

**THE URGENCY OF LEGAL PROTECTION AGAINST THE
IMPLEMENTATION OF ELECTRONIC INFORMATION
TECHNOLOGY-BASED MEDICAL RECORDS IN REGULATION OF
THE MINISTER OF HEALTH OF THE REPUBLIC OF INDONESIA
NUMBER 269 OF 2008**

**Dany Try Hutama Hutabarat^{1*}, Rusti Zebua², Rini Andriani Sitorus³,
Febby Andriana Subakti⁴, Hikmah Ramadhani⁵, Juliana Mangunsong⁶,
Firma Nduru⁷, Gusthi Sulistio Alfah⁸, Julio Calvin Dheo Pasaribu⁹, Rado Maruli Malau¹⁰,
Ibnu Anhar¹¹, Patria Sahdan¹²**

¹⁻¹² Faculty of Law, Asahan University

E-mail: ¹⁾ danytryhutamahutabarat@gmail.com, ²⁾ rustizebua@gmail.com, ³⁾ riniistr77@gmail.com,
⁴⁾ Febbysurbakti@icloud.com, ⁵⁾ hikmahramadhanixiimia@gmail.com,
⁶⁾ julimangunsong3@gmail.com, ⁷⁾ ndrurufirmannnduru@gmail.com, ⁸⁾ Gusthi2017@gmail.com,
⁹⁾ dheopasaribu@gmail.com, ¹⁰⁾ radomalau5@gmail.com, ¹¹⁾ anharibnu4@gmail.com,
¹²⁾ patriasahdan76@gmail.com

Abstract

Indonesia is a country that until now has not have a single law laws specifically regulating the protection of personal data. Lately there have been many cases in the community regarding the misuse of personal data. Especially with the increasingly easy public access to the internet so that the misuse of personal data through electronic media will spread quickly. In the field of health services, the patient's personal data cannot be separated from the possibility of abuse. It would be even more dangerous if the personal data is a trace of the patient's medical record which is indeed highly confidential. The use of Information and Communication Technology (ICT) in health services aims to improve access, efficiency, effectiveness, and quality of medical processes that involve medical service organizations in hospitals, clinics, health centers, medical practitioners both doctors and therapists, laboratories, pharmacies, insurance also involving patients as consumers. However, in the process of service using the E-health program, it will collect a number of consumer personal data which is sensitive personal data and lead to new legal issues, namely the extent to which the health service provider can protect patient personal data can be accessed, disseminated more easily through the progress of ICT. So far, the existing regulations have not provided maximum protection for patient personal data because the arrangements are still sectoral and are scattered in several laws and regulations.

Keywords: Urgency, Legal Protection, Personal Data

1. INTRODUCTION

As stated in the Pancasila and the 1945 Constitution of the Republic of Indonesia, the Unitary State of the Republic of Indonesia comprises of seventeen thousand islands, diverse ethnic groups and customs, but a single objective and ideal as a state. To accomplish and attain a single objective and objective for these values, a strategy that is more specific on the attainment of state objectives is required. According to the Preamble to the 1945 Constitution

of the Republic of Indonesia, the purpose of the state is to protect the entire Indonesian nation and the entire Indonesian homeland, as well as to promote public welfare, educate the nation's life, and participate in implementing a world order based on independence, eternal peace, and social justice. In accordance with Article 4 of Law Number 25 of 2004 pertaining to the National Development Planning System, the National Long-Term Development Plan is formulated as an elaboration of the objectives of the establishment of the Government of the State of Indonesia as stated in the Preamble to the 1945 Constitution of the Republic of Indonesia National development (Sudja'i & Mardikaningsih, 2021). National development is a set of sustainable development activities that include all aspects of community, national, and state life in order to carry out the duty of achieving national goals as stated in the Preamble to the Republic of Indonesia's 1945 Constitution (Junef, 2021).

