# JURIDICAL ANALYSIS OF THE MISUSE OF ELECTRONIC MEDICAL RECORDS IN THE PERSPECTIVE OF THE ELECTRONIC INFORMATION AND TRANSACTION LAW

**Tryda Meutia Anwar[1], Jerry G. Tambun[2], Ahmad Jaeni[3]**

[1]Sekolah Tinggi Hukum Militer, Jakarta, tryda031294@gmail.com
[2]Sekolah Tinggi Hukum Militer, Jakarta, nasserkelly@yahoo.com
[3]Sekolah Tinggi Hukum Militer, Jakarta, ahmad.jaeni@sthm.ac.id

***Abstract***

*The background of this research is regarding the potential for misuse of electronic medical records based on Electronic Information and Transactions (ITE) and patient data protection. Law Number 1 of 2024 concerning Information and Electronic Transactions which replaces Law Number 19 of 2016. And Law No. 27 of 2022 concerning Personal Data Protection. This research method uses qualitative and normative data analysis techniques. The results of this study show that Law Number 1 of 2024 concerning ITE is one of the important pillars that discusses the use of electronic information/documents as legal evidence at trial in the event of the dissemination of electronic medical records that can be used as illegal materials and to protect patients ' personal dataThere is Law No. 27 of 2022 concerning Personal Data Protection in Indonesia which has the main purpose of protecting individual personal data and regulating the collection, use, storage, security, and deletion of personal data by health services that manage patient data. By mandating strict data protection practices, the law upholds the ethical principle of patient confidentiality, which is essential for maintaining patient trust. Therefore, healthcare providers should invest in advanced cybersecurity measures.*

***Keywords: Electronic Medical Records, Personal Data, Security.***

## I. INTRODUCTION

Improving the quality of services from Health Service Facilities has become a public demand in meeting the community's needs for health services. Some of the efforts to improve the quality of health facilities include improving the quality of services themselves, improving the skills of medical personnel and medical personnel and supporting facilities needed for the development of the Health Service Facilities themselves. The development of facilities and infrastructure is one of the important elements in improving the Health Information System. With the increasing development of primary and secondary Health Service Facilities built by the private sector and the government, it is required that a Health Service Facility be able to compete with domestic Health Service Facilities as well as compete with international Health Service Facilities. To be able to win the increasingly fierce competition, both private and government health service facilities are encouraged to improve the quality of services, marketing strategies, and the availability of adequate facilities and infrastructure.[1]

[1] Darmanto Djojodibroto, 1997, *Tips for Managing Hospitals*, Hippocratic, Jakarta, p.5

Technological advancements in the healthcare sector have revolutionized the way healthcare is delivered, improving patient outcomes, increasing efficiency, and reducing costs. One of the most significant developments is the emergence of telemedicine.[2] Medical Records are one of the most important components in a Health Service Facility. The rapid advancement of medical science, health law and technological advances followed by the advancement of the mindset of the community / patients who become smarter and more critical about their rights as consumers of health services, encourages the implementation of medical records to be managed properly according to the progress of the times.[3]

Medical records are essential in healthcare because they ensure continuity of service by providing a comprehensive history of the patient's medical background, facilitating accurate diagnosis and treatment, and supporting medication management. These documents serve as legal documents, which are essential for compliance and protection against malpractice claims. Additionally, they are invaluable for clinical research, medical education, and public health monitoring, helping to improve patient outcomes and the quality of healthcare services. Medical records also enable efficient resource allocation and interdisciplinary communication, encouraging patient engagement and informed decision-making.[4]

Medical records play a crucial role in the healthcare system, serving many functions that improve patient care, simplify administrative processes, and support medical research. One of the main functions of medical records is to provide comprehensive and accurate records of patients' medical history. It includes details of past diseases, medications, allergies, immunizations, and diagnostic test results. Such detailed records are essential for healthcare providers to make informed clinical decisions, avoid redundant tests and procedures, and ensure continuity of service across various medical facilities and specialties.[5] In addition, medical records facilitate effective communication between healthcare providers. In cases where patients are referred to specialist doctors or transferred between hospitals, access to complete medical records will ensure that all healthcare professionals involved are aware of the patient's medical history and current treatment plan. This communication reduces the risk of errors and improves care coordination. In addition, medical records play an important role in monitoring and managing chronic diseases. By tracking the progression of conditions such as diabetes, hypertension, or heart disease, healthcare providers can tailor treatment as needed and intervene early if a patient's condition worsens.[6]

---

[2] Blumenthal, D., & Tavenner, M, 2010, The "Meaningful Use" Regulation for Electronic Health Records. New England Journal of Medicine, 363(6), hlm. 501-504.

