 ISSN: 2963-0584

LEGAL PROTECTION OF PATIENTS FROM LEAKAGE OF ELECTRONIC MEDICAL RECORDS DATA IS REVIEWED FROM LAW NUMBER 27 OF 2022 CONCERNING PERSONAL DATA PROTECTION AND LAW NUMBER 17 OF 2023 CONCERNING HEALTH

Teuku Renardiansyah Akhmad[1]; Nugraha Pranadita[2]; Syahrul Machmud[3]
Master of Laws at Langlangbuana University[1,2,3]
Email : teuku.rnr@gmail.com

ARTICLE INFO

Article history :
Received : Mar 1, 2023
Accepted : Apr 2, 2024
Published : May 6, 2024

Keywords :
Personal Data Protection,
Legal Protection,
Electronic Medical Records,
Data Leakage

ABSTRACT

This research aims to analyze legal protection for patients regarding Electronic Medical Record (RME) data leaks by referring to Law Number 27 of 2022 concerning Personal Data Protection and Law Number 17 of 2023 concerning Health. The research method used is a normative juridical approach using descriptive analysis methods. The results of the analysis show that legal protection for patients against electronic RME data leaks is provided through the provisions regulated in these two laws. The main conclusion from this research is that the PDP Law provides protection in the form of information related to personal data, the right to lawsuit or compensation, as well as administrative and criminal sanctions. Meanwhile, the Health Law emphasizes the obligation to maintain the confidentiality of patient health data and stipulates the legal responsibility of hospitals for losses arising from negligence in maintaining the confidentiality of patient medical data. Although there are no implementing regulations yet, both laws provide guidelines and provisions regarding the protection of personal data, including medical data such as RME. This conclusion underscores the importance for healthcare providers to comply with data protection principles in the collection, use, storage and deletion of patient personal data.

INTRODUCTION

Protection of personal data, including medical data, is very important in the context of protecting human rights and public security in general. Health is the basic right of every individual guaranteed by law to protect citizens from threats to health. This concept is reflected in the 1945 Constitution, Article 28H Paragraph 1, which states that: "Everyone has the right to live in physical and spiritual prosperity, to have a place to live, and to have a good living environment and the right to receive health services."

Article 34 paragraph (3) of the 1945 Constitution also emphasizes the government's role in providing health facilities that the State is responsible for providing adequate health service facilities and public service facilities. The state's responsibility is to ensure the rights of every citizen to achieve a good, healthy and prosperous life physically and mentally. This is done in order to achieve national goals, which involve the protection of all Indonesian people and Indonesian descendants to improve general welfare in accordance with the provisions of the 1945 Constitution.

Medical records, as an integral part of the health system, play an important role in understanding and maintaining an individual's health. Electronic Medical Records (RME) is a modern innovation in health information management that utilizes technology to store, manage and exchange health information electronically. The information/data in RME is an important component in the health system, functioning as a complete collection of information regarding patient identity.

 ISSN: 2963-0584

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and Law Number 17 of 2023 concerning Health (Health Law) provide the legal basis for the protection of personal data, including medical record data, both electronically and non-electronic. Articles 35-39 of the Personal Data Protection Law emphasize the obligation of each sector to ensure the security and confidentiality of personal data, including in the context of health services. Article 296 paragraph (5) of the Health Law confirms the confidentiality of medical record data, that "medical records as intended must be kept and maintained confidentially by medical personnel, health workers and heads of health service facilities." Article 297 paragraph (3) of the Health Law also confirms almost the same sentence that "health service facilities are obliged to maintain the security, integrity, confidentiality and availability of data contained in medical record documents." Article 4 paragraph (1) letter i of the same Law also confirms that "every person has the right to obtain confidentiality of their personal health data and information."

Although implementing regulations for the Health Law are not yet available, the law provides an overview of important provisions related to medical records. The explanation of Article 173 letter (c) of the Health Law confirms the meaning of medical records, that:

"Medical records are documents containing patient identity data, examinations, treatment, procedures and other services that have been provided to patients which are created using an electronic system intended for maintaining medical records. "In the event that a Health Service Facility cannot maintain electronic medical records due to technical obstacles, non-electronic medical records can be used until the obstacles are resolved, and medical record data can be re-entered into the electronic medical record system." Medical records in this context are documents containing important information regarding the patient's health history and treatment which are created and maintained with the aim of providing effective and quality health services.

