Multidiciplinary Output Research For Actual and International Issue
(MORFAI Journal) | ISSN (e): 2808-6635
Volumes 6 No. 4 (2026)

TELEMEDICINE SERVICES IN PERSONAL DATA PROTECTION (LEGAL REVIEW)

Harianto[1*], Marice Simarmata[2], Irsyam Risdawati[3]
Magister of Health Law, Universitas Pembangunan Panca Budi, Indonesia
E-mail: hariantounpab24@gmail.com[1*], ichesmart@yahoo.co.id, irsyam.risdawati@gmail.com

Received : 20 March 2026 Accepted : 17 April 2026
Revised : 30 March 2026 Published : 16 May 2026

Abstract

The development of digital technology has driven significant transformation in healthcare services, one of which is through the implementation of telemedicine between healthcare facilities. Telemedicine provides easy access to medical services, especially in remote areas, by utilizing information technology for consultation, diagnosis, and clinical data exchange. This study aims to analyze and examine legal regulations regarding personal data protection and the responsibility of telemedicine providers in protecting patients' personal data. The research method used is a normative legal research method, also known as doctrinal legal research or dogmatic legal research. This study focuses on written regulations, so it is closely related to a literature study. The results of the study confirm that to ensure that personal data is managed very carefully and cautiously by telemedicine service providers, more serious sanctions can be considered in this case, namely criminal liability for telemedicine service providers as controllers of personal data in the event that personal data is distributed illegally from management activities carried out using Hans Kelsen's legal liability theory, which states "Failure to exercise the care required by law is called negligence, and negligence is usually considered.

Keywords: Telemedicine, Legal Regulation, Personal Data Protection.

INTRODUCTION

In the current era of digitalization, technology is developing rapidly and has become an important and inseparable part of human life. The relationship between technological developments and health services is the emergence of a new method, namely online health services, termed telemedicine, which relies on information technology media with the aim of being able to reduce direct or face-to-face meetings between doctors and patients, where the implementation of health services can be carried out optimally, especially for Indonesia with less supportive geographical conditions, meaning that between one place and the available health facilities there is a considerable distance (Christian Daniel Tombokan et al., 2024). According to the World Health Organization (WHO) document, namely the Global Survey on e-Health 2009, it states that the term telemedicine, also commonly called telemedicine, has existed since the 1970s, defining telemedicine as a health service, where distance is no longer an important factor, carried out by health workers using Information and Communication Technology (ICT) in the exchange of valid information, for diagnosis, treatment, prevention of disease and injury, research and evaluation, and continuing education for health service providers in advancing public health (Damasus Darma Wulan et al., 2022).

Telemedicine, or online consultation, is defined by the American Academy of Family Physicians as the practice of using technology to provide healthcare services remotely. A doctor in one location uses communication technology to serve a patient in another location (Health 2021). The Covid-19 pandemic has driven the adoption of information technology in various sectors, including healthcare. Coronavirus Disease (Covid-19) is an infectious disease of the respiratory system caused by the SARS-CoV-2 virus. The World Health Organization (WHO) declared Covid-19 a pandemic on March 11, 2020 (WHO, 2020). One way to control Covid-19 is by reducing visits to healthcare facilities for non-emergency cases. Non-emergency healthcare services can be provided using information technology through telemedicine. The Indonesian government, through Circular Letter of the Minister of Health of the Republic of Indonesia Number HK.02.01/MENKES/303/2020, urges the use of information and communication technology in the provision of healthcare services to prevent the spread of Covid-19. The use of telemedicine can provide healthcare services beyond physical boundaries. The biggest challenge in utilizing telemedicine is the low adoption rate for healthcare services. Several data breaches at healthcare facilities, including government servers,

indicate weaknesses in the security systems used or human error, such as misdirected emails or security misconfigurations, that open up opportunities for hackers. Between November 1, 2020, and October 31, 2021, at least 5,212 data breaches were identified across various industries within a year. The healthcare industry accounted for 571 of these breaches. This figure places the healthcare industry as the third most vulnerable sector to data breaches. The string of patient data breaches at hospitals and healthcare providers demonstrates the extremely weak data security protection in Indonesia. Patient data security is an absolute requirement for both the government and healthcare providers. Therefore, this study aims to examine the legal regulations and responsibilities of telemedicine providers in protecting patient personal data

LITERATUR RIVIEW

2.1 Theory of Legal Responsibility

According to Hans Kelsen, an Austrian legal expert and philosopher with his theory of legal responsibility, he stated that "a person is legally responsible for a certain act or that he bears legal responsibility, the subject means he is responsible for a sanction in the case of a contrary act. Furthermore, Hans Kelsen stated "Failure to exercise the care required by law is called negligence, and negligence is usually seen as another type of error (culpa), although not as severe as the error that is fulfilled because it anticipates and desires, with or without malice, harmful consequences.