[3] Suryo Nugroho Markus, 2010, *Master Plan for the Development of Hospital Management Information System*, Permata Indonesia Health Polytechnic, Yogyakarta, p. 32.

[4] The Role of Medical Records in Healthcare. National Institutes of Health (NIH)

[5] Health Level Seven International (HL7). 2020. *Introduction to HL7 Standards*. Retrieved from https://www.hl7.org/implement/standards/

[6] *Ibid,* p. 8.

Medical records also play an important role in the administrative aspects of healthcare. They provide the necessary documentation for insurance billing and claims, ensuring that healthcare providers get reimbursement for the services they provide. Accurate recording reduces the risk of billing errors and false claims, thereby contributing to the financial stability of healthcare institutions. In addition, medical records support legal and regulatory compliance. The document serves as official documentation in the event of a medical dispute or malpractice claim, showing the services provided and the decision-making process by healthcare professionals.[7]

In Indonesia, electronic medical records are regulated in the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 which replaces the Regulation of the Minister of Health of the Republic of Indonesia Number 269/MENKES/PER/III/2008 concerning Medical Records. The revocation of the old ministerial regulation is no longer in accordance with the development of science and technology, the needs of health services, and the legal needs of the community. The advancement of digital technology in society has encouraged digital transformation in health services, the management of electronic medical records must prioritize the principles of security and confidentiality of data and information. Medical records play a crucial role in the healthcare system, serving many functions that improve patient care, simplify administrative processes, and support medical research.

One of the main functions of medical records is to provide comprehensive and accurate records of patients' medical history. It includes details of past diseases, medications, allergies, immunizations, and diagnostic test results. These detailed notes are very important for health care providers to make the right clinical decisions, avoid excessive tests and procedures, and ensure continuity of services in various medical facilities and specialties, this is in accordance with article 1 paragraph 1 of the Minister of Health Regulation Number 24 of 2022 which reads "Medical Records are documents that contain patient identity data, examinations, treatments, actions, and other services that have been provided to patients".[8]

One of the aspects that has always been a concern in digital transformation is data security. Digital data that is easily accessible through the internet is considered vulnerable to leaks, especially since cybercrime has been increasing recently. It is a challenge for health service institutions to create an adequate security system when implementing an electronic medical record system. The Ministry of Health emphasized that the digital conversion of patient cards must be carried out in

[7] Muchsin, Fadillah Putra, *Law and Public Policy*, (Bandung: Averrous Press, 2002), p.31.

[8] Agustin, Wafiq, 2022, *Electronic Medical Records as Evidence Reviewed from the Perspective of Indonesia Health Law (Literature Study),* Diploma thesis, STIKES Foundation Dr. Soetomo Hospital Surabaya, p. 2.

accordance with the principles of data and information security and confidentiality. Several personal data breaches in Indonesia have alerted most people to security concerns. The health industry cannot be separated from this cybercrime. According to the www.aptika.kominfo.go.id website, hackers hacked 720 GB of digital data, including 6 million patient records stored by the Ministry of Health. This information was then sold publicly on the Raid forum.[9]

The Ministry of Health data leak is not the only health data leak that has ever occurred in Indonesia. Millions of health data from various health facilities and the health industry, both private and government, have been successfully hacked before. The same thing can happen if the implementation of electronic medical records is not supported by robust data security. As the use of electronic medical records (RME) increases, concerns about the security of electronic medical records (RME) related to the privacy and confidentiality of clinical data are increasing, so an information security strategy is needed to prevent the leakage of patient and hospital information.

