INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS

ISSN(print): 2643-9840, ISSN(online): 2643-9875

Volume 07 Issue 12 December 2024

DOI: 10.47191/ijmra/v7-i12-07, Impact Factor: 8.22

Page No. 5407-5418

Juridical Analysis on Infrigement against Patients' Electronic Medical Records at Telemedicine Services Based on Indonesia Regulation

Rahandy Rizki Prananda[1], Stella Hita Arawinda[2], Herni Widhanarti[3]

[1,2,3]Faculty of Law, Universitas Diponegoro

ABSTRACT: In order to guarantee privacy protection for the health sector, regulations are needed that can bring benefits, balance and legal certainty in securing medical record data and innovation in health services. This research aims to describe the pattern of legal relations in the provision of telemedicine services, the regulatory capabilities of the health and cyber sectors in Indonesia in preventing and enforcing leaks and misuse of patient electronic medical record data. Next, this article will outline the shortcomings in terms of normative, structural and legal culture in enforcing existing rules in Indonesia regarding electronic medical record data. This research is included in qualitative research with a statutory and conceptual approach. The research results show that electronic medical record data is part of human rights which must be protected and recognized as special property rights in terms of civil law. Legal protection for the confidentiality of patient data in Electronic Medical Records (RME) in Indonesia is well accommodated by a number of regulations, including the Personal Data Protection Law, Minister of Health Regulation on RME, and the Civil Code with fairly good and complementary harmonization between regulations. However, Obstacles are still found in enforcement such as a lack of clear boundaries and procedures for opening medical recorddata and reporting data leaks, the legitimacy of the authority of law enforcers who have the authority to take action and the public's low understanding of the importance of data protection on medical records.

KEYWORD: Telemedicine, Electronic-Medical Record, Patient, Privacy, Legal Protection

I. INTRODUCTION

The industrial era 4.0 is marked by the integration of information systems which is realized by the many start-up companies that produce various kinds of products and services on digital platforms. This phenomenon cannot be separated from the development of internet technology which is able to connect people around the world by erasing physical boundaries in the flowof globalization. The health sector is also developing rapidly with the existence of internet technology, which then allows long- distance consultations through e-health or, in other words, telemedicine. Literally, telemedicine comes from Greek, namely tele which means far and the word medical which means health services by health workers (Lestari, 2021). Meanwhile, according tothe Decree of the Minister of Health of the Republic of Indonesia Number: HK.01.07/MENKES/650/2017 concerning Hospitalsand Community Health Centers Organizing Telemedicine Service Program Trials, that telemedicine is a combination of information and communication technology with medical expertise in health services (consultation, diagnosis and medical procedures) that can be applied remotely (Gondhowiardjo, 2020).

Based on the definition above, it can be understood that the scope of telemedicine is quite broad, including the provision of long-distance health services (including clinical, educational and administrative services), through the transfer of information (audio, video, graphics), using telecommunications devices (interactive audio-video two directions, computers and telemetry) involving doctors, patients and other parties. In simple terms, according to Jamil, Khairan and Fuad telemedicine has actually been applied when there is a discussion between two doctors discussing a patient's problem over the telephone (Jamil, 2015).Telemedicine services facilitate access to health services, where patients as telemedicine users can have consultations to obtain treatment services without visiting a health facility (Kvedar, 2014). Some examples of telemedicine in Indonesia include

Alodokter, Klinik Go, Klinikdok, Good Doctor and Halodoc.

However, security regarding the protection of patient medical record data in telemedicine services in Indonesia is still questionable. This was proven in 2022, the Ministry of Communication and Information of the Republic of Indonesia (hereinafter

referred to as the Indonesian Ministry of Communication and Information) discovered that around 6 million patient information in Indonesia was suspected to have been traded on a platform called Raid Forums. The perpetrator of this data sale is believed to use the name Astarte. The seller claims that the data offered comes from the central server of the Ministry of Health of the Republic of Indonesia. The information traded includes images, patient identity details, CT scan results, COVID- 19 tests, and X-ray examination results. (https://nasional.kompas.com/read/2022/01/06/22555491/kemkominfo-telusuri-dugaan- kebocoran-data-pasien-milik-kemenkes.)

Patient medical record data is included in the privacy section of individual legal subjects, where the individual concerned has the right to limit access regarding health conditions. The concept of privacy is closely related to confidentiality, which is maintaining the confidentiality of patient health data by having the right to provide or refuse to provide information to other parties without the data owner's consent. In practice, it is known that legal products which are tools for regulating society in the cyber world or tools of Social Engineering still refer to Law no.19 of 2016 concerning Electronic Information and

Transactions (hereinafter referred to as the ITE Law) which in fact has not been able to accommodate the overall protection of patient data in the cyber world. Patients who become victims of course suffer a number of losses if this leak occurs due to the negligence of the party who should be responsible for maintaining data confidentiality.

The medical record data contains information, both written and recorded, regarding the patient's identity, anamnesis, physical determination, laboratory/radiological examination, diagnosis, all medical services and actions provided to the patient, including outpatient, inpatient and emergency services provided to the patient. . The role of medical records is also very important in measuring the standardized quality of medical services provided by health service providers. Indicators of good medical record quality are the completeness of the content, accuracy, timeliness and fulfillment of aspects of legal requirements. In the event that an error occurs in recording the medical record, the files and records must not be removed or deleted in various ways (Kurniawan, 2021).

