LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 14, No. 2, 2025, pp. 278-285
Published by: IHSA Institute (Institut Hukum Sumberdaya Alam)

Protection of Patient Data Confidentiality in Telemedicine Services In Indonesia: A Human Rights Perspective

Bagus Gede Ari Rama[1], Ni Putu Sawitri Nandari[2], Kadek Julia Mahadewi[3]

[1,2,3]Faculty Of Law, Universitas Pendidikan Nasional, Indonesia

Abstract: The growth of telemedicine in Indonesia has become an innovative solution to improve access to health services, especially in remote areas, but accompanied by an increased risk of leakage of sensitive patient data. This problem is exacerbated by the uneven implementation of data protection regulations, despite the implementation of the Personal Data Protection Law (PDP Law) of 2022, Minister of Health Regulation No. 20 of 2019, and provisions in the Health Law. This study uses a normative legal approach with analysis of legal documents, legal literature, and a study of secondary data related to data leakage incidents in the telemedicine sector. The discussion focused on reviewing the legal provisions that regulate explicit approval, transparency, and information security systems in the management of medical data, as well as analyzing the application of these norms in the field. Furthermore, this study integrates legal theories such as informational self-determination and contextual integrity, as carried out by leading experts (Warren & Brandeis, Solove, Westin, Nissenbaum, and Kuner), to assess the impact of data leaks on human rights, especially the right to privacy and protection of personal information. The results show that although regulations have been legally enforced, implementation constraints such as inequality in digital infrastructure, differences in legal interpretation at the local level, and cross-sector coordination are still major obstacles. Therefore, synergy between strict regulation and a multidisciplinary approach is urgently needed to ensure that telemedicine innovation goes hand in hand with full respect for human rights.

Keywords: Telemedicine, Personal Data Protection, Human Rights

1. Introduction

In the ever-evolving digital era, telemedicine has emerged as an innovative solution to overcome challenges in healthcare, especially in developing countries such as Indonesia. According to a report from the Global Telemedicine Market, the use of telemedicine is expected to grow by 25% per year, reaching a global market value of USD 459.8 billion by 2026. In Indonesia, the adoption of telemedicine increased significantly, especially during the COVID-19 pandemic, with telemedicine platforms seeing a 300% increase in users in 2020.(Permata Seviera, 2024) Globally, the use of telemedicine has increased rapidly, driven by the need for efficiency in healthcare and better access for patients. According to a report from the World Health Organization (WHO), the use of telemedicine in Southeast Asia is expected to increase by up to 60% in recent years, reflecting the great potential that this sector has.(Stoltzfus et al., 2023)

While telemedicine offers convenience and accessibility, this growth also comes with significant risks related to patient data security. Data leakage is a global issue of concern; A report from Cybersecurity Ventures states that cyberattacks against the healthcare sector increased by 45% in 2021.(Oche Joseph Otorkpa et al., 2024). In Indonesia, a number of cases of privacy violations have attracted attention, with news about the data leak of users of popular health apps. This raises concerns about the long-term impact on public trust in telemedicine services.(Syahwami & Hamirul, 2024)

Correspondence:
Name : Bagus Gede Ari Rama
Email : arirama@undiknas.ac.id

Received: May 03, 2025;
Revised: May 07 2025;
Accepted: May 17, 2025;
Published: Jun 30, 2025;

On the other hand, government policies related to personal data protection in Indonesia are also still in the development stage. Despite the Personal Data Protection Law passed in 2022, its implementation still faces many obstacles, including a lack of understanding among healthcare providers about the importance of data security. This adds to the complexity of the problems faced in maintaining patient data privacy.(Rohmah, n.d.)