## II. RESEARCH METHOD

The research method used in this writing uses qualitative and normative data analysis techniques, which are carried out through the approach of applicable laws and regulations to a certain legal problem. And this type of writing is descriptive by presenting, analyzing, and interpreting a problem with the legal rules that apply in it.

## III. DISCUSSION

### a. Legal Framework Governing the Use of Electronic Information/Documents as Evidence in Criminal Prosecution

In the legal context, especially in Indonesia based on Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), electronic information and documents are defined in Article 1 paragraph 1 of the ITE Law. This article describes electronic information as one or a set of electronic data, including but not limited to writing, sounds, images, maps, plans, photographs, emails, or other forms transmitted as part of an electronic transaction. Article 1 paragraph 4 of the ITE Law describes an electronic document as any Electronic Information that is created, transmitted, transmitted, received, or stored in analog, digital, electromagnetic, optical, or similar form, which can be seen, displayed, and/or heard through a Computer or Electronic System, including but not limited to writing, sounds, images, maps, designs, photographs or the like, letters, signs, numbers, Access Code, symbol or perforation that has meaning or meaning or can be understood by a person capable of understanding it. The Electronic Information and Transaction Law (UU ITE) promulgated in Indonesia is a response to the rapid development of information and communication technology. This law

[9] *Ibid,* p. 21.

aims to provide a legal framework for electronic transactions and information, as well as ensure security and justice in the cyber world. Article 5 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) is one of the important pillars in this Law [10]. The article states:

1) Electronic Information and/or Electronic Documents and/or printed results are valid legal evidence.
2) Electronic Information and/or Electronic Documents and/or their printouts as referred to in paragraph (1) are an extension of valid evidence in accordance with the Procedural Law applicable in Indonesia.
3) Electronic Information and/or Electronic Documents are declared valid if using the Electronic System in accordance with the provisions stipulated in this Law.
4) The provisions regarding Electronic Information and/or Electronic Documents as intended in paragraph (1) do not apply to:
    a. A letter that according to the Law must be made in written form; and
    b. letter and its documents which according to the Law must be made in the form of a notary deed or a deed made by the deed-making official.

However, there is an amendment to Law Number 19 of 2016 to Law Number 1 of 2024 concerning Information and Electronic Transactions (UU ITE), there is article 27B paragraph 1 which contains a person who disseminates electronic information/documents that have content that violates decency can be criminally charged. The reading of Article 27B paragraph 1 is *that Every Person intentionally and without the right to broadcast, perform, distribute, transmit, and/or make accessible Electronic Information and/or Electronic Documents that have content that violates morality for public knowledge* [11]*. From the reading of article 27B paragraph 1 of Law Number 1 of 2024, there are several explanations as follows:*

1) *Broadcasting* includes the act of transmitting, distributing, and making accessible electronic information and/or electronic documents in electronic systems.
2) *Distributing* is sending and/or disseminating electronic information and/or electronic documents to many people or various parties through an electronic system.
3) *Transmitting* is sending electronic information and/or electronic documents addressed to other parties through an electronic system.
4) *Making accessible* is all other acts other than distributing and transmitting through electronic systems that cause electronic information and/or electronic documents to be known to other parties or the public.

[10] Cst Kansil, Christine *et all, Dictionary of Legal Terms*, Jakarta, 2009, p. 385

[11] Riduan Syahrani, *Summary of the Essence of Law*, Citra Aditya Bakti Publisher, Bandung, 1999, p.23.

5) *Violating morality* is committing acts of showing nudity, genitals, and sexual activities that are contrary to the values that live in society in the place and time when the act is committed. The interpretation of the meaning of morality is adjusted to the standards that apply to society at a certain time and place (*contemporary community standard*).
6) *It is generally known* that it is to be able or so that it can be accessed by a group of people who mostly do not know each other.