Since the enactment of the Health Law, every health facility, health worker, medical personnel is required to make RME. This provision is as explained in Article 296 (1) – (5). RME must be prepared immediately after the patient has completed receiving health services. In its implementation, each record in the RME must include the patient's name, time of service, and the signature of the medical worker or health worker who provided the service or action. Through circular NUMBER HK.02.01/MENKES/1030/2023, the Minister of Health emphasized that failure to comply with this obligation will result in administrative sanctions for the health facility concerned. These sanctions can take the form of a written warning, revocation of permits, even revocation of accreditation status.

Technology in the modern era has changed the way medical records are organized and managed. RME emerged as a significant innovation in the handling of health information. This model was created using an electronic system, utilizing technology to replace the traditional method of manual writing. RME is an evolution of traditional medical records and involves the use of information and communications technology to store, manage, and exchange health information electronically. RME utilizes specialized computer systems and software to create, access, and maintain patient health records.

Ludwick and Doucette explained that RME can be described as a computerized health information system. This system provides detailed records of patient demographic data, health allergy history, and laboratory test results. RME also features a clustered collection of research, indicating a need for a decision support system. According to Fraser et al, RME offers a number of advantages compared to manual, paper-based medical record systems. One of its main advantages is its ability to support clinical decision making through a decision support *system* . By using RME, health professionals can more efficiently plan medical actions, care or treatment for patients with the support of more structured and up-to-date information. RME also makes the process of monitoring patient data easier. Patient health information can be recorded, updated and accessed more quickly through digital platforms, enabling more effective monitoring of evolving health conditions. This allows for a quicker response to changes in the patient's condition or adjustments in the treatment plan, which in turn can improve the quality of care provided.

Another advantage is the ease of collecting research data. RME provides researchers with easier access to collect necessary health information, increasing efficiency in the medical and scientific research process. Thus, RME is not only a replacement for manual forms of medical records, but also a tool that facilitates more efficient management of health information and

 ISSN: 2963-0584

supports better decision making in clinical and research contexts. The ability to share data instantly between health services is also another advantage.

According to Dodiet, RME is believed to reduce medical errors and increase patient safety. Medical record management application systems enable easy access to complete and detailed patient medical information, helping healthcare professionals make informed decisions. The potential for medical errors is reduced with accurate information about the patient's medical history, diagnosis, and well-documented treatment. The security of medical information is guaranteed with secure and encrypted storage, preventing unauthorized access and the risk of medical errors. In general, the use of technology in electronic medical records aims to increase the efficiency of health services and provide faster access to medical information. This innovation reflects a commitment to providing health services that are more integrated, responsive and oriented towards patient interests.

RME is basically personal data that must be kept secure and confidential. Article 1 of the PDP Law explains that personal data is data about natural persons who are identified or can be identified individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems. Personal data in the context of RME includes specific and general data. Specific data includes medical history, examination results, diagnosis, treatment plans, and other very important health information. Meanwhile, general data includes name, address, date of birth, gender, nationality.

The security aspect of personal data in the context of patient RME is very important considering the potential risk of personal data leakage which can threaten individual privacy and security. Various cases of leaks of personal data, including health data, have occurred in Indonesia, raising public concerns about security aspects in managing health data.

In this context there are several examples of cases such as: the Ministry of Health data leak where 720 GB of data from 6 million patients was misused by hackers and sold online . This reflects a series of similar incidents in Indonesia where the health data of millions of patients was targeted by hackers. Other cases include the BPJS data leak in 2023, where 18.5 million BPJS user data was hacked and traded, including sensitive information such as NIK, addresses and cellphone numbers. In 2021, data on 230 thousand Covid-19 patients was also suspected of being stolen and sold. A Verizon study shows that the healthcare industry experienced 571 cases of data breaches in a short period of time in 2023, placing it as the most vulnerable sector. Medical data leaks can damage public trust in the healthcare industry and reduce its credibility. Legal consequences may occur if the patient whose data was leaked files a lawsuit. The Global Data Breach Stats (Surfshark) report places Indonesia in third place in data hacking in the world in the third quarter of 2022, with 12.7 million data hacking incidents. This indicates a high risk regarding data security in the country.

Choironi and Heryawan researched the level of satisfaction of clinic doctors in using RME. The results of their research found that the use of RME by clinic doctors still faces a number of obstacles, including security and privacy, limited display, and the need for a stable internet network. Ningtyas & Lubis research shows that 70% of people are worried about personal data leaks regarding their health information. This confirms that although electronic medical records provide an efficient solution for presenting, storing and processing *real-time data* , the main challenge is how to maintain the security and confidentiality of this data in its flow and storage in the system.