In the context of Human Rights (HAM), personal data protection is a fundamental aspect that must be upheld. Under Article 28G of the 1945 Constitution, everyone has the right to personal protection, including information related to health (Singh, 2024). However, many telemedicine service providers in Indonesia still face challenges in protecting patient data, potentially violating basic individual rights. Research by the Personal Data Protection Institute shows that only 30% of telemedicine service providers implement adequate data security standards. (Iswandari et al., 2024). Based on the presentation that has been described earlier, it will be very interesting to discuss further in the form of a legal journal with the title: Protection of Confidentiality of Patient Data in Telemedicine Services in Indonesia: Human Rights Perspective

If viewed from previous studies, (Fakih, 2022) indicated that patient data protection in telemedicine services in Indonesia remains significantly weak, as evidenced by the data breach incident involving 1.3 million eHAC users. How Kit Thong and Danny Kit Chung Wong also identified similar issues in Malaysia, particularly concerning the legality and security of data in electronic prescription use within telemedicine services. (Thong et al., 2021) Meanwhile, Fanny Priscyllia (Priscyllia, 2019) revealed that Malaysia has a stricter data protection framework through the *Personal Data Protection Act (PDPA) 2010*, which provides more comprehensive safeguards compared to Indonesia's regulations.

The study conducted by Ramdhani Simatupang (Rahmadhani Simatupang & Fahmi, 2023) reinforces these findings by demonstrating that telemedicine regulations in Indonesia remain limited to services between healthcare facilities, whereas Malaysia enforces stricter regulations for medical practitioners. Overall, patient data protection in Indonesia's telemedicine sector is still suboptimal and requires a more comprehensive regulatory reform to ensure the security of personal data and compliance with higher data protection standards.

This study aims to analyze the relationship between patient data leakage in telemedicine and its implications for human rights, with a focus on the application of existing legal norms. The formulation of the problems that will be discussed in this study includes: 1) What are the legal provisions that govern the protection of personal data in the context of telemedicine in Indonesia? 2) How is the implementation of these legal norms in practice and their impact on human rights?

2. Materials and Methods

The normative legal research method used in this study provides a structured approach to analyzing existing legal norms and their effectiveness in protecting patient data in telemedicine services. By examining statutory regulations, official legal documents, and legal literature, this method identifies gaps and inconsistencies in current legal frameworks. Previous research by Briant and Budiarsih (2022) found that telemedicine regulations in Indonesia remain fragmented, leaving legal loopholes, particularly concerning doctors' liability. Similarly, (Arfah & Puspitosari, 2023) emphasized healthcare providers' responsibilities in protecting patient data and the legal risks posed by data breaches. By building on these findings, this study evaluates the adequacy of Indonesia's **Personal Data Protection Act** and **Medical Practice Law** in addressing patient data security. The research highlights ambiguities and inconsistencies in the law while proposing leg-

islative improvements, stricter enforcement mechanisms, and clearer sanctions to enhance patient data protection in telemedicine services.

Furthermore, this research method facilitates an examination of differences in legal interpretations at both regional and national levels. By analyzing regulatory texts, judicial decisions, and legal scholarship, the study uncovers variations in how patient data protection is enforced across different jurisdictions. (Arfah & Puspitosari, 2023) noted that while national laws impose responsibilities on healthcare providers, these obligations may be interpreted differently at the regional level due to varying local policies. Additionally, (Marune, 2023) identified inconsistencies in regulatory enforcement that contribute to legal uncertainty. Through comparative legal analysis, this study explores these disparities, demonstrating the need for harmonization between national policies and regional regulations to ensure consistent and effective patient data protection. By addressing these legal challenges, the study provides a foundation for policy recommendations aimed at strengthening the legal framework governing patient data security in telemedicine services.

3. Results and Discussion

3.1 Legal Provisions for Personal Data Protection in Telemedicine in Indonesia

The protection of personal data in the context of telemedicine in Indonesia is governed by a number of complementary regulations, creating a legal framework that aims to protect the rights of individuals regarding their health information. The Personal Data Protection Law (PDP Law) passed in 2022 is the main legal foundation, adopting principles that are in line with international standards, such as the obligation to obtain clear consent from data subjects, transparency in data collection and processing, and the responsibility of organizers in maintaining the security of personal data. The Act provides that any data collection must be carried out with the explicit consent of the individual, which gives them the right to know the purposes for which the data is used and which third parties may be involved. (Yuniarti, 2022)

In addition to the PDP Law, the Regulation of the Minister of Health No. 20 of 2019 concerning the Implementation of Telemedicine also has an important role in regulating the practice of telemedicine in Indonesia. This regulation puts forward guidelines for health workers in using information technology, with an emphasis on the importance of patient data protection. In this context, telemedicine service providers are required to implement adequate security measures to protect patient data from unauthorized access and information leakage.(Iswandari et al., 2024)