2.2 Principles of legal protection

According to Soerjono Soekanto, legal protection according to Soekanto is basically protection given to legal subjects in the form of legal instruments. Furthermore, Soekanto explains that in addition to the role of law enforcers, there are five other factors that influence the process of law enforcement and its protection, namely the statutory factor, namely written regulations that apply generally and are made by legitimate authorities, law enforcer factors, namely parties involved in law enforcement, both directly and indirectly, factors of means or facilities that support law enforcement, such as skilled human resources or adequate tools, community factors, namely the environment where the law applies and is implemented. Acceptance in society of applicable laws is believed to be the key to peace, cultural factors, namely as a result of work, creativity, and feelings that are based on human initiative in social life.

METHOD

The research method used is the normative legal research method, which is often also referred to by other terms, namely doctrinal legal research or dogmatic legal research. This research is only aimed at written regulations, so the research is closely related to library research. Research sources are in the form of legal materials, namely materials traced to legal sources (formal) with the aim of being used to analyze applicable law, which consists of primary legal materials, secondary legal materials, and tertiary legal materials.

RESULTS AND DISCUSSION

4.1 Legal regulations regarding the protection of personal data in the implementation of telemedicine in Indonesia

Health is crucial to human life. Health is defined as a state of physical, mental, spiritual, and social well-being that enables everyone to live productively, socially and economically. Health is also something that is valuable, even very important, so vital for human life in living life to achieve (fight for) their ideals or hopes (Sinamo 2019). Currently, the use of telemedicine services is growing in the community. This is evident in the numerous online health applications such as Halodoc, KlikDokter, Alodokter, GrabHealth, and others (Yussy Adelina Mannas dan Siska Elvandari 2022). This service plays a crucial role in providing support and assistance to the community, particularly amidst the social and physical restrictions imposed in Indonesia. Furthermore, telemedicine also facilitates access to healthcare services for those limited by distance and time (Wahyu Andrianto and Atika Rizka Fajrina 2021). In the context of regulation, the Indonesian government has also begun to formulate policies that support the implementation of telemedicine as follows:

a. Minister of Health Regulation No. 20 of 2019 concerning the Provision of Telemedicine Services Between Health Service Facilities

   This Ministerial Regulation is an initial step in regulating the provision of telemedicine services between healthcare facilities. This policy aims to provide a clear legal framework for medical personnel and patients in using telemedicine services (Ahmad Hariri 2024). The background to the formation of regulations on

OPEN ACCESS

telemedicine in Indonesia can be seen in the considerations of the Minister of Health Regulation Number 20 of 2019 concerning the Provision of Telemedicine Services Between Health Service Facilities..Meanwhile, the definition of telemedicine according to Article 1 number 1 of the Minister of Health Regulation 20/2019 explains that telemedicine is the provision and facilitation of clinical services through telecommunications and digital communication technology which includes the exchange of information on diagnosis, treatment, prevention of disease and injury, research and evaluation, and continuing education of health service providers for the benefit of improving individual and community health. However, the limited scope of this Ministerial Regulation has been highlighted, as modern telemedicine practices are now often conducted directly between doctors and patients through online applications, which are not fully covered by this regulation. Therefore, while Ministerial Regulation 20/2019 represents a step forward, it is not yet fully adaptable to the rapid development of digital health technology (Max Bonsapia 2025). In the Regulation of the Minister of Health Number 20 of 2019, there is no specific regulation on legal protection for patients, only regulating the rights and obligations of service providers and service requesters, which of course can be a reference for legal protection for patients who consult online/telemedicine (Rifki 2023). In the context of legal protection, it is also important to understand that the law functions not only as a repressive tool but also as a preventive instrument. Hadjon's Theory of Legal Protection distinguishes between preventive and repressive legal protection.