The fairly sporadic penetration of telemedicine platforms in society is not only related to efficiency and effectiveness in facilitating services in the health sector, but it is also necessary to pay attention to the existence of regulations that are adaptive and able to overcome the problem of protecting patient medical record data as part of protected privacy. by law. The existence of Telemedicine as a social phenomenon in health services must be responded to responsively by law so as not to injure human values. Providing cyber security and protecting the confidentiality of patient medical record data must be considered by telemedicine application providers. Article 28 H of the 1945 Constitution of the Republic of Indonesia implicitly recognizes the position of patient medical record data as part of human rights, especially individual personal property rights, and these property rights must not be disturbed or misused by anyone. Starting from these legal issues, this research will examine two problem formulations, namely the scope of legal protection that can be provided to patients regarding the security of confidentiality of patient medical record data in the telemedicine platform and identifying patterns of legal relationships that occur between patients and doctors and telemedicine service providers so that they can It is clearly known about the scope of liability following leakage, misuse of patient medical record information and legal countermeasures for violations of medical record data as part of patient privacy.

A number of studies have discussed legal issues related to telemedicine but have different perspectives from this research, including: First, Mohammad Hilman Nursalat, Efa Lailah Fakriah and Tri Handayani entitled "Judicial problems and principles of legal protection in long-distance health services using information technology and Communication" (Mursalat, 2022). This research focuses on the regulation of telemedicine services in Indonesia and legal protection for service recipients & health workers on telemedicine platforms. Furthermore, in a study researched by Andre M. Watulingas et al regarding the Implementation of Legal Protection of the Medical Profession for Telemedicine Services at RSUP Prof. Dr. R. D. Kandou Manado, focuses on implementing the legal protection given to doctors who provide telemedicine services (Watulingas, 2022). Legal research on telemedicine was also carried out by Carolina Kuntardjo in her scientific paper entitled: "Dimension of Ethics and Telemedicine in Indonesia: Enough of Permenkes No.20/2019 as a Frame for Telemedicine in Indonesia?", which found conflicting legal ambiguities regarding the administration of telemedicine. with the principles of non-maleficence (not harming the patient), beneficence (providing the good of the patient), autonomy (respecting the patient's rights) and justice (justice), so that This has the potential to harm the doctor's legal position because they do not carry out direct examination interactions with

Patients (Kuntardjo, 2020).

II. RESEARCH METHOD

This article is included in the type of Normative Legal Research, which is a type of legal research methodology that bases its analysis on applicable laws and regulations that are relevant to the legal issues that are the focus of the research (Benuf & Azhar, 2020).

The statutory approach and conceptual approach are used to outline the legal protection that can be provided to patients using telemedicine according to regulations applicable to the health and cyber sectors for violations of leakage ormisuse of patient medical record data as well as errors in providing health service consultations to patients. Then this study will reveal the legal relationship between the parties involved in the practice of telemedicine, therefore the scope of responsibility for losses experienced by patients can be clearly identified. The data used in this study is secondary data collected through literature study including books, journals, data laws and regulations and other supporting documents related to the legal issue being studied. The research specifications applied are analytical descriptive which aims to describe the research object through the collected data or samples, analysis is then carried out and qualitative conclusions are made (Sugiyono, 2009).

III. RESULT AND DISCUSSION

3.1. Legal Protection to Record Medical-Electronic on Telemedicine's Platform

3.1.1. Mechanism of Telemedicine as the Platform of Health's Service and Legal Position of Each PartiesAccording to Regulations in Indonesia

Litererally, telemedicine comes from the words "tele" which means "long distance", and "medical" means "of a medical nature". In general, telemedicine services are classified as services that use electronic communication facilities to provide medical services or support from a separate distance (not face to face) (Pukovisa Prawiroharjo, Pratama, & Librianty, 2019). The diversity of telecommunications facilities varies greatly, including: telephone, video calls, internet sites, or other sophisticated tools. 19 Apart from that, Telemedicine can also be interpreted as the use of information andcommunication technology (including electronics, telecommunication, computers, informatics) to transfer (send and/or receive) medical information, in order to improve clinical services (diagnosis and therapy) and education (Masa, 2014).

Commonly the definition beneath always misunderstood and overlapping perspective with E-Health is the use of telecommunications and information technology to provide access to health assessment, diagnosis, intervention, consultation, supervision and information across distance (Public Health Institute, 2018)[1]Technologies as telephones, facsimile machines, electronic mall systems, and remote member monitoring devices, which are used to collect and transmit member data for monitoring and interpretation (Public Health Institute, 2018).

Paying attention to the scope of the differences in definitions between telemedicine and telehealth above, it is clear that telemedicine has a more specific meaning, referring to health practices using long-distance methods, or in other words the doctor and patient are in different locations. In telemedicine, doctors cannot provide examinations and consultationservices to patients directly. The communication pattern between patients and doctors is carried out through available media, for example: chat boxes, such as those available in the application to convey complaints they are experiencing. Meanwhile, doctors can only make diagnoses based on the patient's complaints unilaterally.

Telemedicine is an option for patients who need health services, especially in efforts to heal and restore health. Even though the service delivery is on a different platform from conventional health services, its implementation must still pay attention to the three main components of health services, namely informed consent, medical records and medicalconfidentiality. Apart from that, patient safety and protection are also aspects that need to be considered in telemedicine's application.

The telemedicine are divided into two types are real-time (synchronous) and store-and-forward (asynchronous) (Public Health Institute, 2018). Real time telemedicine (synchronous telemedicine) is applied simply by using a telephone or sophisticated equipment such as the use of a surgical robot. Synchronous Telemedicine requires the presence of both parties at the same time, then a liaison media is needed between the two parties that can offer real time interaction so that one party can carry out health care. Another form of Synchoronous Telemedicine is the use of medical equipment that is connected to a computer so that health inspections can be carried out interactively. An example of a telestethoscope is where a doctor listens to a patient's heartbeat remotely.