Furthermore, Health Law No. 36 of 2009 also provides a legal basis related to patients' rights, including the right to protect their personal data. The articles in this law affirm that every patient has the right to have protection for the health information in his possession, which should not be misused by health care providers.(Maria Maddalena Simamora, 2022)

In detail, there are several articles in Indonesia's positive law that regulate the protection of personal data of telemedicine patients, including: The Personal Data Protection Law (PDP Law) which was passed in 2022 has a number of key articles that are directly related to patient data protection. Article 1 defines important terms, such as "personal data," "data controller," and "data processing," which provide a basic framework of understanding. Article 6 emphasizes the obligation to obtain consent from the data subject before collection is carried out, especially in telemedicine where sensitive health data is often collected. Article 14 regulates the right of data subjects to access and correct their personal data, which ensures that patients can verify the accuracy of their health information. In addition, Article 15 requires data controllers to report data leaks to the authorities and data subjects, increasing transparency and accountability. (Siti Yuniarti, et.al, 2023).In addition, the Minister of Health Regulation No. 20 of 2019 pro-

vides specific guidelines in the implementation of telemedicine. Regulation of the Minister of Health No. 20 of 2019 concerning the Implementation of Telemedicine Services Between Health Service Facilities provides an important legal framework for the implementation of telemedicine services in Indonesia. In the increasingly developing digital era, telemedicine is an effective solution to expand access to health services, especially in remote areas that are difficult for medical personnel to reach. However, in its implementation, the security aspect of patient personal data is one of the important elements that is strictly regulated.

This regulation defines telemedicine as the provision of telemedicine health services carried out by health workers by utilizing information and communication technology. This includes the exchange of information, diagnosis, treatment, as well as research and evaluation that allows the sending and receiving health care facilities to work together in handling patients. In this case, the exchange of data and information between the two healthcare facilities poses challenges related to the confidentiality and security of patients' personal data. (Adrianto, et.al, 2021)

As stipulated in Article 17 paragraph (2) letter b and Article 18 paragraph (2) letter b of this regulation, every patient data and information obtained from telemedicine services must be guaranteed confidentiality by the Health Facility.(Delva Primayani et al., 2021.)

This provision emphasizes the importance of protecting patients' personal information from unauthorized access or unlawful use. Given that health data falls under the category of sensitive personal data, the protection of confidentiality is part of the individual's right to privacy, which is protected both nationally through the Personal Data Protection Law and internationally through human rights instruments, such as the Universal Declaration of Human Rights. (Ariyanie Yusuf et al., 2024)

In the context of telemedicine, patient data sent electronically through telecommunication systems needs to be protected from the threat of data leakage, hacking, or misuse by third parties. Article 12 of this regulation stipulates that health service facilities that provide telemedicine must use a telemedicine application with a data safety system in accordance with the provisions of laws and regulations. This technology must meet the security standards set by the Ministry of Health, including securing communication systems and storing data in an encrypted manner. (Tombokan,2024)

In addition, this rule also requires every health facility involved in telemedicine to maintain patients' electronic medical records. These medical records are an important part of personal data that must be maintained in integrity. Article 3 letter 7, Article 7 Paragraph (1) letter c, Article 7 Paragraph (2) letter c and Article 14 paragraph 4 require documentation of all telemedicine services in electronic medical records, which must be protected from being accessed by uninterested parties. (Lestari, 2021)

Furthermore, Health Law No. 17 of 2023 also includes relevant provisions, Article 4 paragraph (1) letter i affirms that patients have the right to obtain confidentiality of their personal health data and information. Article 32 states that every patient has the right to protect their personal data from unauthorized access, providing a legal basis to address privacy violations in telemedicine. The implications of these articles are significant, as healthcare providers must be aware of their legal obligations and the consequences of violations.

Given these regulatory limitations, Indonesia must strengthen its legal framework to ensure more comprehensive and effective patient data protection in telemedicine. Compared to countries with stricter oversight on individual medical practitioners, Indonesia’s regulations remain primarily focused on healthcare facilities, creating gaps in accountability. Aligning national regulations with international standards, expanding legal coverage to include individual healthcare practitioners, and enhancing enforcement mechanisms are essential steps to closing existing legal gaps and mitigating risks associated with data breaches.