b. Law Number 17 of 2023 concerning Health

Law Number 17 of 2023 concerning Health Article 4 paragraph (1) letter i states that everyone has the right to obtain confidentiality of their personal health data and information, except in circumstances as formulated in Article 4 paragraph (4), namely in the case of fulfilling requests from law enforcement officers in the context of law enforcement, handling of KLB, Epidemics, or disasters, limited educational and research interests, protection efforts against threats, the safety of others individually or in society, the interests of maintaining health, treatment, healing, and patient care, the patient's own request, administrative interests, insurance payments, or health financing guarantees; and/or other interests regulated in statutory regulations. Then Article 177 paragraph (1) emphasizes that every health service facility must keep the confidentiality of the patient's personal health, except in the cases as described in Article 4 paragraph (4). In the era of digitalization of health services, the protection of patient personal data is a crucial aspect that must receive serious attention, especially in the implementation of telemedicine services. According to Satjipto Rahardjo, legal protection is an effort to safeguard a person's interests by allocating a human right and the authority to act in accordance with those interests. This concept is inspired by Fitzgerald's stated purpose of law. According to Fitzgerald, the purpose of law is to integrate and coordinate various interests in society by regulating the protection and restrictions on these interests.

c. Law Number 27 of 2022 concerning Personal Data Protection.

Personal data, as regulated in Article 1 number 1 of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), is any data about an individual that is identified or identifiable individually or in combination with other information. In the context of digital health services, personal data includes patient name, address, medical record number, and contact information. Sensitive personal data or specific personal data as described in Article 4 paragraph (2) of the PDP Law includes health data, biometric data, and genetic data, which if misused can pose serious risks to individuals. Therefore, protection of this data must be implemented with high security standards and strict legal compliance (Edy Susanto 2024). Based on Article 16 of the 2022 Personal Data Protection Law (PDP Law), the processing of personal data must be based on the explicit consent of the data owner, and data controllers are required to maintain its security and confidentiality. In the context of telemedicine, service providers, both healthcare facilities and commercial platforms, must ensure that patients provide consent before their data is collected or shared. As part of the legal protection of personal data, preventative measures, as referred to in Article 39 paragraph 1, are explained in paragraph 2 of the PDP Law. This prevention is carried out using a highly reliable, safe, and responsible security system. Article 39 paragraph 3 of the PDP Law further states that this prevention is carried out in accordance with statutory provisions. In the context of telemedicine, patient personal data becomes more vulnerable because information transmission takes place online. The transmission of medical data through digital networks increases the possibility of unauthorized access, data leaks, or information misuse (Budhijanto Danrivanto 2021). Therefore, healthcare facilities are obliged to guarantee the security

OPEN ACCESS

and confidentiality of patient medical data as regulated in Law Number 27 of 2022 concerning Personal Data Protection (Lestari 2021).

d. Government Regulation (PP) Number 28 of 2024 concerning Implementing Regulations of Law Number 17 of 2023 concerning Health

In order to increase the capacity and resilience of Health within the framework of Health transformation to achieve the highest level of public health improvement, Health Efforts, Health Resources, and Health management are carried out which are supported by strengthening regulations with the enactment of Law Number 17 of 2023 concerning Health. In Article 549 paragraph (1) of Government Regulation (PP) Number 28 of 2024 concerning Implementing Regulations of Law Number 17 of 2023 concerning Health, the Implementation of Health Efforts can utilize information and communication technology with the aim of expanding access and improving the quality of Health Services. The use of information and communication technology as referred to in Article 549 paragraph (1) can be implemented through Telehealth and Telemedicine. Telehealth consists of providing clinical services and non-clinical services while the provision of clinical services is carried out through Telemedicine. Every Health Service Facility that provides Health Services through information and communication technology is required to implement data security standards and electronic systems in accordance with the provisions of laws and regulations.

4.2 Responsibility of telemedicine providers in protecting patient personal data

The growth of telemedicine in Indonesia has made healthcare services easier to access, especially for people living in remote areas or regions with limited healthcare facilities. However, this change also presents various challenges that must be addressed. Key issues include maintaining effective and empathetic digital communication, as well as the security and privacy risks of medical data, which must be strictly safeguarded. A number of data breach incidents in recent years have further highlighted the weaknesses in Indonesia's digital healthcare data security system. One of the most prominent cases occurred in early 2022, when data allegedly leaked and freely sold on the RaidForum website involved COVID-19 patient data.-19 belonging to the Ministry of Health (Kemenkes), which allegedly originated from 6 million patient medical records. Reports emerged on January 6, 2022, stating that the sample documents totaled at least 720 GB of personal data and patient medical records, with the document description "Centralized Server of the Ministry of Health of Indonesia." The impact of this data breach is very serious, because personal medical information can be used for identity theft, financial fraud, and even cause psychological stress for victims.