The concept of direct telemedicine services is also almost the same as this system, where patients and/or doctors interact via teleconference to convey their health problems. Patients directly communicate with doctors/nurses regarding their health complaints and follow up by providing feedback from the nurse/doctor. This type of telemedicine service is very suitable for use when there is a very emergency situation, and requiring direct media action is more important than the loss, inconvenience, and cost (Rizkiyani Istifada, Sukihananto, & Laagu, 2017). In case a life-threatening injury occurs, real-time teleconsultation or synchronous telemedicine will play a more beneficial role compared to store-and-forward telemedicine.

[1] Public Health Institute, *State Telehealth Laws & Reimbursement Policies: A Comprehensive of the 50 States & The District of Columbia*(Center for Connected Health Policy 2018) 27.

Meanwhile, store-and-forward telemedicine (asynchronous telemedicine) includes collecting medical data and sending thisdata to a doctor at the right time for offline evaluation.This type of telemedicine does not require the presence of both parties at the same time.Dermatologists, radiologists and pathologists are specialists who usually use asynchronous telemedicine. Medical records in an appropriate structure should be a component of this transfer (Wootton & Craig, 1999).The concept of indirect telemedicine services is also almost the same as this system, where patients and nurses interact using e-mail as a link between the two. Patients consult about problems or laboratory results with the nurse (Indonesia, 2018). This form of store-and-forward or pre-recorded telemedicine is suitable for use if all the required information can be met without any disturbance for the doctor or medical personnel or the patient who receives it.

Memperhatikan pada pola kerja kedua jenis telemedicine, maka praktek telemedicine tidak mencakup sisi afeksi dikarenakan dokter tidak berurusan secara fisikal dengan pasien dalam mendiagnosa keluhan kesehatan pasien yang dinafikan sebagai pola perubahan gaya hidup baru dengan menekankan bahwa interaksi antara dokter dengan pasien tidak memerlukan sentuhan fisik melainkan cukup dengan melakukan komunikasi verbal atau tertulis melalui suatu platform digital.

Referring to the working patterns of both types of telemedicine, the practice of telemedicine does not include the affection side because doctors do not deal physically with patients in diagnosing patient health complaints which are dismissed as a new lifestyle change pattern by emphasizing that interaction between doctors and patients does not require physical touch but is sufficient. by carrying out verbal or written communication via a digital platform

Telemedicine is regulated in Article 1 number 22 Law No.17 of 2023 concerning National Health which defines it as the provision and facilitation of clinical services through telecommunications and digital communication technology. Furthermore, telemedicine is also recognized in more technical settings, namely Government Regulation No. 28/2024 concerning implementing regulations for the National Health Law which confirms that the practice of telemedicine is the provision of long-distance health services by health professionals using information and communication technology including the exchange of information on diagnosis, treatment and disease and injury prevention, research and evaluation, and continuing education and health care providers for the benefit of individual and public health. The scope of telemedicine services is regulated in Minister of Health Regulation No. 20 of 2019 concerning the Implementation of Telemedicine Services which includes: teleradiology, teleelectrocardiography, teleultrasonography, clinical teleconsultation, telepharmacy and other telemedicine consultation services in accordance with developments in Science and Technology.

According to the understanding outlined in several national regulations in the health sector above, the provision of telemedicine includes various variants of health services provided by health workers who have practice permits at health service providers such as doctors, paramedics and nurses which are carried out in a digital system. The health services provided by health workers in telemedicine include: health facilities providing consultations and receiving consultations. Health facilities that can provide telemedicine include hospitals, community health centers, clinics, independent practices of media or health workers, health laboratories and pharmacies.

The five health service facility providers above are able to conduct telemedicine independently or in collaboration with registered electronic system providers in accordance with the provisions of applicable laws and regulations, where electronic system providers for health services can be carried out by individuals, the State, business entities and communities that provide, manage and/or operate electronic systems either individually or jointly with electronic system users for their own needs and/or the needs of other parties. For example, the telemedicine platform operated by the Indonesian Government is "Telemedicine Indonesia (Temenin)" which was developed by the Ministry of Health. The scope of health service facilities includes radiocardiography, ultrasound, radiology and consultation.

Generally, the provider of telemedicine in Indonesia, are categorized into two kind as follow: health-care facility- provide consultation and health-care facilty-receive concultation. Both of them are engage to several mandatory obligations which is stipulated inside The Ministry of Health's Regulation No.20 of 2019 concerning telemedicine are elaborated further in the table below:

Table 1 Comparation Right and Obligation Amongs Heath-Care Facility

	Health Care Facility- Consultation's Provider	**Health Care Facility- Receive Provider**
Right	Accepting medical information including: picture, image, text, bio- signal,video and good voice to carry and answer online consultation.	Get an consulattion's answer jawaban konsultasi dan obtain the expertise based on proper standart Acquire clear, correct, accountable and credible information relating to the result of consultation and or

	Gain an honorarium on Teleemedicine's service	expertise
Obligation	Delivering a answer consultation and expertise based on standardization Maintain the confidentiality of patient's data Acquire clear,correct, resilience and credible information relating to the result of consultation and or. Expertise Allocate to do consultation for 24 hours/day, 7 days in one week	Delivering a answer consultation andexpertise based on standardization Maintain the confidentiality of patient'sdata Acquire clear, correct, accountable and credible information relating to the result of consultation and or expertise

However, not all digital platforms that provide health facility services can be categorized as Telemedicine according to the regulations in force in Indonesia. Currently, there are a number of platforms providing online consultation services with doctors such as KLikDokter, Good Doctor, Get Well, YesDok and AloDokter. Some examples of these platforms are only a means to facilitate the search for health services by consumers. A number of the platforms above can be categorized as E- Health which utilizes information and communication technology for health services with the aim of creating effective and
efficient work processes. Indonesian Cyber Law is a regulation which is being a legal basis in utilizing Information Technology. Its existence is effecting significantly on every activitiest in cyber space. According to article 15 paragraph (1) and (2) arrange that every online platform has responsibility to conduct resilience electronic system and secure dan on operational system inside the relevant platform.