3.2 Implementation of Personal Data Protection Law in Telemedicine and Its Impact on Human Rights

In the increasingly evolving digital era, the protection of personal data—especially medical data in telemedicine—has become a central issue in efforts to ensure human rights. At the global level, the concept of data protection has been driven by the thinking of pioneers such as Warren and Brandeis (1890), who in their classic work "The Right to Privacy" emphasized that privacy is a fundamental right that must be protected from unauthorized intervention. (Hansen Samin, 2023)This thinking has provided the basis for modern privacy theory, which was later further developed by Daniel J. Solove in Understanding Privacy (2008). Solove stated that privacy is a multifaceted phenomenon, which covers all aspects of data collection, storage, and dissemination, so that each stage of data processing carries potential risks that must be anticipated through comprehensive legal regulations. (Widigdo & Ferry Rosando, 2023)Alan Westin, in Privacy and Freedom (1967), emphasized that individual control over his or her personal information is an absolute requirement for freedom and autonomy. This concept requires an informed consent mechanism, where each individual must get a thorough explanation before their personal data is processed.(Djafar, 2019)

In addition, the theory of "contextual integrity" introduced by Helen Nissenbaum (2009) emphasizes that data processing must be in harmony with social norms and cultural expectations in a certain context. (Bahram, 2023()In the realm of telemedicine, medical data is not only concerned with technical aspects, but also reflects the identity and dignity of the patient which must be respected in accordance with socially agreed confidentiality standards.

In line with these thoughts, Christopher Kuner (2013) reveals the challenges that arise due to cross-border data flows, which require harmonization between international standards—as embodied in the European Union's General Data Protection Regulation (GDPR) (2016)—and national legal frameworks.(Czerniawski et al., 2024.) In Indonesia, efforts to align international regulations with local needs have been realized through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and Minister of Health Regulation Number 20 of 2019 concerning Telemedicine.

The PDP Law establishes a strict legal framework by demanding transparency, accountability, and informed consent in the processing of personal data. Telemedicine service providers are required to register data processing systems, conduct internal audits, and implement advanced security technologies such as encryption and multi-factor authentication to protect sensitive data. On the other hand, Permenkes No. 20 of 2019 regulates operational and technical standards in the implementation of telemedicine, with the aim of ensuring that each medical data processing procedure meets the security and accuracy standards that have been set.

Theoretically, the concept of informational self-determination—which is widely associated with Solove and Westin's thinking—is the foundation that every individual has the right to control his or her personal data.(Aji, 2023) This is strengthened by the application of the principles of transparency and accountability, which require service providers to always convey clear information to data subjects, as well as account for every data processing action through an effective monitoring mechanism. In addition, the principles of legal certainty and due process are absolute requirements so that any violation of personal data can be identified and followed up fairly.(Situmeang, 2021)

From a conceptual perspective, the concept of cross-sector harmonization is also very important. In Indonesia, the successful implementation of data protection regulations does not only depend on one institution, but is the result of coordination between the Ministry of Health, the Ministry of Communication and Informatics, and other supervisory agencies. This is a manifestation of efforts to harmonize global standards and local needs—a challenge expressed by Kuner—so that there is no fragmentation of data protection that can open up legal loopholes.

In addition to the normative aspect, the ethical criticisms delivered by Shoshana Zuboff in The Age of Surveillance Capitalism (2019) and Viktor Mayer-Schönberger in Delete: The Virtue of Forgetting in the Digital Age (2009) highlight the dangers of excessive data commercialization. They argue that the massive collection of data for economic purposes should be balanced with the right of individuals to control and, if necessary, delete data that is no longer relevant. (Putranto, 2020)This perspective emphasizes that data protection in telemedicine is not only a technical issue, but also an effort to maintain the dignity and autonomy of each individual.

Although the regulations have been strictly stipulated through the PDP Law and Permenkes Number 20 of 2019, a critical analysis of its implementation shows that there are challenges in the field. The gap in digital infrastructure between regions, variations in legal interpretation at the local level, and cross-sectoral coordination that has not been maximized are real obstacles. Therefore, the success of personal data protection in telemedicine is highly dependent on capacity building, policy harmonization, and comprehensive legal education to all stakeholders.