This series of development initiatives consists of continuous development actions that raise the level of community welfare from one generation to the next. The implementation of these activities is conducted with consideration for the ability of future generations to meet their own demands. Health development as an integral component of national development is essentially the implementation of health efforts to attain the ability to live a healthy life for every population to realize optimal health degrees and is a major contributor to the development and growth of Human Resources as National Development Capital. One of the goals of the National Development is a healthy Indonesia in 2010, specifically by improving the quality of community resources that are healthy, intelligent, and productive. Efforts to improve (promotive), prevent (preventive), heal (curative), and recover (rehabilitate) at this time are equipped with technological means to make it more effective, efficient, and facilitate the delivery of health services to patients (Effendy, 1998; Nurmala, 2020). In accordance with the government's Health Development program and in order to realize the Healthy Indonesia Vision 2025, the Health Development mission is to increase and utilize health resources, including health human resources, health financing, and pharmaceutical preparations and medical devices. Health resources consist of mastery of health/medical science and technology, as well as data and information whose importance is growing.

In addition to the large population advantage, health care technology innovation faces additional obstacles. Indonesia is a country with 171.2 million internet users (results of an Indonesian Polling survey conducted in partnership with the Indonesian Internet Service Providers Association / APJII) (Franedya, 2019), however there is not a single regulation that regulates the security of personal data. The Personal Data Protection Draft Law (also refers to RUU) has been included in the National Legislation Program (*Prolegnas*) since 2016, although the bill offered by the government, in this case the Ministry of Communication and Information (*Kominfo*), has not yet been ratified. Recently, there have been numerous instances of the exploitation of personal data in the community. Due to the ease with which people can use the internet, the misuse of personal information via electronic media will expand swiftly. As of November 2018, the Jakarta Legal Aid Institute (LBH) had received 1.330 complaints against online loan providers for alleged violations of the law and human rights (Nursaidi, 2021).

After further examination, at least fourteen alleged infractions were identified, including the disclosure of personal information to coerce borrowers into returning the money immediately. Article 1 paragraph 3 of the 1945 Constitution of the Republic of Indonesia

describes Indonesia as a legal state. This indicates that Indonesia is a law-based nation. In and of itself, legal protection becomes an indispensable component and consequence of the rule of law. The government must protect the legal rights of its citizens. Legal protection is an acknowledgement of the humanity of a country's residents. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia mandates the protection of personal data, stating that "everyone has the right to personal protection, family, honor, dignity, and property under their control, as well as the right to a sense of security and protection from the threat of fear to do or not do something, which is a human right." The issue of protecting personal data emerges due to worries about privacy violations that individuals and/or legal entities may encounter. Invasion of privacy can result in both money and moral losses, such as the destruction of a person's or institution's reputation.

Personal information in the healthcare industry cannot be isolated from the risk of abuse. It will be even more dangerous if the personal data is a patient's medical record track data, which is in fact highly confidential, so that there are a number of special regulations, such as Law Number 29 of 2004 concerning Medical Practice, which stipulates that every Doctor and Dentist in carrying out medical practice must make every effort to protect the confidentiality of patients' medical records. This medical record and medical record must be kept confidential by the physician or dentist as well as the facility's administrator (Rocca et al., 2012; Steward, 2005). Then, the Regulation of the Minister of Health Number 269 of 2008 about Medical Records says that doctors shall maintain the confidentiality of patient identity, diagnosis, disease history, examination history, and medical history information.

The request must be made in writing to hospital administration. Additionally, Ministry of Health regulations controls the ownership, benefits, and obligations associated with the management of Medical Records. The medical record file is the property of the health care facility, whereas the summary of the record is the patients. The summary may be delivered, recorded, or copied by the patient, an authorized individual, or with the patient's or his family's written agreement if they are entitled to it. The utilization of Information and Communication Technology (ICT) to link Community Health Centers and Hospitals utilizing electronic health (e-health) applications has become a global concern.

The use of e-health applications aims to improve access, efficiency, effectiveness, and quality of medical processes involving medical service organizations in hospitals, clinics, health centers, medical practitioners both doctors and therapists, laboratories, pharmacies, insurance also involving patients as consumers; however, in the service process using the E-health program, a number of sensitive personal data will be collected from consumers, which raises new privacy concerns. If a data provider or third party misappropriates a person's personal information, this violates fundamental human rights, especially the protection of a person's privacy and personal information, which are safeguarded by international, regional, and national instruments. There is currently no legislation in Indonesia that safeguard citizens against the arbitrary use of personal data by the government, private companies, or individuals (Dewi, 2016).