Based on research by Tiorentap & Hosizah in the clinic, it was found that there was a non-compliance with the principles of information system security. One of the striking findings is the exchange of information between users. There is even a practice of using one *user-id* by several people which turns out to be a common occurrence.

The security aspect of patient data is very crucial. Especially when medical record data is integrated with all health service providers, which are not limited by regional boundaries. As is known, the data in medical records is confidential, sensitive and personal for each patient, so it needs special attention regarding its security.

Basically, not ensuring the security and confidentiality of patient data at RME is not only a loss for patients, but also a serious threat to public trust in the health system as a whole. This can result in a decrease in trust in health institutions and the government, as well as a potential negative impact on the quality of health services provided. In addition, data leaks can also endanger individual privacy and security, as well as increase the risk of misuse of personal information.

 ISSN: 2963-0584

Therefore, protecting patient data in electronic medical records is very important to ensure the security, confidentiality and integrity of patient health information.
Legal protection is needed for patients when the security and confidentiality of their electronic medical record data is not guaranteed. Legal protection in this context refers to efforts to protect the rights, interests and security of individuals or groups in terms of personal data from misuse or violations of the law.

RESEARCH METHODS

The research method used is a normative juridical approach and descriptive analysis. The normative approach analyzes law based on norms in legislation, while descriptive analysis provides an in-depth description of the observed phenomena. Secondary data from various sources, including primary legal materials such as the Personal Data Protection Law and the Health Law, were used using library data collection techniques. Data analysis was carried out qualitatively with a descriptive approach, ensuring the accuracy and harmony of the data used.

RESULTS AND DISCUSSION

The form of legal protection for patient RME data leaks is reviewed by the PDT Law and the Health Law

Indonesia , as a country that upholds the principle of the rule of law, has its commitment expressly stated in Article 1 paragraph (3) of the 1945 Constitution which states that this country is a rule of law. This principle underlines that all activities, whether carried out by the government or by citizens, must be within the limits set by applicable law. In this context, the main aim is to ensure that the rights and obligations of each individual are guaranteed and protected fairly, as well as to enable the state to act as a supervisor and protector of the interests of the entire society as a whole. With this approach, Indonesia emphasizes that the rule of law is the main basis for regulating social life, both in aspects of government and daily life. The principle of the rule of law also reflects a commitment to maintaining the supremacy of law, where the law applies to all people and institutions, without exception.

In practical terms, the principle of the rule of law is the basis for the formation and implementation of policies and regulations, including in the context of protecting patient electronic medical record (RME) data. By having clear legal rules that apply to all parties, this can encourage the creation of a safe and fair environment for each individual, as well as protect the interests of society as a whole. In this context, RME legal certainty provides a solid basis for stability and order in a society. When legal norms can be clearly understood by all parties, a more structured and orderly environment will be created. Individuals and institutions can plan and make better decisions, because they can anticipate the legal consequences of the actions they take.

To ensure legal certainty, the Indonesian government has regulated several laws, including Law No. 17 of 2023 concerning Health, hereinafter referred to as the Health Law. Data security and confidentiality is regulated through Law No. 27 of 2022 concerning Personal Data Protection, hereinafter referred to as the PDP Law.

The Health Law provides a comprehensive legal framework for regulating various aspects of health in Indonesia. One of the main concerns is the protection of patient health data, including RME data. Meanwhile the PDP Law provides a strong legal basis for protecting the privacy and security of personal data, including RME data. This law sets out the principles of data protection, the rights of individuals regarding their personal data, as well as the obligations of organizations in managing and protecting that data. This law also regulates 3 parties regarding personal data, namely: (i) data owner/data subject, (ii) data controller/collector, and (iii) data processor.

The explanation of Article 173 letter (c) of the Health Law confirms that : "What is meant by "medical record" is a document containing patient identity data, examinations, treatment, procedures and other services that have been provided to patients which are created using the system. electronic equipment intended for maintaining medical records. "In the event that a health service facility cannot maintain electronic medical records due to technical obstacles, non-

 ISSN: 2963-0584

electronic medical records can be used until the obstacles are resolved, and medical record data can be re-entered into the electronic medical record system."

RME, as a type of personal data in the health sector, is important data that is personal and sensitive. This data is patient data which includes examinations, treatment, procedures and services, including specific and general personal data.