3.1.2. Perspective of National Cyber law and Health Law to prevent Data Breach and Misuse of dan RecordMedical Electronic in Telemedicine

Accommodating and organizing Health Services to the Community is a mandate mandated by Article 28 H paragraph (1) of the 1945 Constitution of the Republic of Indonesia) which states that: "Everyone has the right to live in physical and spiritual prosperity, to have a place to live, and to have an environment live a good and healthy life and have the right to receive health services." The state guarantees the right of every citizen to have a good and prosperous life physically and mentally in order to realize its commitment to protect all the blood of the Indonesian nation. The development of thepublic health services sector is part of the development of quality and productive human resources, so policies are needed to support an adaptive and sustainable health sector by emphasizing the principles of equity, prosperity, equity and non- discrimination.

Law No. 17 of 2023 concerning Health (hereinafter referred to as the National Health Law) distinguishes between the practice of telemedicine and telehealth (telehealth) as two different entities even though they are both integrated in electronic systems and offer health services. According to the provisions of Article 1 number 21 of the National Health Law, telehealth is the provision and facilitation of health services, including public health, health information services and independent services, through telecommunications and digital communication technology.Meanwhile, according to Article1 number 2 of the National Health Law, Telemedicine is the provision and facilitation of clinical services through telecommunications and digital communication technology. The differences of among health service provider lies in the scope of providing services to patients. According to the World Health Organization, Telemedicine services are divided into four elements as follow (Organization, 2009):

a) *Its purpose is to provide clinical support*, aims to give an health service assistance or clinical support.
b) *It is intended to overcome geograpichal barriers, connecting users who are not in the same physical location*its mean that the existence of telemedicine has objectives to resolve geographical barriers, and connecting users are not stand in same location.
c) *It involves the use of various types of ICT*, by involving multi-type of information technology and communication such as computer, internet,and another devices.
d) *Its goal is to improve health outcomes*, yang artinya bertujuan akhir untuk meningkatkan hasil dari pelayanan kesehatan.

Telemedicine is a system that uses information technology to support long-distance health care for patients in contact with medical personnel or doctors (Andrianto & Athira, 2022). The scope of telehealth is wider than telemedicine. In addition to providing health services, telehealth platforms refer to knowledge, administrative management and clinical care that are broader than in remote health services. Meanwhile, Telemedicine is the provision of medical services remotely by doctors and dentists

using information and communication technology, including the exchange of information on diagnosis, treatment, disease and injury prevention, research and evaluation, and continuing education of health service providers for the benefit of improving individual and community health.

Telemedicine services function to provide a medium of communication between doctors and patients in a digital application, but basically Telemedicine does not change the ethics of medical personnel in their ethics and obligations to seriously maintain the confidentiality of patient information. This information includes all personal, medical and historical patient information that must be kept confidential without exception.Regulation on medical ethics to maintain the confidentiality of patient data are usually regulated in codes of ethics or medical professional guidelines. In many countries, medical organizations have codes of ethics that outline the principles that medical personnel must follow in maintaining the confidentiality of patient data. One of the codes of ethics that is commonly used is the "Hippocratic Oath", as well as codes of ethics issued by national or international medical associations. Some general principles in regulating medical ethics relating to maintaining the confidentiality of patient data are as follows:

a) Professional Confidentiality: Physicians have an ethical obligation to maintain the confidentiality of patient information they obtain in the course of medical practice. This information should not be disclosed to third parties without valid patient consent.

b) Informed Consent: Doctors must obtain written permission from patients before disclosing personal or confidential medical information to other parties, except in certain situations regulated by law.

c) Data Security: Doctors must ensure that patient data is stored securely and protected from unauthorized access. This may include the use of information security technology and strict internal policies.

d) Confidential Communication: Doctors must be careful when communicating about patients, whether verbally or in writing. Medical discussions involving patients should be conducted in an appropriate and private environment.

e) Emergencies: Although the principle of confidentiality is very important, in some life-threatening emergencies, doctors may provide necessary information to relevant parties for the purpose of saving the patient.

f) Data Deletion: Patient data that is no longer needed should be securely deleted or destroyed to prevent misuse.

g) Professional Code of Ethics: Doctors must follow codes of ethics and guidelines issued by local, national, or international medical institutions that regulate medical practice.

Legal Basis that binds and underlies the professional ethics of doctors or medical personnel is Law Number 29 of 2004 concerning Medical Practice. One of the important parts of Law Number 29 of 2004 is Article 45, which regulates the doctor's code of ethics. This article emphasizes that doctors are obliged to comply with the code of ethics established by the Indonesian Doctors Association. This code of ethics includes ethical principles and procedures for carrying out medical practice, including maintaining patient confidentiality.

Since the advent of telemedicine, the legal basis governing patient confidentiality apart from Law no. 29 of 2004 concerning Medical Practice is Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the Indonesia Data Protection Law) which is important in maintaining individual privacy in an increasingly complex digital environment. Article 2 of the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Platforms states that Protection of Personal Data in Electronic Systems includes protection of the acquisition, collection, processing, analysis, storage, display, announcement, sending, dissemination, and destruction of Personal Data.

3.1.3. Imposement of Liabilty on Misuse of Record Medical Electronic in Telemedicine

According to Handiwidjojo, electronic medical record data is the use of information technology devices for collecting, storing, processing and accessing data stored in patient medical records at hospitals in a database management system that collects various sources of medical data (Handiwidjojo., 2009). As explained previously, electronic medical records can also be interpreted as an application environment consisting of clinical data storage, clinical decision support systems, standardization of medical terms, computerized data entry, as well as medical and pharmaceutical documentation.

