUD. (2023). *Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan [Law Number 17 of 2023 concerning Health]*.

WHO. (2021). *Ethics and Governance of Artificial Intelligence for Health*. WHO.