General RME data includes information such as the patient's full name, medical record number, complete address, date of birth, gender, marital status, family contacts, as well as details of registration time at a health facility. Apart from that, general medical record data also includes patient clinical information, such as patient identity, date and time of medical treatment, results of history and physical examination, diagnosis, management plan, type of treatment given, and other supporting information. Therefore, the existence of data on RME is very important and must be kept secure and confidential. Moreover, this data is stored in electronic/digital form, the existence of which provides a number of benefits or advantages for all parties (patients and health service providers), but on the other hand there are a number of risks that can be detrimental to both parties, especially for patients, such as leaks/ data hacking.

Even though medical record documents are legally owned by health service facilities, patients still have full access rights to this information, patients can even submit corrections if there is incorrect/valid data in the RME. The provisions for ownership of RME data are as contained in Article 297 paragraphs (1) and (2) of the Health Law. For this reason, legal protection is needed for patients to safeguard and ensure that RME data does not experience leaks. As explained in the previous chapter, legal protection is an effort to protect the rights, interests and security of individuals or groups from abuse or violation of the law. This involves providing legal means and mechanisms to ensure that individual rights are recognized, respected and maintained in accordance with applicable legal provisions. In short, legal protection focuses more on efforts to protect the rights of individuals or groups from legal violations or abuse.

In general, the Indonesian government has provided guarantees for the protection of personal data in its constitution. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia states as follows: "every person has the right to personal protection, family, honor, dignity and property under his control and has the right to a sense of security and protection from the threat of fear of doing or not doing." something that is a human right." This article guarantees individuals' rights to feel safe and protected from various forms of abuse or violation of their privacy, honor and property.

Forms of legal protection for patients against leaks of personal data can be found in the PDP Law. Articles 5 to Article 12 provide the legal basis regarding the rights of individuals/personal data subjects. In short, individuals as owners of personal data have the right to know information about clarity of identity, the purpose of collecting the data, the legal basis underlying the data request, the accountability of the party collecting the data, and how the data will be accessed and used. Apart from that, they also have the right to sue or demand compensation if there is a violation of the protection of their personal data in accordance with the provisions of the law. However, there are certain exceptions, such as in law enforcement or national security cases, where this right may be limited.

Article 46 (1) of the PDP Law stipulates that if there is a failure to protect personal data, the personal data controller is obliged to provide written notification to the personal data subject and the relevant institution within 3 x 24 hours (three times twenty-four hours) at the latest. . Interpretation/Explanation of Article 46 (1) confirms that: " What is meant by failure to protect personal data is a failure to protect a person's personal data in terms of confidentiality, integrity and availability of personal data, including security breaches, whether intentional or unintentional, leading to destruction, loss, unauthorized alteration, disclosure or access regarding personal data sent, stored or processed."

The term "notification" in article 46 above is notification to personal data subjects or general notification via mass media, both electronic and non-electronic. The content of the written notification must at least contain: (1) the personal data that was disclosed, (ii) when and how the personal data was disclosed, (ii) efforts to handle and recover the disclosure of personal data by the personal data controller.

 ISSN: 2963-0584

For anyone who violates the provisions of this article, based on Article 57 (2) and (3), administrative sanctions will be given. These sanctions include:

1. Written Warning: This warning aims to warn violators and remind them of their obligations in complying with personal data protection provisions.
2. Temporary Suspension of Personal Data Processing Activities: If the violation committed by an entity or organization is very serious, a temporary suspension of personal data processing activities may be imposed as a sanction. This aims to stop the violating activity until the problem can be resolved.
3. Deletion or Destruction of Personal Data: As a sanction, violators are required to delete or destroy personal data that they have processed or managed unlawfully. This is done to protect the privacy and security of the data subject's personal data.
4. Administrative Fines: Violators are also subject to administrative fines as a form of sanction. The maximum administrative fine is 2 percent of the violator's annual income or receipts, according to the level of the violation committed.

Article 65 of the PDP Law also states a strict prohibition against actions that violate the privacy and security of personal data. The prohibition covers three main things, namely:

1. Obtaining or collecting personal data that does not belong to them with the intention of benefiting themselves or others, which may result in losses for the personal data subject.
2. Disclosing personal data that does not belong to him.
3. Using personal data that does not belong to him.

For anyone who violates the provisions of this article, criminal sanctions will be given to the violator. This criminal sanction is in accordance with the provisions of Article 67. The article reads:

Article 67

(1) Any person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or another person which may result in loss to the Personal Data Subject as intended in Article 65 paragraph (1) shall be punished by imprisonment for a maximum of 5 (five)) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).
(2) Any person who intentionally and unlawfully discloses Personal Data that does not belong to him as intended in Article 65 paragraph (2) shall be punished by a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000.00 (four billion rupiah).
(3) Any person who deliberately and unlawfully uses Personal Data that does not belong to him as intended in Article 65 paragraph (3) shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of IDR 5,00OOOO,000.00 (five billion rupiah).