In order to offer legal protection for patients' personal data in Indonesian health services based on health information technology, it is necessary to conduct this research and develop an appropriate regulatory model. Information and communication technology has altered the behavior of society and human civilization on a global scale, where information technology has rendered the world borderless and accelerated the occurrence of fundamental social

changes. In addition to contributing to the enhancement of human happiness, progress, and civilization, information technology is currently an effective way of breaking the law.

In connection with the explanation of Article 26 paragraph (1) of Law No. 11 of 2008 on Information and Electronic Transactions, there are regulations that specifically regulate the use of personal data (in this case personal data as privacy), which is regulated in Article 84 paragraph (1) of Law No. 23 of 2006 on Population Administration, as this Article reads: "(1) Resident's Personal Data that must be protected contains: a. Family Card (KK) number; b. National Identity Number (NIK); c. Date of Birth." Although it is guaranteed by the 1945 Constitution of the Republic of Indonesia and controlled by Law No. 11 of 2008 about Information and Electronic Transactions (ITE) and its revisions, the right to privacy is not universally recognized.

Based on this background, the following legal concerns will be examined in this article: How does Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) as amended by Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE) inform the legal protection of patients' personal data in health information technology-based health services? (2) How urgent is the legal protection of patients' personal data in Indonesian technology-based health services? These are the objectives of this study: (1) Analyze the application of legal protection to patient's personal data in existing technology-based health services; (2) Evaluate the need for legal protection of patient's personal data in technology-based health services in Indonesia. This magazine publishes literary or library research, which is a study conducted by examining books or books connected to this research that originate from libraries (library materials). All sources consist of textual (printed) materials and other (electronic) literature pertaining to research issues.

2. THEORETICAL BASIS

Positive legal theory (The Pure Theory of Law) aims to solve the questions of what the law should be and how it is created. Hans Kelsen's Pure Theory of Law has emancipated the science of law from any external components. The theory restricts the understanding of law to the law itself and removes anything else that is not the purpose of understanding law (Kelsen, 2011).

All legal problems are addressed and handled as systemic issues. The system of law is a system of legal rules. A norm is considered legitimate if its substance can be derived from the highest norm. The author will utilize The Pure Theory of Law as a legal theory to determine the elements and indications of the current importance of legal protection of patient's personal data in technology-based health services in Indonesia.

According to experts, several definitions of legal protection include providing protection for human rights that have been harmed by others and granting protection to the community so that it can enjoy all the rights allowed by law (Rahardjo, 2007). Legal protection for the people, according to another viewpoint, is a preventive and coercive government action. Preventive legal protection attempts to avoid disputes from happening, directing government activities to be cautious when making judgments based on discretion, whereas repressive legal protection aims to settle problems, including their adjudication by the courts (Hadjon et al., 2005).

Personal data is information on an individual's attributes, name, age, gender, education, occupation, address, and family status (Li et al., 2021). Another meaning of "personal data" is private and confidential information in the form of a person's identity, code, symbol, letter, or number (Latumahina, 2014).

There is frequent exploitation of personal data by the government and private parties; hence, it is vital to have accommodating legislation that can give guarantees and protection for personal data so that personal data cannot be misused. Each jurisdiction distinguishes between personal information and personal data using a distinct nomenclature. However, the two phrases have essentially the same meaning, therefore they are frequently used interchangeably. For instance, the United States, Canada, and Australia use the phrase personal information, but the European Union, Malaysia, and Indonesia use the term personal data in the ITE Law (Dewi, 2016).

Patient Personal Data refers to information that has a formal relationship with patients and health service providers, including but not limited to patient information supplied to health service providers during the registration process. Currently, almost all health service providers in Indonesia employ technology support (hardware and software) for processing patient data information in terms of storage, searching, and sharing, as well as for communication and decision-making.

Information technology has negative effects that must be recognized and expected in addition to all of the benefits that can be derived from its application in health services. Negative effects may include unsafe equipment, breach of privacy, data theft, and lack of patient contact. The size is qualitatively determined by Law no. 11 of 2008 concerning Information and Electronic Transactions (ITE), as amended by Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions (ITE), as well as other laws and regulations, in an effort to guarantee legal certainty and legal protection in order to protect patients.