The misuse and leakage of data in cyberspace is something that happens quite often, especially during the COVID-19pandemic, where all offline habits have been shifted, making people's activities, especially in Indonesia, completely online. A survey from Karpersky stated that as many as 54 percent of respondents admitted that some doctors had conducted remote sessions using applications that were not specifically designed for telehealth, such as FaceTime, Facebook Messenger, WhatsApp, Zoom, so there was still a high risk of leaking patient data. Carrying out the telemedicine process should be the best solution for maintaining the security of patient data leaks. This case of personal data leakage, as mentioned in the introduction, also includes images and patient identity details, one of which includes drug prescriptions.

However, on the one hand, Article 13 of the Indonesian Medical Ethics Code (hereinafter referred to as KODAKI) regulates the obligation of doctors to maintain the confidentiality of everything they know about a patient, including the patient's personal data in the context of administering drug prescriptions. Apart from that, in Chapter II Article 9 of the Code of Ethics for Pharmacists, a pharmacist must maintain patient confidentiality properly. Ethics comes from the Greek word ethos which means morals, customs, habits, character, feelings, attitudes, what is good, what is worthy. Ethics is also a systematic consideration of right and wrong behavior. According to the Big Indonesian Dictionary, ethics, which was later adapted into ethics, is a collection or set of principles or values relating to morals. Basically, drug prescriptions given to patients via the telemedicine platform are included in the electronic medical record data. Data that can be categorized as patient personal data is as follows:

1. Patient Clinical Data refers to the patient's medical records. This data must cover several aspects, including complete patient identity information. In addition, the patient's clinical data must include the date and time of treatment. The patient's clinical data also records the results of the anamnesis (patient complaints and history) as well as the results of the physical examination carried out by the treating doctor. Finally, clinical data should include the diagnosis, treatment methods, and supporting information on the actions recommended by the physician.
2. Patient Administrative Data Patient administrative data is not related to medical records. This data focuses more on patient personal information, such as patient civil administrative records. This includes the following:

- Full name
- Medical record number/identification used
- The complete address of the patient's residence
- Details of the patient's birth (date, month, year and city)
- Patient gender
- Marital status (married or not)
- Contact the patient's closest family
- Date and time the patient received treatment
- Name and identification of the health worker. After these two types of patient data have been recorded completely, it can be said that the data has been recorded correctly. Even though it may seem simple, managing patient data requires accurate knowledge. Apart from its sensitivity, this data also has confidential characteristics.

Specifically regarding the application of electronic medical records, Article 21 of the 2012 Indonesian Medical Code of Ethics (KODEKI) requires every doctor to always follow developments in science and technology, especially regarding medicine and Health. In this case, the application of electronic medicine prescriptions includes the use of technology that can improve the performance of doctors and medical personnel as providers of health services to the community. In the medical field, there are 5 main principles in ethics, namely as follows (Triwibowo, 2014): The principle of nonmaleficence (no harm); The principle of beneficence (only doing something good); The principle of confidentiality (meaning patient information must be kept confidential); The principle of justice (equal treatment). and fairness towards others) and the principle of fidelity (the principle of respecting one's promises and commitments).

Patient data information listed on electronic drug prescriptions is also a top priority and is something that really requires an appropriate level of privacy and legal basis in telemedicine practice. Behind the various advantages of implementing electronic medical records specifically designed by telemedicine companies such as Alodokter and HaloDoc, of course it requires an implementation that is supported by qualified technological capabilities through to the quality of human resources who understand the technology. Legally, the data in electronic medical records is a legal record of the services provided to patients and the hospital has the right to store this data. This becomes illegal if the person behind the telemedicine company misuses the data for certain interests that are not related to the patient's health services. Including if internal telemedicine parties are unable to maintaining and securing of the patient's personal data. According to health's management sector perspective, medical record data is closely correlated with health service activities, so there is an expression that medical colleagues are third parties when doctors receive patients. The medical data is a record of examinations and actions related to the treatment of a patient by a doctor. In short, medical record data is a file that contains notes and documents regarding patient identity, examinations, treatment, procedures and other services that have been provided to the patient. Meanwhile, in Indonesian property law optics in Article 570 chapter II of the Civil Code regulates the authority and restrictions for property rights holders, of course these provisions also apply to ownership of the contents of medical records. Telemedicine platforms' failure to fulfill their obligations to safeguard information in patient medical record data not only violates the patient's privacy rights but also the patient's property rights. Even if a telemedicine platform accesses and uses the contents of medical records without the patient's consent, it

should be considered an infringement of the patient's property rights. However, until now the existing health sector legal regulations still do not clearly regulate the limitations and authority over patient ownership rights over the contents of medical records.

The implementation of telemedicine itself cannot be separated from the medical trilogy as something that is very essential in medical practice, namely informed consent, medical records, and medical confidentiality. In telemedicine, medical record data is arranged in electronic form to suit the medical practice location. The high risk of data leakage in telemedicine applications can be regulated using Indonesian Personal Data Protection Law. This regulation is a new reference for protecting personal data in Indonesia, including medical record data for telemedicine patients. So that legal protection for patient media record data when undergoing telemedicine health services can use this legal instrument as a general umbrella law. According to the provisions of Article 4 Paragraph 1 of the Personal Data Protection Law, it is emphasized that personal data regulated and protected in this law is personal data that is specific and general in nature. General personal data is personal data

That contains a person's identity such as full name, gender, nationality, religion, marital status and other personal data that can identify a person. Meanwhile, data is specific as stated in Article 4 Paragraph 2 letter a, including health data and information such as medical records.