Electronic devices in any form as explained in Article 27B paragraph 1 can be used as valid evidence if there is a person who is able to understand it or a certain person who is an expert in the field. Similarly, electronic medical records, either in the form of recordings or or other electronic data used by doctors to carry out treatment, can be used as evidence because they have a meaning or meaning that can be understood.[12] Basically, electronic information and electronic documents are closely related, although the two are not the same. Electronic information refers to data or data sets that can exist in various forms. On the other hand, electronic documents function as a container for such electronic information. To illustrate, consider a file in digital form filled into a flash drive format, which can contain music, movies, songs, videos, and other data that we can hear or see over and over again is electronic information. Meanwhile, the file in the flash disk that accommodates and distributes data is an electronic document. These differences help in understanding how digital content is stored and accessed. This electronic information is what is needed in doing proof, but it is electronic tools that we use as auxiliary tools in proving because this information exists in electronic form, so electronic tools that are said to be containers are tools that store the information data used.[13]

The Law on Information and Electronic Transactions is one of the important pillars that discusses the use of electronic information/documents as valid evidence in court. The article states: "Electronic information and/or electronic documents and/or printed results are valid evidence in the judicial process." With this provision, information or documents in electronic form are accepted and recognized as one of the evidence in the judicial process in Indonesia. This is a significant step forward because previously, the judiciary in Indonesia relied heavily on physical documents as evidence. Furthermore, an analysis will be given related to the legal regulation of the use of electronic information/documents as evidence in criminal law enforcement, analyzed with positive legal theory from John Austin. The theory of positive law was developed by John Austin, a jurist and philosopher from the United Kingdom. This theory emphasizes that law is an order issued by a sovereign ruler that must be obeyed by the subject of law in a country, with certain sanctions if the order is violated. When we analyze the legal regulation of the use of electronic

[12] Achmad Ali, *Uncovering the Veil of Law (A Philosophical and Sociological Study),* Toko Gunung Agung Publishers, Jakarta, 2002, p. 95.
[13] Zainal Asikin*, Introduction to Law*, (Depok: Rajawali Pers, 2011), p. 10.

information/documents as evidence in criminal law enforcement through the lens of John Austin's positive law theory, several key points can be identified:[14]

1) Sovereign Order. In the context of the ITE Law and the Criminal Code in Indonesia, regulations regarding the use of information or electronic documents as evidence can be seen as an "order" from the sovereign ruler, namely the government and the legislature that passed the law.
2) Legal Sanctions. Austin emphasized the importance of sanctions as part of the law. In the case of the use of electronic evidence, sanctions may be applied if the evidence is obtained illegally, manipulated, or presented in a misleading manner in court. The sanctions aim to ensure integrity and fairness in the judicial process.
3) Compliance and Acceptability. According to Austin, the success of the law depends on the level of compliance and acceptability by the community. Therefore, it is important for the legal community and the public in general to understand and accept electronic evidence as a valid means of evidence. This requires education and understanding of technology and how electronic evidence can play a role in law enforcement.
4) Clarity and Assertiveness. In Austin's view, the law must be clear and unequivocal. Regarding electronic evidence, it demands clear regulations and guidelines on how electronic evidence is collected, stored, analyzed, and presented in court.

Using Austin's positive law theory as the framework of analysis, it is clear that the legal regulation regarding electronic evidence in Indonesia follows the basic principles proposed by Austin. However, in their implementation, challenges such as rapidly changing technology, privacy issues, and the need for digital forensic experts require continuous adaptation and updates in the law to ensure fairness and effectiveness in the judicial process.

**b. Accountability for Misuse of Electronic Medical Records in the Perspective of Information and Electronic Transactions**

The development of electronic medical records (EMR) has revolutionized healthcare, improving the efficiency and accuracy of patient data management. However, with the shift from paper-based recording to digital recording, new challenges and risks have emerged, especially related to the misuse of recording. From the perspective of information and electronic transactions, responsibility for the misuse of ESDM involves various legal, ethical, and technical considerations. Misuse of electronic medical records can have a huge impact on patients. Unauthorized access or disclosure of medical information can lead to identity theft, discrimination, and psychological distress. Patients may suffer financial losses if their health information is exploited for fraudulent activities. In addition, violations of medical records can result in