Digital forensics expert Ruby Alamsyah considers the BPJS Kesehatan data breach to be the largest data leak ever to occur in Indonesia. Ruby revealed that the BPJS Kesehatan data leak occurred because data access was granted to a third party or vendor. Ruby Alamsyah said this internal error resulted in carelessly trusting a third party without proper authorization. The third party appeared to be able to access the data legally, because it was permitted, but it was not monitored or audited. Granting such access must be accompanied by strict monitoring. Granting access accompanied by strict supervision can allow vendors to continue working effectively amidst data security guarantees. Article 274 letter c of Law Number 17 of 2023 concerning Health states that medical personnel are required to maintain patient health confidentiality. Legal protection provided to legal subjects contains sanctions for anyone who violates or intentionally violates the law established in accordance with legal norms. In this case, health service providers are responsible as organizers of electronic systems and as data controllers for the processing of personal data. Legal protection for recipients and providers of health services regarding the implementation of Telemedicine is a mandate from Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia which states that, "everyone has the right to protection of themselves, their families, honor, dignity, and property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a basic human right."

To protect the rights of individuals in society in relation to the processing of Personal Data, whether carried out electronically or non-electronically using data processing devices, is carried out by Personal Data Controllers, namely every person, public body, and international organization acting individually or jointly in determining the purpose and exercising control over the processing of Personal Data (Masnun 2022). Any data collection and processing must obtain explicit consent from the patient as stipulated in Article 20 of Law Number 27 of 2022 concerning Personal Data Protection. The Personal Data Controller has an obligation to protect and ensure the security of the Personal Data it processes, by preparing and implementing operational technical measures to protect Personal Data from interference with Personal Data processing that is contrary to the provisions of laws and regulations and determining the level of security of Personal Data by taking into account the nature and risks of the Personal Data that must be protected in the processing of Personal Data. Article 36 of Law Number 27 of 2022

OPEN ACCESS

concerning Personal Data Protection states that when processing personal data, personal data controllers are required to maintain confidentiality. Within this framework, telemedicine service providers act as data controllers, obligated to ensure the security, accuracy, and legal and transparent use of data (Aenun Nadiroh 2025). Telemedicine providers are also required to conduct a Privacy Impact Assessment to identify potential data breach risks early on. Equally important, if a breach or data breach occurs, data controllers are required to report it to the relevant authorities and notify the data owner. As stipulated in Article 46 of Law Number 27 of 2022 concerning Personal Data Protection, in the event of a failure in Personal Data Protection, the Personal Data Controller is required to provide written notification to the Personal Data Subject within no later than 3 x 24 (three times twenty-four) hours; and the institution. The legal consequences for the failure of the party managing personal data are also regulated in several regulations in Indonesia, including Government Regulation (PP) Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, which regulates the obligation of Electronic System Operators (PSE) to maintain the confidentiality, integrity, and availability of Personal Data, and requires the consent of the data owner for its acquisition, use, and disclosure, unless there is another legal basis that regulates differently. This regulation ensures the protection of personal data by emphasizing transparency of purpose and user consent, which are basic principles in the digital ecosystem, including further regulated in various relevant Ministerial Regulations. In the event of a failure in protecting the confidentiality of the Personal Data it manages, the Electronic System Operator is required to notify the owner of the Personal Data in writing. Personal data controllers who are not careful in managing personal data may be subject to administrative sanctions in the form of written warnings, temporary suspension of processing and personal data activities, deletion or destruction of personal data and/or the imposition of administrative fines.

The application of criminal sanctions can only be applied in cases where the act is carried out intentionally, this can be seen in the formulation of Article 67 paragraph (1) which states "Any person who intentionally and unlawfully obtains or collects Personal Data that is not his/hers with the intention of benefiting himself/herself or another person which can result in losses to the Personal Data Subject shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah)". Article 67 paragraph (2), any person who intentionally and unlawfully shows personal data that is not his/hers is threatened with imprisonment for a maximum of four (four) years and/or a maximum fine of Rp. 4,000,000,000.00 (four billion rupiah). Article 67 paragraph (3) "Any person who unlawfully and unlawfully uses personal data that is not his/hers shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah).