3. RESEARCH METHOD

The approach in research is divided into two, namely a qualitative approach and a quantitative approach. In writing this journal, the approach used is a qualitative approach, namely an approach that in processing and analyzing data does not use numbers, symbols and or mathematical variables but with in-depth analysis. In the discussion, the researcher uses a normative juridical approach, which is a type of approach using the provisions of the legislation in force in a country or a doctrinal legal approach method, namely legal theories and opinions of legal scientists, especially those related to the issues discussed (Mertokusumo, 1999). The juridical-normative approach used in this research is the approach through positive law, namely examining positive legal rules to find the importance of legal protection of patient personal data in technology-based health services in Indonesia. This paper uses secondary data, namely: (Arikunto, 2013)

1. Primary legal materials are binding legal materials (Arikunto, 2013) such as the 1945 Constitution; Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE); Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and other laws and regulations.

2. The secondary legal materials used in this paper are materials that can help develop the primary legal materials that have been used, such as academic manuscripts. Draft laws, research, or legal expert doctrine.
3. Tertiary legal materials used in this paper are materials that can help develop primary and secondary legal materials, including dictionaries and encyclopedias (Amiruddin & Asikin, 2006). Other materials that are the object of research are Books and Legislation on Personal Data Protection Law, Information Technology Law, and Consumer Protection Law. In addition, to complete the data and information, it is also necessary to understand by interviewing parties related to the theme of writing this scientific article.

Other materials that are the object of research are Books and Legislation on Personal Data Protection Law, Information Technology Law, and Consumer Protection Law. In addition, to complete the data and information, it is also necessary to understand by interviewing parties related to the theme of writing this scientific article.

4. RESULT AND DISCUSSION

4.1. Legal protection of patient's personal data in health information technology-based health services based on Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE).

The rules governing the protection of personal data in Indonesia are still weak and general because they are contained in a number of separate laws and regulations, they only describe the concept of personal data protection in general, and they are only set forth in the form of a Ministerial Regulation. Some of these separate laws are included in the Information and Electronic Transactions (ITE) Law No. 11 of 2008, the Law No. 43 of 2009 on Archives, the Law No. 8 of 1997 on Company Documents, the Law No. 10 of 1998 on Amendments to Law No. 7 of 1992 on Banking, the Law No. 36 of 2009 on Health, the Law No. 36 of 1999 on Telecommunications (Telecommunication Law), and the Law No. 24 of 2013 on Amendments to Law No. 23 (*UU Adminduk*). In addition to some of the implied regulations stated above, the Indonesian Constitution (UUD NKRI 1945) has provisions for the protection of personal data.

Article 28 G, paragraph 1 states, "Everyone has the right to personal safety, family, honor, dignity, and his own property" (Supriadi, 2019). Several articles of the ITE Law govern the protection of personally identifiable information. This law does not contain strong and exhaustive requirements for the protection of personal data. However, this law indirectly gives rise to a new notion of the protection of both public and private electronic data and information. In addition, the ITE Law's on the Implementation of Electronic Systems and Transactions mandates the disclosure of personal electronic data (PSTE). In accordance with the ITE Law, the security of personal data in an electronic system includes protection against unauthorized use, protection by electronic system operators, and protection against unauthorized access and interference. Regarding the protection of personal data from unauthorized use, Article 26 of the ITE Law stipulates that the authorization of the data

owner is required for the use of any personal data in an electronic medium. Anyone who breaches this clause is liable for any resulting damages.

In his explanation, Article 26 of the ITE Law stipulates that personal information is a component of an individual's personal rights. The ITE Law (11/2008 jo. 19/2016) as a generic law contains the norms for protecting personal data in Article 26. In essence, the use of any data and information in electronic media related to a person's personal data must be conducted with the consent of the person concerned or on the basis of positive law (statutory regulations). Essentially, this clause provides two justifications for the processing of personal data: (a) consent; and (b) positive legal norms. These two tenets form the foundation of legal data processing.