Based on the article above, what is meant by each person is an individual and a corporation. Article 70 confirms that if the violation is committed by a corporation, it can be subject to criminal sanctions. Sanctions that can be imposed on corporations include fines, the maximum limit of which is 10 times the regulated fine. Apart from that, corporations can also be subject to additional crimes such as confiscation of profits, freezing of business, prohibition of carrying out certain actions, closure of business, payment of compensation, revocation of permits, and dissolution of the corporation. This aims to put pressure on corporations to comply with personal data protection provisions and prevent similar violations from occurring in the future.

In the context of patient RME data leakage, Article 46, Article 65, Article 67, Article 70 of the PDP Law, provide a solid basis for legal certainty, and at the same time provide legal protection for patients from misuse of personal data or RME data in this context. These articles emphasize that every person/corporation is legally prohibited from carrying out certain actions related to personal data that they do not own, which can include actions taken by parties involved in leaking patient medical data.

Apart from being regulated in the PDP Law, forms of legal protection for leaks of patient RME data are also regulated by the Health Law. However, the regulations in this law are not regulated in detail and completely, this is because there are no derivative/implementing regulations

 ISSN: 2963-0584

from this law to date, especially regarding medical records. However, several articles that are relevant in terms of legal protection for patients in the context of data leaks can be explained in several articles below.

Article 4 paragraph (1) letter i of the Law emphasizes that "every person has the right to obtain confidentiality of his personal health data and information." In this context, patients have the right to protect the privacy and confidentiality of medical information, including data in their electronic medical records. Article 301 of the Health Law also explains the provision that: "every medical worker and health worker in carrying out health services is obliged to keep the patient's personal health confidential." This article implies that medical/health personnel must treat patient health data confidentially and must not disclose it without permission from the patient concerned or without a clear legal basis.

Another provision is in Article 193 which states that: "The Hospital is legally responsible for all losses incurred due to negligence committed by the Hospital's health human resources." This means that if there is a violation of the confidentiality of patient medical data by medical personnel/health personnel/support personnel, whether accidentally or intentionally without any applicable legal basis, the hospital will be legally responsible for the consequences of the violation.

Article 193 above can be seen as one of the legal mechanisms that supports the protection of patient medical data, by placing a clear responsibility on hospitals to ensure the confidentiality and security of patient medical data, including in terms of RME management.

The Relevance of Legislation regarding the Protection of Personal Data with the Protection of Electronic Medical Record Data

Legislation relating to the protection of personal data, especially Law Number 27 of 2022 concerning Personal Data Protection, has significant relevance to the protection of electronic medical record data (RME). Likewise with Law Number 17 of 2023 concerning Health which provides a legal framework for regulating health practices and protecting patient data.

The PDP Law provides a very important legal basis for managing or guaranteeing the security and confidentiality of personal data, including in this context personal data in the form of electronic medical record data / RME. RME as part of personal data of a specific or general nature, its security must be guaranteed. Even though the government regulations/implementing regulations for these two laws have not yet been issued, they provide sufficient description/provisions regarding personal data/medical data such as RME. In the context of legal protection for patients against RME data leaks, these laws and regulations stipulate obligations for health service providers to maintain the confidentiality and security of patient personal data. This includes provisions on the collection, use, storage and deletion of patient personal data in compliance with established data protection principles.

Both laws provide a framework for regulating patients' rights regarding their personal data, such as the right to know the purpose of data collection, the right to access and update their personal data, and the right to claim compensation in the event of a violation of data protection.
A deep understanding of laws and regulations related to personal and health data protection is essential in protecting patient rights against RME data leaks, which will ensure that technology-based health practices can operate safely, ethically, and in accordance with applicable data protection standards. tall.

CONCLUSIONS AND SUGGESTIONS

Legal protection against patient Electronic Medical Record (RME) data leaks is based on the principle of the rule of law which confirms the right of every individual to be protected from misuse or violation of the privacy and security of their personal data. This form of protection is regulated in the Personal Data Protection Law (PDP) through Articles 5 to Article 12, which stipulates several aspects, including: *First:* Information Rights, patients have the right to know various information related to their personal data, such as clarity of identity, the purpose of data collection, the legal basis for the data request, and how the data will be accessed and used. *Second:* Right to Suit or Compensate, Patients as owners of personal data have the right to sue or demand compensation if there is a violation of the protection of their personal data. This ensures that

individuals can protect the privacy and security of their personal data, including RME data, and hold themselves accountable for breaches. *Third:* Administrative and Criminal Sanctions **,** the PDP Law also provides the basis for imposing administrative and criminal sanctions based on Articles 57 and 67, which aim to provide adverse consequences for personal data violators, including in the context of patient RME data leaks. Legal protection under the Health Law also provides security guarantees for patients, as regulated in Article 4 and Article 301, which confirms that medical personnel and health workers are obliged to keep patient health data confidential. In addition, Article 193 confirms the hospital's legal responsibility for losses arising from the negligence of health human resources in maintaining the confidentiality of patient medical data.