According to Hans Kelsen, an Austrian legal expert and philosopher with his theory of legal responsibility, he stated that "a person is legally responsible for a certain act or that he bears legal responsibility, the subject means that he is responsible for a sanction in the event of a contrary act (Kelsen, 2018). Hans Kelsen further states “Failure to exercise the care required by law is called negligence, and negligence is usually considered as another kind of fault (culpa), although less serious than the fault that is fulfilled by anticipating and intending, with or without malice, a harmful consequence (Salim, 2009). Law of the Republic of Indonesia Number 20 of 2022 concerning Personal Data Protection regulates legal accountability for personal data protection by imposing administrative and criminal sanctions for violations of personal data protection. However, law enforcement in the field remains weak, as evidenced by news reports. To date, no parties have been criminally charged for violations of personal data protection. Furthermore, an independent and operational data protection oversight body has not been established, resulting in no institution having full authority to audit, verify, or take action against violations that occur in the implementation of personal data protection, including in telemedicine services. This situation still creates the potential for leaks of personal data originating from healthcare services, including telemedicine, as existing regulations regarding the personal data protection system in the management of telemedicine services are not yet optimal. The consequences of administrative and criminal sanctions in Law of the Republic of Indonesia Number 20 of 2022 concerning Personal Data Protection are not yet optimal enough to create general deterrence for others from committing violations of the law, as the relative theory emphasizes that the purpose of criminal law is to prevent crime (Devara 2020).

CONCLUSION

Normatively, the legal framework for personal data protection in telemedicine has been regulated through various laws and regulations, namely Minister of Health Regulation No. 20 of 2019 concerning the Provision of Telemedicine Services Between Health Service Facilities, Law No. 17 of 2023 concerning Health, Law No. 27 of 2022 concerning Personal Data Protection, Government Regulation (PP) No. 28 of 2024 concerning Implementing

OPEN ACCESS

Regulations of Law No. 17 of 2023 concerning Health. Telemedicine has become a significant innovation in increasing access to health services in Indonesia, especially for communities in remote areas and during the pandemic. However, the development of these digital health services must be accompanied by adequate legal protection, particularly regarding the security and confidentiality of patient personal data. Although Minister of Health Regulation 20/2019 provides the basis for regulating telemedicine, this regulation does not fully cover modern telemedicine practices conducted directly between doctors and patients through digital platforms. A number of major data breaches, such as those involving the Ministry of Health and the Social Security Agency (BPJS Kesehatan), demonstrate the weakness of the system, with no parties held legally accountable for these personal data protection violations. The 2023 Health Law and the Personal Data Protection Law are crucial in guaranteeing patient rights and the obligations of service providers. Law No. 17 of 2023 concerning Health and Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) affirm the obligation of healthcare facilities and digital service providers to maintain the confidentiality, security, and use of patient data in accordance with the principles of prudence and explicit consent. However, the provisions in these laws are considered insufficient to provide general prevention measures to prevent the possibility of personal data leaks originating from healthcare services, including telemedicine services, as early as possible. To ensure that personal data management is carried out very carefully and cautiously by telemedicine service providers, it is possible to consider the application of more serious sanctions in this case criminal liability against the telemedicine service provider as the controller of personal data in the event that personal data is distributed illegally from management activities carried out using the legal liability theory approach from Hans Kelsen which states "Failure to exercise the care required by law is called negligence, and negligence is usually seen as another type of error (culpa)".