The challenges in implementing data protection regulations in telemedicine highlight the need for a more integrated and technology-driven approach. Harmonizing national and international data protection frameworks remains a challenge, as regional disparities in legal interpretation create uncertainty. Compared to countries with clearer enforcement mechanisms, Indonesia still faces infrastructure gaps that increase the risk of data breaches. Future policies should focus on improving legal certainty, fostering cross-sectoral collaboration, and leveraging emerging technologies such as AI and blockchain to enhance data security while ensuring compliance with human rights principles, in line with evolving global standards.

4. Conclusions

Indonesia's legal framework for patient data protection in telemedicine, established through the PDP Law 2022 and Minister of Health Regulation No. 20 of 2019, faces significant challenges in integrating human rights principles. Inconsistent legal interpretation and enforcement, coupled with regional disparities in digital infrastructure, weaken data protection efforts. Ethical concerns, particularly regarding informed consent, transparency, and commercialization of personal data, further highlight the need for stronger safeguards.

Future research should explore AI and blockchain technologies to enhance data security and patient control. AI can improve real-time threat detection, while blockchain offers tamper-proof data storage aligned with international privacy standards. Strengthening cross-sectoral collaboration among regulators, healthcare providers, and technology developers is crucial to ensuring a more secure and ethically responsible telemedicine ecosystem in Indonesia.

References

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Arfah, N. A., & Puspitosari, H. (2023). PERLINDUNGAN HUKUM TERHADAP DATA PASIEN TELEMEDICINE DALAM MENERIMA PELAYANAN MEDIS BERBASIS ONLINE. *JURNAL FUSION*, *3*, 7. https://doi.org/10.54543/fusion.v3i05.339

Ariyanie Yusuf, S., Herlina, C., & Sibarani, L. (n.d.). *Kongres ke-6 MHKI Aspek Legal dan Etika Penggunaan Data Pasien dalam Teknologi Big Data dan Kecerdasan Buatan di Sektor Kesehatan*.

Bahram, M. (2023). TANTANGAN HUKUM DAN ETIKA (REKAYASA SOSIAL TERHADAP KEBEBASAN BERPENDAPAT DI DUNIA DIGITAL). In *Jurnal Riset Ilmiah* (Vol. 2, Issue 12).

Czerniawski, M., Jerker, D., Svantesson, B., & Svantesson, D. (n.d.). *Challenges to the extraterritorial enforcement of data privacy law-EU case study Challenges to the extraterritorial enforcement of data privacy law-EU case study Challenges to the extraterritorial enforcement of data privacy law-EU case study*. https://www.researchgate.net/publication/377463968

dan Kebutuhan Pembaruan, U., & Djafar, W. (n.d.). *Hukum Perlindungan Data Pribadi di Indonesia*. http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

Delva Primayani, F., Farhan Pratama, M., & Julia Putri, Z. (n.d.). *Layanan Telemedicine: Aspek Hukum dan Perjanjian Terapeutik Telemedicine Services: Legal Aspects and Therapeutic Agreement*. https://doi.org/10.24167/shk.v9i2.10624

Fakih, M. (2022). Telemedicine in Indonesia During the Covid-19 Pandemic: Patients Privacy Rights Protection Overview. *Fiat Justisia: Jurnal Ilmu Hukum*, *16*(1), 81–102. https://doi.org/10.25041/fiatjustisia.v16no1.2583

Hansen Samin, H. (2023). PERLINDUNGAN HUKUM TERHADAP KEBOCORAN DATA PRIBADI OLEH PENGENDALI DATA MELALUI PENDEKATAN HUKUM PROGRESIF. *Jurnal Sains Student Research*, *1*(2), 1–15. https://doi.org/10.61722/jssr.v1i3.386

Hukum, J., & Indonesia, K. (2021). *TINJAUAN PERBANDINGAN PENYELENGGARAAN TELEMEDICINE ANTARA INDONESIA DAN AMERIKA SERIKAT*. *01*(02), 70–85.

Iswandari, H. D., Erawati, A. D., Sugiharto, S., & . H. (2024). Reconstructing Legal Frameworks for Safeguarding Telemedicine Consumers. *International Journal of Religion*, *5*(11), 4309–4315. https://doi.org/10.61707/kdp0eq44

Jurnal+Christian+Daniel+Tombokan (1). (n.d.).