Legislation relating to personal data protection, such as Law Number 27 of 2022 concerning Personal Data Protection, has very important relevance in protecting electronic medical record (RME) data. Likewise with Law Number 17 of 2023 concerning Health, which provides a legal framework for regulating health practices and protecting patient data. The PDP Law provides a significant legal basis for managing and ensuring the security and confidentiality of personal data, including RME. Although these two laws do not yet have complete government regulations or implementing regulations, they provide descriptions and provisions regarding personal data, including medical data such as RME. In the context of legal protection for patients against RME data leaks, these laws and regulations stipulate obligations for health service providers to maintain the confidentiality and security of patient personal data. This includes arrangements for the collection, use, storage and deletion of patient personal data in compliance with established data protection principles.

Some suggestions that can be recommended are as follows:

First: It is necessary to prepare more detailed and detailed implementing regulations to regulate patient RME data management practices more comprehensively. This will help clarify the responsibilities and obligations of the parties involved, as well as provide clear guidance in dealing with data leak situations. *Second:* It is important to increase legal awareness for both health service providers and patients about the rights and obligations regarding the protection of personal data, including RME data. This can be done through training, outreach and public campaigns aimed at increasing understanding of data protection. *Third:* It is necessary to strengthen data security systems in patient RME management practices, including the implementation of encryption and double authentication technology to prevent unauthorized access. Additionally, it is important to regularly update and monitor system security to deal with ever-evolving security threats.

BIBLIOGRAPHY

Books :

Abdul Aziz Hakim. (2015). *State of Law and Democracy in Indonesia, Student* Library Publisher , Yogyakarta, 2nd Printing.

Indonesian Ministry of Education and Culture Language Development and Development Agency. (2016). *Big Indonesian Dictionary (KBBI)* , online version.

Bagir Manan. (2013). *Enforcing the Law of a Search* , AAI, Jakarta.

Bambang Sunggono. (2013). *Legal Research Methodology* , Raja Grafindo Persada, Jakarta.

Dodiet Aditya Setiawan. (2017). *Electronic Medical Record (RME)* , Polytechnic: Surakarta.

Firdaus, Sunny Ummul. (2012). *Medical Records in the Spotlight of Law and Ethics* , Surakarta, UNS Pres.

Gemala R Hatta. (2010). *Guidelines for Health Information Management in Health Service Facilities* , University of Indonesia: Jakarta.

Hans Kelsen. (2013). *General Theory of Law and the State*, Translator: Raisul Muttaqien, Nusamedia, Bandung.

Hotma P. Sibuea. (2010). *Principles of the Rule of Law, Policy Regulations & General Principles of Good Government* , Erlangga, Jakarta.

Yasyfilga's inspiration. (2021). *Juridical Analysis of Patient Protection for Electronic Medical Records by Private Hospitals Based on Law Number 8 of 1999 concerning Consumer Protection,* Thesis, Parahyangan Catholic University.