REFERENCES

[1] Adelina Yussy Mannas and Siska Elvandari, (2022), "Legal Aspects of Telemedicine in Indonesia", 1st Edition Rajawali Pers, Depok
[2] Asti Dwiyanti, et al., (2024), “Introduction to Criminal Law: Theory, Principles, and Implementation”, PT. Green Pustaka Indonesia, Jakarta
[3] Christian Daniel Tombokan et al., (2024), Legal Protection of Patient Data Confidentiality in Misused Online Health Service Applications, Lex Privatum. Vol 14 No 4, p. 2
[4] Damasus Darma Wulan et al., (2022), Legal Study of Telemedicine Services in Providing Protection of Patient Personal Data, Cahaya Mandalika Journal, p. 7
[5] Yussy Adelina Mannas, Siska Elvandari, (2022), Legal Aspects of Telemedicine in Indonesia, Depok: Rajawali Pers, p. 16
[6] Wahyu Andrianto and Atika Rizka Fajrina, (2021), Comparative Review of Telemedicine Implementation Between Indonesia and the United States, Indonesian Health Law Journal, p. 71
[7] Ahmad Hariri, Puspa Pamela, et al., (2024), Telemedicine: Health at Your Fingertips, Indonesia's Intellectual Pearl
[8] Minister of Health Regulation No. 20 of 2019 concerning the Provision of Telemedicine Services Between Health Service Facilities.
[9] Max Bonsapia, Jumiran, (2025), “Legal Aspects of Telemedicine in Indonesia”, Journal of Legal Studies “THE JURIS” Vol. IX,. http://ejournal.stih-awanglong.ac.id/index.php/juris
[10] Fauzullail, Ahmad Rifki. (2023), "Legal Protection for Patients According to the Minister of Health Regulation Number 20 of 2019 Concerning the Implementation of Telemedicine Services Between Health Service Facilities", Scientific Journal, Faculty of Law, University of Mataram, p. 10
[11] Edy Susanto, Adhani Windari, and Rizkiyatul Amalia, (2024), EDIKASI: Empowering Data Integrity and Knowledge on Health Information Release in the Digital Era, pp. 113-117.
[12] Budhijanto Danrivanto, (2021), Personal Data Protection Law in Indonesia, Bandung: PT.Refika Aditama,.
[13] Health Law, Law No. 36 of 2009, LN No. 144 of 2009, TLN 5063, Article 1
[14] Lestari, RD (2021), Legal Protection for Patients in Telemedicine. Journal of Information Horizons, 51–65. https://doi.org/10.54066/jci.v1i2.150
[15] Mohammad Hilman Mursalat, et al., Legal Problems and Principles of Legal Protection in Remote Health Services Using Information and Communication Technology, Padjadjaran Law Axis Journal, P-ISSN: 2715-7202.
[16] Lestari, H. (2020). National Health Insurance Law. Student Library.

OPEN ACCESS

[17] Puteri Alika Rahma Syawalia, Olih Solihin, "Privacy and Protection of Medical Data in the Digital Era", https://www.researchgate.net/publication/394275915_Privacy_And_Protection_of_Medical_Data_In_the_Digital_Era
[18] https://www.hukumonline.com/berita/a/kebocoran-data-pribadi-kemenkes-lt61dc13b07180f/
[19] Smsul Arifin, (2025), Protecting Privacy in the Digital Era: Addressing Leaks of COVID-19 Patient Medical Record Data, Jatim. Tribunnews.Com, https://jatim.tribunnews.com/2025/01/08/melindungi-privasi-di-era-digital-mengatasi-kebocoran-data-rekam-medis-pasien-covid-19.
[20] https://www.tribunnews.com/nasional/2022/09/10/ahli-digital-forensik-beberkan-penyebab-bocornya-247-juta-data-nik-peserta-bpjs-kesehatan
[21] Calvin Anthony Putra and Muhammad Ali Masnun, (2022), Analysis of Hospital Liability Regarding Potential Leaks of Electronic Medical Record Data Due to Cyber Crime, Novum: Jurnal Hukum, pp. 191–200.
[22] Aenun Nadiroh, Sidi Ahyar Wiraguna, (2025), Legal Analysis of Data Leaks in Digital Health Services: Case Study of Telemedicine Applications in Indonesia, Indonesian Legal Media, Vol, 2, No. 6, P. 313-320
[23] Kelsen, Hans, (2018), Pure legal theory: Basics of Normative Legal Science Hans Kelsen, Translator, Raisul Muttaqien editor Nurainun Mangunsong. Bandung: Nusa Media.
[24] Salim HS and Erlies Septiana Nurbani, (2009), Application of Legal Theory in Dissertation and Thesis Research, Second Book, Rajawali Pres, Jakarta, p. 7.
[25] Devara, IGDG, Dewi, AASL, & Ujianti, NMP (2020), Legal Protection of Personal Data of Online Transportation Service Users, Journal of Legal Preferences, https://doi.org/10.22225/jph.1.1.2259, pp. 1-7

OPEN ACCESS