Legal protection of personal data in the Personal Data Protection Law is explained in Articles 35 to 39. Article 35 regulates that personal data controllers or in this case electronic system operators are obliged to protect and ensure the security of personal data under their systems. Through implementing appropriate technical operations to protect personal data from personal data processing interference that is contrary to statutory regulations and determining the appropriate level of personal data security by taking into account the risks of protected personal data.

If connected to the provision of health facility services via telemedicine, the context of the data controller in question is the application provider or telemedicine service site. Telemedicine platforms are required to maintain the confidentiality of personal data when processing personal data including patient medical records. In relation to its implementation, this is enforced by requesting informed consent from the patient to the doctor as the provider of the consultation to be provided with the patient's medical record data in electronic format. This medical record data must be kept confidential by the telemedicine provider as the data controller.

Apart from that, article 37 of the Personal Data Protection Law requires data controllers, in this case the telemedicine platform, to supervise the parties involved in electronic system processing and the telemedicine platform is obliged to protect personal data from all forms of unauthorized processing.

Based on the legal protection contained in the Personal Data Protection Law, telemedicine platforms as patient data controllers are also required to have internal policies for data management that are in line with these regulations. The policy of health service facilities providing telemedicine services is in the form of legal protection for patient data, namely personal data and medical records. Reviewing the juridical basis regarding the protection of personal data in cyber space, some of them are the Indonesian Informatic and Electronic Transaction Law Article 32 paragraphs (1), (2), and (3) which stipulate:

(1) "Any person intentionally and without right or against the law in any way changes, adds, reduces, transmits, damages, deletes, moves, hides electronic information and/or electronic documents belonging to other people or public property."

(2) "Any person intentionally and without right or against the law in any way transfers or transmits electronic information and/or electronic documents to another person's electronic system without the right."

(3) "Regarding actions as intended in paragraph (1) which result in the disclosure of confidential electronic information and/or electronic documents to be accessible to the public with the data not being as intact as it should be.

Some of the juridical implications if a case of data leakage is found refer to the legal basis in Indonesian Informatic and Electronic Transaction Law , there are criminal sanctions against the telemedicine party responsible with several sanctions as stated in article 48 paragraphs (1), (2) and (3). In the civil aspect, acts of negligence that cause harm to patients can be categorized as Torts which is regulated in article 1365 of the Civil Code. An unlawful act is an action or behavior that iscontrary to applicable law or legal norms. In the context of civil law, unlawful acts refer to actions that cause loss or damage to another party and are the basis for demanding compensation or legal responsibility. There are aspects that can be categorized as Unlawful Acts if they fulfill the following elements, as follow (Agustina, 2003):

1. Deeds: Refers to actual actions or behavior carried out by a person or legal entity.
2. Unlawful: Refers to actions or behavior that are contrary to applicable law or legal norms. This could mean violating

contractual agreements, ignoring legal obligations, or carrying out actions that are deemed to violate the rights of another party.

3. Loss: An unlawful act must cause loss or damage to another party. This loss could be financial, reputational, or even physical Loss.

When an unlawful act occurs, the party who suffers the loss usually has the right to demand compensation from the party who committed the act. The aim is to return the injured party to the position they would have had if the unlawful act had not occurred. Examples of unlawful acts in civil law can include breach of contract, defamation, acts that interfere with property rights, and other acts that harm other parties. However, each legal jurisdiction may have different interpretations and definitions regarding unlawful acts, and this may be governed by the laws and legal precedents of that country.

According to the perspective of medical personnel, referring to the rules of the Organization and Management Guidelines for the Honorary Council for Medical Ethics (ORTALA MKEK), if data leaks are still found due to doctors not using the official telemedicine platform, resulting in leaks of patient data in the form of drug prescriptions, then this violates the KODEKI and the Code of Ethics. Pharmacists can lead to advice, verbal warnings, written warnings, behavioral coaching, re-education (re-schooling), and even dismissal from membership of the Indonesian Doctors Association, either temporarily or permanently. In fact, the protection of patient data is regulated in medical ethics and Health law which states that it is the doctor's obligation to maintain the confidentiality of everything he knows about a patient (Article 13 of the Indonesian Medical Ethics Code). With the existence of telemedicine, of course there is no reason not to implement a medical code of ethics to maintain the confidentiality of patients' personal data, including when prescribing medication to patients. In fact, agreements in general, agreements between medical personnel, in this case doctors and patients, still require guarantees regarding the protection of user data, especially in the provision of drug prescriptions as one of the medical procedures.

Tortorious actions in the terms of patient’s data breach in telemedicine bring some serious legal consequences are:

1). Non –Material damages

a). Infringement against patient’s medical record is extraordinary breach to privacy. The scope of personal datain telemedicine including: medical history, name, address, telephone number,and another personal data. The violation of privacy would lead into emotionally , financially and personal reputation.

b). Violation of Data Protection Laws. Many jurisdictions have data protection laws that regulate how personal data should be managed and protected. Data leaks may result in legal violations of these regulations, such as the General Data Protection Regulation (GDPR) in the European Union or personal data protection laws in various countries.

c). Legal Demands

Individuals affected by a data leak may file a lawsuit against the telemedicine service provider responsible for the leak. These claims may include compensation for financial losses, reputational losses, and other losses arising from a data breach. Data protection authorities in some jurisdictions may impose administrative sanctions on service providers who violate data protection laws. These sanctions can include significant financial fines.

d). Reputation’s Damage

Data leaks can damage the reputation of telemedicine service providers. Patients' trust in telemedicine systems can be shaken, and this can impact the relationship between providers and patients. Some personal data leaks may be considered criminal acts, depending on applicable laws. This may result in investigations and criminal prosecution of the parties responsible for the leak. In addition to the legal impact, data leaks can also cause significant business losses due to loss of customer trust and potential loss of customers and business contracts. It is therefore very important for telemedicine service providers to implement strict security measures, comply with applicable data protection regulations, and have an effective data security response plan in dealing with potential data leaks. Meanwhile, regarding regulations regarding Personal Data Protection in cyber space in Indonesia, apart from the Indonesia Informatic and Electronic Transaction Law, namely the latest Law of 2022 concerning Personal Data Protection Law. If there is a breach of medical record data as part of Personal Data which results in loss to the individual concerned, then the party committing the breach may be required to pay compensation to the individual who sufferedthe loss. Individuals who feel their privacy rights have been violated under the PDP Law have the right to sue the party who committed the violation, either civilly, administratively or criminally.