Jimly Asshiddiqie. (2012). *The Idea of the Indonesian Rule of Law, National* Law Magazine STIK-PTIK Library, No. 1.
M Soerjono Soekanto. (2006). *Introduction to Legal Research* , Jakarta: UI-Perss.
Mirza Satria Buana. (2012). *The Attractive Relationship Between the Principle of Legal Certainty and the Principle of Justice (Substantial Justice) in the Decisions of the Constitutional Court* , Thesis: Faculty of Law, Islamic University of Indonesia.
Muhaimin. (2020). *Legal Research Methods* , Mataram University Press, Mataram.
Muhammad Tahir Azhary. (2015). *State of Law* , Fifth Cet, Kencana Prenadamedia Group, Jakarta.
Munandar Wahyudin Suganda. (2017) . *Medical Law* , Alfabeta, Bandung.
Muninjaya GAA. (2016). *Health Management 3rd Edition* , Jakarta: EGC.
Salim HS., and Erlies Septiana Nurbani. (2014). *Application of Legal Theory in Thesis and Dissertation Research* , Rajawali Press, 3rd Edition, Jakarta.
Satjipto Rahardjo. (2012). *Legal Studies* , Bandung, Citra Aditya Bakti.
Soerjono Soekamto. (2014). *Introduction to Legal Research* , UI Press, 3rd Edition, Jakarta.
Soerjono Soekanto and Siti Mamuji. (2012). *Normative Legal Research: A Brief Overview, Jakarta,* Rajawali Press.
Silvia Anjani et al. (2023). *Digital Disruption and the Future of Medical Records 1 (Review of Minister of Health Regulation No. 24 of 2022 concerning Electronic Medical Records)* , Yogyakarta: Selat Media Partners.
Thalal, M., & Hiswanil. (2011). *Legal Aspects in Health Services* , IKM Journal: Public Health Sciences.
Tiorentap and Hosizah. (2020). *Information Security Aspects in the Implementation of Electronic Medical Records in MP Medical Check-Up Clinics* , Proceedings 4 of SENWODIPA.
Tjia Siauw Jan. (2013). *Tax Court: Efforts for Legal Certainty and Justice for Taxpayers ,* Alumni, Bandung.
Yusuf & Amri Amir. (2009). *Medical Ethics & Health Law* , ECG: Jakarta,

Scientific journals :
Alfian Listya Kurniawan and Anang Setiawan. (2021). *Medical Record Data Protection as a Form of Protecting Patient Personal Data During the Covid-19 Pandemic, Journal of Law and Economic Development,* Volume 9, Number1, p.95-112.DOI: https://doi.org/10.20961/hpe.v9i1.52586
Arifah Alfiyyah. (2022). *Telemedicine and Electronic Health Record Implementation in Rural Areas: A Literature Review,* Journal of Indonesian Health Policy and Administration, Vol. 7, no. 2, p. 221-228. http://dx.doi.org/10.7454/ihpa.v7i2.4116
Aurellia Vinta Aryanti Bintoro et al. (2022). *Evaluation of Electronic Medical Record Format and Security System in Dental Clinic of the General Hospital in Batam City* , MEDALI Journal, Volume 4, Number 1, p. 1-10. DOI: http://dx.doi.org/10.30659/medali.4.1.1- 10
CA J Sulistya and Rohmadi. (2021). *Review of Readiness for Implementing Electronic Medical Records in Management Information Systems in Hospitals,* Indonesian Journal of Health Information Management, Vol 1, No. 2, p. 1-7. https://doi.org/10.54877/ijhim.v1i2.12
Choironi and Heryawan. (2022). *Perceptions of Clinical Doctors in Using Cloud Computing-Based Electronic Medical Records : Survey on the Use of rekmed.com* , Global Informatics Scientific Journal, Vol. 13, no. 03, p. 176- 181. https://doi.org/10.36982/jiig.v13i3.2691
Davis Giardina et al. (2014). *Patient Access to Medical Records and Healthcare Outcomes: a Systematic Review,* Journal of the American Medical Informatics Association Vol 21 No 4, p. 737-41. DOI:10.1136/amiajnl-2013-002239
Emi Azmi Choironi and Lukman Heryawan. (2022). *Perceptions of Clinical Doctors in Using Cloud Computing-Based Electronic Medical Records : Survey on the Use of rekmed.com,* Global Informatics Scientific Journal , Vol. 13, no. 03, p. 176-181. https://doi.org/10.36982/jiig.v13i3.2691
Fraser et al, (2005). *Implementing Electronic Medical Record Systems in Developing Countries* , Inform Prim Care, Vol 13 No 2, p. 83-95. https://pubmed.ncbi.nlm.nih.gov/15992493/

Hanna Melyanti and Pan Lindawaty Suherman Sewu, (2023). Personal *Data Protection in Electronic Medical Records Regulations Based on Indonesian Laws Linked to Legal Principles* , JIMPS Journal, Vol 8, No3,p.1415-1422. DOI: https://doi.org/10.24815/jimps.v8i3.25191

Imam Subechi. (2012). *Realizing the Indonesian Rule of Law* , Journal of Law and Justice, Volume 1, Number 3, 2012, p. 340-358. DOI: http://dx.doi.org/10.25216/jhp.1.3.2012.339-358

International Convention on Economic, Social, and Cultural Rights. December 16, 1966. Article 12, p. 4. Can also be seen in the Convention on the Elimination of All Forms of Racial Discrimination, Article 5, 21 December 1965.