4.2. The urgency of legal protection of patient's personal data in technology-based health services in Indonesia

According to Lubis et al. (2016) of the International Islamic University Malaysia, Law Number 11 of 2008 concerning Electronic Information and Transactions is still largely ineffective in regulating the use of personal data, as the articles of the ITE Law contain only general provisions and do not elaborate on various issues. It is currently the subject of significant international discussion. Based on the above description, it is clear that the rules governing the Protection of Indonesian Personal Data are still of a broad nature and are located in distinct laws and regulations.

In addition, it is hoped that the Indonesian government and parliament will immediately discuss the Personal Data Protection Bill so that Indonesia is better prepared to face the challenges of the digital economy, can provide security guarantees for users' personal data, and can impose severe penalties on parties who misuse the personal data of others. Recently, there have been numerous instances of the exploitation of personal data in the community. Due to the ease with which people can use the internet, the misuse of personal information via electronic media will expand swiftly.

As of November 2018, the Jakarta Legal Aid Institute (LBH) had received 1,330 complaints against online loan providers for alleged violations of the law and human rights. Following a thorough investigation, at least 14 alleged violations were identified, including the disclosure of personal information to pressure borrowers to return the money immediately. The potential for misuse of patient data in technology-based health services in Indonesia is not significantly different from these examples.

It will be even more dangerous if the personal information is a patient's medical record track data, which is in fact highly confidential. As a result, there are a number of special regulations, such as Law Number 29 of 2004 concerning medical practice, which mandates that every doctor and dentist conducting medical practice must create a medical record, which must be kept confidential by the doctor or dentist and the head of the health service facility. Subsequently, Regulation of the Minister of Health Number 269 of 2008 concerning Medical Records specifies that doctors, management officers, and leaders of health facilities shall maintain the confidentiality of a patient's name, diagnosis, disease history, examination history, and medical history.

The request must be made in writing to hospital administration. Additionally, this Ministry of Health regulations controls the ownership, benefits, and obligations associated with the management of Medical Records. The medical record file is the property of the

health care facility, whereas the summary of the record is the patients. The summary may be delivered, recorded, or copied by the patient, an authorized individual, or with the patient's or his family's written agreement if they are entitled to it. The utilization of Information and Communication Technology (ICT) to link Community Health Centers and Hospitals utilizing electronic health (e-health) applications has become a global concern.

The use of e-health applications aims to improve the accessibility, efficiency, effectiveness, and quality of medical processes involving medical service organizations in hospitals, clinics, health centers, medical practitioners both doctors and therapists, laboratories, pharmacies, and insurance, as well as patients as consumers. Nonetheless, the service process utilizing the E-health program will collect a number of sensitive consumer personal data, which raises new legal issues, namely the extent to which health service providers can protect patient personal data, which can be accessed and disseminated more easily as a result of ICT advancements.

Whenever a data provider or third party misappropriates a person's personal information, this violates fundamental human rights, especially the protection of a person's privacy and personal information, which are safeguarded by international, regional, and national instruments. Until date, Indonesia has lacked legislation that safeguard its residents against the arbitrary use of personal data by the government, commercial companies, or individuals (Dewi, 2016). In order to ensure legal protection for patients' personal data in Indonesian health services based on health information technology, it is essential to develop an appropriate legislative framework.

5. CONCLUSION

Based on the discussion above, it can be concluded that the number of cases that exist in the community regarding the misuse of personal data cannot be separated from the easier it is for people to access the internet so that the misuse of personal data through electronic media will spread quickly. The issue of protection of personal data arises because of concerns about privacy violations that can be experienced by individuals and or legal entities. Violation of privacy can cause losses that are not only material but also moral, namely in the form of destroying the good name of a person or institution. In the health sector, personal data cannot be separated from the possibility of misuse, it will be even more dangerous if the personal data is a patient's medical record data which is indeed very confidential, so there are several special regulations such as Law No. medicine which stipulates that every Doctor and Dentist in carrying out medical practice must make a medical record and this medical record must be kept confidential by the Doctor or Dentist and the head of health service facilities. Then, the Regulation of the Minister of Health Number 269 of 2008 concerning Medical Records states that although information about the identity, diagnosis, disease history, examination history and patient treatment history must be kept confidential by clinicians, management officers and leaders of health facilities, this information can be disclosed, among others to fulfill requests from law enforcement officials on court orders and fulfill requests from institutions/institutions in accordance with the provisions of the legislation.