Criminal sanctions for telemedicine providers according to the provisions of Article 67 of the Personal Data Protection Law are qualified as a criminal offense by a corporation, criminal penalties can be imposed on the management, control holder, order giver, beneficial owner, and/or the responsible corporate party. Furthermore, Paragraph (2) of the Personal Data Protection Law explains that health service facilities as absolute corporations as a whole can only be subject to fines. As stated in Article 70

Paragraph (2), health service facilities can be subject to additional penalties in the form of confiscation of profits from criminal acts, freezing of all or part of the health service facility, permanent prohibition on continuing to operate the business, closure of all functions of the health service facility, implementation of obligations as a result of criminal acts, payment of compensation, revocation of permits, and dissolution of health service facilities.

In civil law point of view, as discussed in the previous section, medical record data is an intangible asset owned by the patient. Medical records contain notes and documents about patients which include personal, social and financial data as well as medical data in the form of examination results, treatment, procedures and other services that have been provided to patients. Through medical record data, patients are authorized to defend their personal information from interference by other parties so that parties who do not have authority according to regulations do not have the right to gain access and use it without the consent of the patient concerned. Apart from that, this property right also gives the patient the authority to access and utilize information documented in the medical record for their personal interests.

Referring to the concept of medical record data as part of the patient's property rights, any interference such as misuse of data, access without owner consensus and sharing of medical record data for purposes that are not in accordance with the purpose of processing, these actions can be considered as unlawful acts. if it reduces or eliminates the enjoyment of the use of someone's property rights intentionally. So there is a causal relationship between intentional actions and loss of enjoyment in the use of property rights. Losses resulting from interference can be sued based on Article 1365 of the Civil Code concerning unlawful acts (onrechtmatige daad).

1.2. Complexity of Implementation of Record Medical Electronic's Protections in Indonesia

Lawrence M. Friedman stated that the effectiveness and success of law enforcement depends on three elements of the legal system, namely the structure of the law, the substance of the law and the legal culture. Legal structure concerns law enforcement officers, legal substance includes statutory instruments and legal culture is the living law adopted in a society (Friedman, 2009).

Based on the current status quo conditions in Indonesia, of course implementation will encounter various obstacles. The existing obstacles will prevent the implementation of electronic medical records in Indonesia from being optimal. The lack of optimal protection of electronic medical record data in Indonesia has an impact on disrupting the performance of medical record officers, resulting in incomplete electronic medical record data. Electronic medical records, which were expected to be a source of complete data, ultimately could not be achieved due to limited competency of medical record officers, inadequate supporting facilities and infrastructure, and non-existent regulations regarding the administration of electronic medical records.

The use of electronic medical records was only based on Article 2 of the Minister of Health Regulation Number 269/Menkes/Per/III/2008 concerning Medical Records which explains that medical records can be maintained electronically. However, the regulations regarding electronic medical records in Indonesia are only limited to that and there have only been further detailed regulations regarding the administration of electronic medical records. The legal basis for the protection of electronic medical records is currently only based on Article 2 of the Minister of Health Regulation Number 269/Menkes/Per/III/2008 concerning Medical Records which explains that the administration of medical records can be done electronically. However, the regulations regarding electronic medical records in Indonesia are only limited to that and there have only been further detailed regulations regarding the administration of electronic medical records.

The Personal Data Protection Law as the main regulation that covers the protection of personal data is also experiencing difficulties in enforcement. This is because there are no technical regulations under it that regulate the implementation of these regulations, especially in the health services sector. Another weakness of the Personal Data Protection Law is related to the institutional enforcement of personal data protection in Indonesia. This is shown by the fact that although a number of laws have appoint independent agencies that specifically have the authority to carry out supervision – both directly and indirectly – on the protection of personal data, inter alia, Natioanl Human Rights Comission, Information Commission, BRTI, Indonesia Financial Agency, Honorary Council of Advocates, National Trade Committee and Energy Council Indonesian Health. However, all of these independent institutions are subordinate to the government, meaning that these institutions are completely under the government's authority. In fact, Indonesia already has technical regulations contained in Minister of Health Regulation No. 24 of 2022 concerning Electronic Medical Records. However, this regulation does not yet contain technical instructions, such as provisions regarding limits on opening patient electronic medical record data as well as reporting mechanisms that can be carried out by the public in the event of a violation of medical record data leakage by certain parties, especially those who manage the medical record data. These two points should be very vital because they are seen as a form of recognition of human rights both from the perspective of patients and the wider community

The urgency of protecting personal medical records in Indonesia at this time is in fact not directly proportional to the public's understanding of the importance of protecting this data. This is actually recognized by academics, as well as real evidence that there is still a low rate of filing cases in court related to interference with the privacy of someone's data , despite the existence of existing laws that relate to the protection of personal data and the health sector. Lack of awareness of the importance of protecting personal data is a challenge that needs to be overcome, especially because health data includes specific/sensitive data.