[14] Mochtar Kusumaatmadja, *Introduction to Law*, (Bandung: Alumni, 2009), p.4

stigmatization, especially if sensitive information regarding mental health or infectious diseases is revealed. This potential danger highlights the importance of strict security and the need for accountability in the management of electronic health information. Legally, the misuse of electronic medical records is under strict regulations designed to protect patient privacy and data security in the United States for example, the Health Insurance Portability and Accountability Act (HIPAA) establishes health information protection standards.[15]

HIPAA mandates that healthcare providers implement adequate safeguards to prevent unauthorized access to electronic health information. Failure to comply with these regulations can result in severe penalties, including hefty fines and potential criminal charges. Healthcare organizations and their employees are liable for breaches, whether due to negligence, such as inadequate security measures, or intentional errors, such as unauthorized access or sharing of patient information. Based on Law No. 27 of 2022 concerning Personal Data Protection in Indonesia, the main purpose is to protect individual personal data and regulate the collection, use, storage, security, and deletion of personal data by health services that manage patient data. The implementation of the law in cases of leakage of patient personal data involves several important aspects, including:[16]

1) Obligations of the Person in Charge of Data.
   The law will establish obligations for data responsible persons, such as companies or healthcare services that collect and manage personal data. They must maintain the confidentiality and security of the personal data they have. The implementation of the Law may require the person in charge of data to adopt adequate technical and organizational measures to protect personal data from unauthorized access or unauthorized use.
2) Notification Obligations.
   In the event of a data leak, the law may require the person in charge of the data to provide notice to the affected individual in the event of a data security breach that could result in loss or risk to them. Such notifications should be made as soon as a data breach is detected, so that individuals can take the necessary steps to protect themselves, such as changing passwords or monitoring their financial activities.
3) Data Transfer Settings.
   The implementation of the law can regulate the transfer of personal data to other countries. The law may require the person in charge of the data to ensure that the destination country has an adequate level of data protection before transferring personal data to it. The law may establish specific requirements, such as written consent from individuals or the use of security mechanisms, to ensure that personal data remains protected when transferred.

[15] Satjipto Raharjo, *Law Studies,* (Bandung: PT. Citra Aditya Bakti, 2000), p. 53.

[16] Philipus M. Hadjon, *Legal Protection for the People in Indonesia*, (Surabaya: PT. Bina Ilmu, 1987), p. 25.

4) Sanctions and Responsibilities.
   The implementation of the law will establish sanctions and responsibilities for personal data violators. These sanctions can be in the form of significant fines or lawsuits against data responsible persons who violate data protection provisions. The law could also establish compensation liability for individuals who suffer losses as a result of personal data breaches, including recovery of financial losses or restoration of reputation.

The implementation of the law will establish sanctions and responsibilities for personal data violators. These sanctions can be in the form of significant fines or lawsuits against data responsible persons who violate data protection provisions. The law could also establish compensation liability for individuals who suffer losses as a result of personal data breaches, including recovery of financial losses or restoration of reputation. Law Number 27 of 2022 is a significant step in protecting patient data in health services, overcoming the rapid digitization of health services and the risks that come with it.

The law provides a comprehensive framework for preventing and sanctioning misuse of patient data, ensuring that healthcare providers maintain the highest standards of data security and patient confidentiality. Law Number 27 of 2022 outlines strict requirements for the collection, storage, and handling of patient data. The regulation mandates that healthcare providers implement robust data protection measures to prevent unauthorized access, modification, or disclosure of patient information. The law stipulates that patient data must be used solely for medical purposes and within the limits of the patient's consent. Any deviation from this provision is considered misuse of patient data, so violators will be subject to severe legal sanctions. The law also introduces a transparency obligation, which requires healthcare providers to inform patients about how their data is being used and the steps taken to protect it.[17]

In Law Number 27 of 2022, accountability is the main thing. Healthcare providers are responsible for ensuring that their data management practices comply with legal requirements. This includes not only implementing technical safeguards but also fostering a culture of privacy and security within their organization. The law establishes severe penalties for non-compliance, ranging from fines to imprisonment, depending on the severity of the abuse. This punishment serves as a deterrent effect for potential offenders and underscores the importance of maintaining patient data. In addition to legal compliance, Law Number 27 of 2022 emphasizes the ethical implications of misuse of patient data.