Kajian, J., Dan, H., Kewarganegaraan, P., Martupa, A. E., & Marune, S. (2023). *Civilia : METAMORFOSIS METODE PENELITIAN HUKUM: MENGARUNGI EKSPLORASI YANG DINAMIS* (Vol. 2, Issue 4). http://jurnal.anfa.co.id

Lestari, R. D. (2021). Perlindungan Hukum bagi Pasien dalam Telemedicine. *Jurnal Cakrawala Informasi*, *1*(2), 51–65. https://doi.org/10.54066/jci.v1i2.150

Maria Maddalena Simamora, I. (2022). PERLINDUNGAN HUKUM ATAS HAK PRIVASI DAN KERAHASIAAN IDENTITAS PENYAKIT BAGI PASIEN COVID-19. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *1*(7), 1089–1098. https://doi.org/10.54443/sibatik.v1i7.126

Oche Joseph Otorkpa, Ololade Esther Olaniyan, & Adefunmilola Adebola Onifade. (2024). Protecting patient privacy in the age of smart healthcare: practical cybersecurity measures for individuals and healthcare providers. *World Journal of Advanced Research and Reviews*, *23*(1), 3047–3050. https://doi.org/10.30574/wjarr.2024.23.1.2334

Permata Seviera, A. (2024). *HAMBATAN TELEMEDICINE PADA MASA PANDEMI COVID-19 DI INDONESIA: LITERARURE REVIEW*. *9*(7). https://doi.org/10.36418/syntax-literate.v9i7

Privasi, P., & Priscyllia, F. (2019). *PERLINDUNGAN PRIVASI DATA PRIBADI PERSPEKTIF PERBANDINGAN HUKUM* (Vol. 34, Issue 3).

Rahmadhani Simatupang, J., & Fahmi, S. (2023). EFEKTIVITAS PENGGUNAAN MEDIA TELEMEDICINE BERDADASARKAN HUKUM INDONESIA DAN MALAYSIA. In *JHSK* (Vol. 18, Issue 1). Januari-Juni. https://kominfo.go.id/content/detail/27509/penggunaan-aplikasi-telekonferensi-naik-443-persen-

Rohmah, N. Q. (n.d.). *Health Data Protection and Privacy in The Internet of Things Era: The New Legal Challenges in Indonesia*.

Situmeang, S. M. T. (2021). PENYALAHGUNAAN DATA PRIBADI SEBAGAI BENTUK KEJAHATAN SEMPURNA DALAM PERSPEKTIF HUKUM SIBER. *SASI*, *27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394

Stoltzfus, M., Kaur, A., Chawla, A., Gupta, V., Anamika, F. N. U., & Jain, R. (2023). The role of telemedicine in healthcare: an overview and update. *The Egyptian Journal of Internal Medicine*, *35*(1). https://doi.org/10.1186/s43162-023-00234-z

Syahwami, S., & Hamirul, H. (2024). The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia. *Enigma in Law*, *2*(2), 75–84. https://doi.org/10.61996/law.v2i2.56

THE NEW CHAPTER OF INDONESIA'S DATA PROTECTION ON DIGITAL ECONOMY PERSPECTIVE. (2023). *Journal of Southwest Jiaotong University*, *58*(3). https://doi.org/10.35741/issn.0258-2724.58.3.9

Thong, H. K., Wong, D. K. C., Gendeh, H. S., Saim, L., Athar, P. P. B. S. H., & Saim, A. (2021). Perception of telemedicine among medical practitioners in Malaysia during COVID-19. *Journal of Medicine and Life*, *14*(4), 468–480. https://doi.org/10.25122/jml-2020-0119

Widigdo, Z., & Ferry Rosando, A. (2023). PERLINDUNGAN NEGARA TERHADAP PRIVASI DATA PRIBADI DALAM LAYANAN SIM CARD DI ERA DIGITAL. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *3*(1). https://doi.org/10.53363/bureau.v3i1.210

yeremias,+Journal+editor,+1_Hendar_9-48. (n.d.).

Yuniarti, S. (2022). PROTECTION OF INDONESIA'S PERSONAL DATA AFTER THE RATIFICATION OF THE DRAFT PERSONAL DATA PROTECTION LAW. *Progressive In Law*, *4*(2).