The suggestions from this research are that although it has been guaranteed in the 1945 Constitution of the Republic of Indonesia, and is also regulated in Law Number 11 of 2008

concerning Information and Electronic Transactions (ITE) and its amendments, it is not sufficient to guarantee a legal protection for personal data of a person or patient in a health service based on Health Information Technology. Indonesia also feels that it is very necessary to immediately apply special rules regarding the protection of personal data which are legalized in the form of a law. It is hoped that the existence of strict and adequate regulations can provide security for users of information technology and also in particular can improve technology-based health services.

In addition to having strict and adequate regulations to provide security for information technology users in order to improve technology-based health services, it is also important to establish an institution that functions as a regulator, supervisor and controller (independent regulatory body), or a personal data protection commission. Instead, this supervisory task is left to the government, in accordance with their respective sectors, in coordination with the Minister of Communication and Information Technology. This means that the Ministry of Home Affairs will oversee personal data related to population, Financial Service Authority (OJK) will oversee personal data related to finance and banking, and the Ministry of Health will oversee personal data related to patient medical records.

REFERENCES

- Amiruddin, & Asikin, Z. A. (2006). *Pengantar Metode Penelitian Hukum*. PT. Raja Grafindo. .
- Arikunto, S. (2013). *Prosedur penelitian suatu pendekatan praktik*.
- Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, 5(1), 35–53.
- Effendy, N. (1998). *Dasar-dasar keperawatan kesehatan masyarakat*.
- Franedya, R. (2019). Survei: Pengguna Internet di RI Tembus 171, 17 Juta Jiwa. *CNBC Indonesia*.
- Hadjon, P. M., Martosoewignjo, S. S., & Basah, S. (2005). *Pengantar hukum administrasi Indonesia*.
- Junef, M. (2021). Penegakkan Hukum Dalam Rangka Penataan Ruang Guna Mewujudkan Pembangunan Berkelanjutan. *Jurnal Penelitian Hukum P-ISSN*, 1410, 5632.
- Kelsen, H. (2011). *General Theory Of Law and State*, diterjemahkan oleh Rasisul Muttaqien. Nusa Media.
- Latumahina, R. E. (2014). *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*.
- Li, X., Liu, X., & Motiwalla, L. (2021). Valuing Personal Data with Privacy Consideration. *Decision Sciences*, 52(2), 393–426.
- Lubis, M., Kartiwi, M., & Zuhuda, S. (2016). Election fraud and privacy related issues: addressing electoral integrity. *2016 International Conference on Informatics and Computing (ICIC)*, 227–232.
- Mertokusumo, S. (1999). *Mengenai Hukum Suatu Pengantar*, Cet. Ke-4, (Liberty, Yogyakarta, 2008).
- Nurmala, I. (2020). *Promosi Kesehatan*. Airlangga University Press.

- Nursaidi, N. A. (2021). *Perspektif Hukum Positif dan Hukum Ekonomi Syariah terhadap Perlindungan Hukum Nasabah (Customer) dalam Transaksi Pinjaman Online (Fintech)* [Doctoral dissertation]. Universitas Islam Negeri Alauddin Makassar.
- Rahardjo, S. (2007). *Membangun polisi sipil: Perspektif hukum, sosial, dan kemasyarakatan*. Gramedia Pustaka Utama.
- Rocca, W. A., Yawn, B. P., Sauver, J. L. S., Grossardt, B. R., & Melton, L. J. (2012). History of the Rochester Epidemiology Project: half a century of medical records linkage in a US population. *Mayo Clinic Proceedings*, 87(12), 1202–1213.
- Steward, M. (2005). Electronic medical records: privacy, confidentiality, liability. *The Journal of Legal Medicine*, 26(4), 491–506.
- Sudja'i, & Mardikaningsih, R. (2021). Correlation Of Worker Welfare And Industrial Relations. *CASHFLOW: Current Advanced Research On Sharia Finance And Economic Worldwide*, 1(1), 29–32.
- Supriadi, D. (2019). *Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya*.