[17] Setiono, *The Rule of Law*, (Surakarta: UNS, 2004), p. 3.

The law recognizes that violations of patient confidentiality can cause significant harm, including psychological distress, stigmatization, and discrimination. By mandating strict data protection practices, the law seeks to uphold the ethical principle of patient confidentiality, which is the basis of patients' trust in their healthcare providers. Ethical violations, such as unauthorized access to data for personal gain or out of curiosity, are treated as severely as violations of the law, thus reinforcing the importance of ethical behavior in healthcare. The enactment of Law Number 27 of 2022 has a significant impact on health service providers. They are now required to invest in advanced cybersecurity measures and keep updating their data protection protocols to comply with the law. This includes regular staff training on data privacy and security, conducting thorough audits, and ensuring that all electronic health record systems are secure. While these requirements may initially pose challenges and incur additional costs, they ultimately contribute to the integrity and trust of the healthcare system as a whole.

## IV. CONCLUSION

In the context of Indonesia law, Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE provides a clear definition of electronic information and documents, the ITE Law aims to establish a legal framework for electronic transactions and ensure cyber security and justice, and with the enactment of Law Number 1 of 2024, Article 27B paragraph 1 criminalizes the dissemination of electronic content that violates morals deliberately, emphasizing the role of the law in maintaining public order and ethical standards in the digital realm.

Law Number 27 of 2022 prioritizes accountability and holds health service providers accountable to align their data management practices with legal requirements. This includes not only implementing strong technical safeguards but also fostering a culture of privacy and security within their organization. The law imposes severe penalties for non-compliance, including fines and imprisonment, which serve as a deterrent and emphasize the importance of protecting patient data. In addition to legal compliance, the law also underlines the ethical consequences of data misuse, and recognizes the significant harm that breaches can cause, such as psychological distress and discrimination. By mandating strict data protection practices, the law upholds the ethical principle of patient confidentiality, which is essential for maintaining patient trust. Therefore, healthcare providers should invest in advanced cybersecurity measures, conduct regular staff training, and continuously update their data protection protocols, to ensure the integrity and trust of the healthcare system as a whole.

## REFERENCES


Achmad Ali, *Uncovering the Veil of Law (A Philosophical and Sociological Study),* Toko Gunung Agung Publishers, Jakarta, 2002.

Agustin, Wafiq, 2022, *Electronic Medical Records as Evidence Reviewed from the Perspective of Indonesia Health Law (Literature Study),* Diploma thesis, STIKES Foundation Dr. Soetomo Hospital Surabaya.

Blumenthal, D., & Tavenner, M, 2010, The "Meaningful Use" Regulation for Electronic Health Records. New England Journal of Medicine, 363(6).

Cst Kansil, Christine *et all, Dictionary of Legal Terms*, Jakarta, 2009.

Darmanto Djojodibroto, 1997, *Tips for Managing Hospitals*, Hippocratic, Jakarta.

Health Level Seven International (HL7). 2020. *Introduction to HL7 Standards*. Retrieved from https://www.hl7.org/implement/standards/

Mochtar Kusumaatmadja, *Introduction to Law*, (Bandung: Alumni, 2009).

Muchsin, Fadillah Putra, *Law and Public Policy*, (Bandung: Averrous Press, 2002).

Philipus M. Hadjon, *Legal Protection for the People in Indonesia*, (Surabaya: PT. Bina Ilmu, 1987).

Riduan Syahrani, *Summary of the Essence of Law*, Citra Aditya Bakti Publisher, Bandung, 1999.

Satjipto Raharjo*, Law Studies,* (Bandung: PT. Citra Aditya Bakti, 2000).

Setiono*, The Rule of Law*, (Surakarta: UNS, 2004).

Suryo Nugroho Markus, 2010*, Master Plan for the Development of Hospital Management Information System*, Permata Indonesia Health Polytechnic, Yogyakarta.

The Role of Medical Records in Healthcare. National Institutes of Health (NIH).

Zainal Asikin*, Introduction to Law*, (Depok: Rajawali Pers, 2011).