Lim CSE et al. (2019). *Electronic Medical Records Management Systems: An Overview.* J Library Information Technol, Vol 29, No 6, p. 3-12. DOI: https://doi.org/10.14429/djlit.29.6.273

M. Ehsan Rana, M. Kubbo, and M. Jayabalan. (2017). *Privacy and Security Challenges Towards Cloud Based Access Control in Electronic Health Records* , Asian J. Inf. Technol, Vol. 16, no. 2, p. 2–5. https://paper.researchbib.com/view/paper/92281

Mustajab, Juridical Analysis. (2013). *Legal Relations Between Doctors and Patients in Health Services* , Journal of Legal Studies Legal Opinion, Edition 4, Volume 1, 2013, p.1-11. https://media.neliti.com/media/publications/146294-ID-analysis-juridical-relations-legal-antara-d.pdf

Ningtyas & Lubis. (2018). *Privacy Issues in Electronic Medical Records* , Pseudocode Journal , Volume V Number 2, p. 12-17. https://doi.org/10.33369/pseudocode.5.2.12-17

Raden Minda Kusumah. (2022). *Comparative Analysis Between Electronic and Manual Medical Records,* Journal of Research and Community Service, Vol. 1, No. 9, p. 595-604. https://doi.org/10.59141/comserva.v1i9.67

Rospita Adelina Siregar. (2024). *Implementation of Minister of Health Regulation Number 24 of 2022 concerning Medical Records on the Effectiveness of Health Services,* Kyadiren Legal Science Journal . Vol. 5, no. 2, p. 1-12. https://doi.org/10.46924/jihk.v5i2.182

Saif S, Wani S, Khan SA. (2010). *Network Engineering Solution for Data Sharing Across Healthcare Providers and Protecting Patients Health Data Privacy Using EHR System* . J Global Res in Computer Sci, Vol 2 No 8, 2010, p. 67-72. https://ejournal.unjaya.ac.id/index.php/mik/article/view/561

Sinta Dewi Rosadi, (2016). *The concept of legal protection for privacy and personal data is associated with the use of cloud computing in Indonesia,* Yusti sia Journal , Vol. 5 No. 1, p. 22-30. https://doi.org/10.20961/yustisia.v5i1.8712

Windy Cahyani et al. (2022). *Application of the Professional Code of Ethics for Medical Recorders in the Filing Section in General Hospitals* , Journal of Medical Records, Vol.VII No. 2, p. 61-73. https://ejurnal.stikesmhk.ac.id/index.php/rm/article/view/287

Wirajaya & Dewi. (2020). *Analysis of the Readiness of the Dharma Kerti Tabanan Hospital to Implement Electronic Medical Records ,* Vocational Health Journal , Vol. 5 No. 1, p. 1-9. https://doi.org/10.22146/jkesvo.53017

Zahermann Armandz Muabezi, (2017). *State Based on Law (Rechtsstaats) Not Power (Machtsstaat) Rule of Law and Not Power State,* Journal of Law and Justice, Volume 6 Number 3, November p. 421-446. DOI: http://dx.doi.org/10.25216/jhp.6.3.2017.421-446

Internet Source :

Janne Makdani. (2023). *Implementation of RME Encourages Efficiency and Quality of Health Services in Clinics,* https://aptika.kominfo.go.id/2023/09/implementasi-rme-besar-bisnis-dan-kualitas-pe jasa-kesehatan-di-klinik/ (Accessed on Saturday, 20 November 2023).

Verizon. (2022). *Financial Industry Most Vulnerable to Data Leaks,* https://dataindonesia.id/internet/detail/verizon-industri-keuangan-paling-vulnerable-data-leakage (accessed March 10 2024).

Aviat. (2023). *Challenges of Implementing an Electronic Medical Record System in Indonesia* https://aviat.id/tantangan-penerapan-sistem-rekam-medis-elektronik-di- indonesia/ (accessed March 10 2024).

 ISSN: 2963-0584

Dian Dewi Purnamasari. (2023). *BPJS Employment Investigates Bjorka Claims,* https://www.kompas.id/baca/polhuk/2023/03/14/bpjs-kerja-investigasi- claims -bjorka (accessed March 10 2024).

CNN Indonesia. (2020). *230 Thousand Data on Covid-19 Patients in Indonesia Leaked and Sold* , https://www.cnnindonesia.com/technology/20200620083944-192 515418/230-ribu-data-covid-19-patients-in-Indonesia-leaked-and-sold. (Accessed November 20, 2023).

Constitution :

The 1945 Constitution of the Republic of Indonesia.

Law No. 17 of 2023 concerning Health.

Law No. 27 of 2022 concerning Personal Data Protection.