IV. CONCLUSION

Record Medical Electronic is part of patient's privacy that must be protected when implementing telemedicine health service practices. However, regulations regarding electronic medical records in Indonesia have not been regulated in a comprehensive and holistic manner so that gaps in legal substance mean that the protection provided is not fully beneficial. Even though Indonesia has regulations in the Minister of Health Regulation regarding Electronic Medical Records, these regulations still have shortcomings, including migration of medical record data, procedures for disclosing medical information, and reporting data leak violations. The Government of the Republic of Indonesia must immediately formulate specific regulations for the protection of medical record data in the health sector and regulations derived from the Personal Data Protection Law which regulate the implementation of law enforcement. Apart from that, there needs to be a clear delegation of authority regarding the authority that supervises and takes action against violations of misuse of electronic medical record data in Indonesia. The need for harmonization in implementation between the Minister of Health Regulation on RME and the Personal Data Protection Law can be seen when the Personal Data Protection Law allows specific data processing actions such as electronic medical record data, as long as the party who will carry out the processing first carries out a Personal Data Protection Impact Assessment and iscarried out to public interest in the context of state administration.

REFERENCES

1) Agustina, R. (2003). *Perbuatan Melawan Hukum, .* Depok: Universitas Indonesia, Fakultas Hukum, Pascasarjana.
2) Andrianto, W., & Athira, A. B. (2022). Telemedicine (Online Medical Services) Dalam Era New Normal Ditinjau Berdasarkan Hukum Kesehatan. *Jurnal Hukum dan Pembangunan Vol.52. No.1 (2022):*, 220-250.
3) Benuf, K., & Azhar, M. (2020). Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer. *Jurnal Hukum Gema Keadilan Volume 7 Edisi I, Juni 2020*, 24.
4) Friedman, L. M. (2009). *System Hukum Dalam Perspektif Ilmu Sosial, The Legal System: A Sosial Science Perspektiv.* Bandung.
5) Gondhowiardjo, S. A. (2020). *Kebijakan PORI Teleradioterapi Di Masa Pandemik Covid 19. .* Perhimpunan Dokter Spesialis Onkologi Radiasi Indonesia (PORI), .
6) Handiwidjojo., W. (2009). Rekam Medis Elektronik. *20 Jurnal Eksis Vol.2 No.1 (2009)*, 1.
7) *https://nasional.kompas.com/read/2022/01/06/22555491/kemkominfo-telusuri-dugaan-kebocoran-data-pasien-milik-kemenkes.* . (n.d.). Retrieved October 2022 , from https://nasional.kompas.com/read/2022/01/06/22555491/kemkominfo-telusuri- dugaan-kebocoran-data-pasien-milik-kemenkes. .
8) Imam Santoso, ". A. (n.d.). *Antara news* .
9) Indonesia, P. B. (2018). *Telemedisin: Rekomendasi Ikatan Dokter Indonesia Untuk Masa Depan Digitalisasi Kesehatan di Indonesia.* Jakarta : Ikatan Dokter Indonesia .
10) Jamil, M. K. (2015). Implementasi Aplikasi Telemedicine Berbasis Jejaring Sosial dengan Pemanfaatan Teknologi Cloud Computing. *Jurnal Edukasi dan Penelitian Informatika (JEPIN),*.
11) Kuntardjo, C. (2020). Dimension of Ethics and Telemedicine in Indonesia: Enough of Permenkes No.20/2019 as a Frame Telemedicine in Indonesia . *Soepra Jurnal Hukum Kesehatan*.
12) Kurniawan, A. L. (2021). Perlindungan Data Rekam Medis sebagai bentuk perlindungan data pribadi pasien selama PandemiCovid 19. *Jurnal Hukum dan Pembangunan Ekonomi*.
13) Kvedar, J. C. (2014). Connected health: a review of technologies and strategies to improve patient care with telemedicine andtelehealth. . *Health Affairs*, 194-199.
14) Lestari, R. D. (2021). Perlindungan Hukum bagi Pasien dalam Telemedicine. *Jurnal Cakrawala Informasi Vol 1 No.2 (2021),*, 51-65.
15) Masa, M. A. (2014). Strategi Pengembangan Implementasi Telemedicine di Sulawesi Selatan" . *Jurnal Telekomunikasi dan Komputer, Vol. 5 No. 3, (September 2014),*

16) Mursalat, M. H. (2022). Problematika yuridis dan Prinsip perlindungan hukum dalam Pelayanan Kesehatan Jarak Jauh menggunakam Teknologi Informasi dan Komunikasi. *Jurnal Poros Hukum Padjajaran*.
17) Organization, W. H. (2009). *Telemedicine: Opportunities and Developments in Member States,.* Geneva: WHO Press .
18) Public Health Institute. (2018). *State Telehealth Laws & Reimbursement Policies: A Comprehensive of the 50 States & The District of Columbia.* Center for Connected Health Policy 2018) .
19) Pukovisa Prawiroharjo, Pratama, P., & Librianty, N. (2019). Layanan Telemedis di Indonesia: Keniscayaan, Risiko, dan Batasan Etika. *Jurnal Etika Kedokteran Indonesia, Vol. 3 No. 1 (Februari 2019)*.
20) Rizkiyani Istifada, Sukihananto, & Laagu, M. A. (2017). Pemanfaatan Teknologi Telehealth Pada Perawat di Layanan Homecare. *Jurnal Nursing Current Vol. 5 No. 1, (Januari – Juni 2017)*.
21) Sugiyono. (2009). *Metode Penelitian Kuantitatif Kualitatif dan R&D.* Bandung: Alfabeta.Triwibowo, C. (2014). *Etika & Hukum Kesehatan.* Yogyakarta .
22) Watulingas, A. M. (2022). Implementasi Perlindungan Hukum Profesi Dokter Terhadap Layanan Telemedicine di RSUP Prof.
23) Dr. R. D. Kandou Manado. *Medical Scope Journal*.
24) Wootton, R., & Craig, J. (1999). *troduction to Telemedicine.* Kansas: The Royal Society of Medicine Press Limited, 1999.