The Legal Power in Evidence of Electronic Medical Records As A Substitute for A Doctor's Signature

Kekuatan Hukum pada Pembuktian Rekam Medis Elektronik Atas Pengganti Tanda Tangan Dokter

[1]Christine Widjaja; [2]Adriano

Coresponden e-mail: christinewidjaja5@gmail.com

[1,2]Faculty of law, University of Hang Tuah, Surabaya

Abstract: The existence of related regulations regarding validity of Electronic Medical Record (EMR) in proving a case explained that it requires a signature in proving an EMR. The use of a personal identification number (PIN) only performs a verification function, not someone's authentication.UU No. 29 of 2004 regarding Medical Practice states that it is sufficient to replace the obligation to sign an EMR with a Personal Identification Number (PIN), while in Permenkes Medical Records 2022, it is expanded by granting access rights to certain people where the security system depends on the decision of the leadership of each health care facility and can be equipped with an Electronic Signature. The use of a PIN alone is considered insufficient form EMR authentication functions, so other options need to be raised such as Electronic Signature which carry out both verification and authentication functions. The aims of research were to find out how the legality and strength of evidence of PIN and Electronic Signature as substitution of doctor's signature on electronic medical records. This study used a normative juridical method, with two approaches, namely statutory and conceptual approaches. The results showed that PIN and Electronic Signature could legally replace a doctor's signature on EMR, but hada different strength as evidence. The strength of EMR as evidence depends on the judge's point of view which is influenced by validity of EMR evidence, namely the presence/absence of a PIN and electronic signature as a function of verification and authentication.

Keywords : Biometric, Evidence, Electronic, Medical Record and Verification

Abstrak: *Adanya peraturan terkait mengenai keabsahan Rekam Medis Elektronik (EMR) dalam pembuktian suatu perkara menjelaskan bahwa dalam pembuktian suatu perkara diperlukan tanda tangan. Penggunaan Personal Identification Number (PIN) hanya menjalankan fungsi verifikasi, bukan otentikasi seseorang. UU Nomor 29 Tahun 2004 tentang Praktik Kedokteran menyatakan cukup menggantikan kewajiban menandatangani ESDM dengan Personal Identification Number (PIN) Sedangkan pada Permenkes Rekam Medis 2022 diperluas dengan memberikan hak akses kepada orang tertentu dimana sistem keamanannya bergantung pada keputusan pimpinan masing-masing fasilitas pelayanan kesehatan dan dapat dilengkapi dengan Tanda Tangan Elektronik. Penggunaan PIN saja dirasa belum mencukupi fungsi autentikasi EMR, sehingga perlu dimunculkan opsi lain seperti Tanda Tangan Elektronik yang menjalankan fungsi verifikasi dan autentikasi. Tujuan penelitian adalah untuk mengetahui bagaimana legalitas dan kekuatan pembuktian PIN dan Tanda Tangan Elektronik sebagai pengganti tanda tangan dokter pada rekam medis elektronik. Penelitian ini menggunakan metode yuridis normatif, dengan dua pendekatan, yaitu pendekatan perundang-undangan dan pendekatan konseptual. Hasil penelitian menunjukkan bahwa PIN dan Tanda Tangan Elektronik secara sah dapat menggantikan tanda tangan dokter di EMR, namun mempunyai kekuatan pembuktian yang berbeda. Kekuatan alat bukti EMR tergantung pada sudut pandang hakim yang dipengaruhi oleh keabsahan alat bukti EMR, yaitu ada/tidaknya PIN dan tanda tangan elektronik sebagai fungsi verifikasi dan autentikasi.*

Kata Kunci : *Biometrik, Alat Bukti, Elektronik, Rekam Medis dan Verifikasi*

INTRODUCTION

Health development aims at increasing awareness, willingness and ability to live healthy in the realization of welfare in the Preamble to the 1945 Constitution of the Republic of Indonesia. This is carried out by providing efforts to the community in achieving the goal of increasing quality and affordable health status.[1]Efforts to improve health status require the availability of health resources, where the two main components are health workers and health service facilities.[2]Provision of health facilities can support efforts to improve services to the community.

Hospital is one form of health service facility. Health workers provide health services with the obligation to provide quality, optimal and sustainable services. The way to realize this obligation is by recording and documenting it in the medical record file properly, accurately and responsibly by these health workers.[3]

Medical records are not just health records and documentation. Medical record is a file that contains the patient's identity, every medical intervention performed on the patient (from the beginning) in connection with the provision of health services. These records and documentation must be made chronologically, systematically and accurately, so as to provide information about the course of a person's illness, examinations that have been carried out on them, treatment plans, clinical observations and treatment results, approval / refusal of action, discharge summary, name and signature of the health worker providing the health service. All of that must also meet the principle of continuous service (continuity of care).[4]

Medical records have been regulated in several laws, namely among others Law Number 29 of 2004 concerning Medical Practice (here in after referred to as the Medical Practice Law), Law Number 44 of 2009 concerning Hospitals (here in after referred to as the Hospital Law), and Permenkes Number 24 of 2022 concerning Medical Records (here in after referred to as Permenkes Medical Records 2022), as the implementation of Article 47 paragraph (3) of the Medical Practice Law. The regulation contains the obligation of a doctor and dentist to make complete, clear and accurate medical records. The Permenkes also mentions the importance of affixing the identity of the name, time and signature of the health worker.

Medical records are part of the health information system subsystem in health care facilities. The role of medical records is important and closely related to the function of medical services. Recording of medical records is very important and closely related to the function of medical services. Recording of medical records can be made manually and electronically. The management of manual and electronic medical records must be able to guarantee legal certainty and legal protection for all elements of all medical services in health care facilities, both at the primary and advanced levels.[5]

In the 2022 Permenkes Medical Record, every health service facility is required to organize Electronic Medical Records. Electronic medical records are basically the use of electronic methods to collect, store, process and access patient medical records in health care facilities that have been stored in a multimedia database management system. A

[1] Hafld Abbas, et.al. Buku Pedoman Hak Asasi Manusia bagi Dokter dan Pasien dalam Mencegah Malpraktek Kedokteran Badan Penelitian dan Pengembangan HAM Departemen Hukum dan HAM RI, 2008, p.1.
[2] Nabil Atta Samandari, Wila Chandrawila S dan Agus H. Rahim, Kekuatan Pembuktian Rekam Medis Konvensional dan Elektronik, dalam *SOEPRA Jurnal Hukum Kesehatan* Vol. 2, No. 2, 2016, p.154.
[3] *Ibid*. p.156
[4] *Ibid*. p.158
[5] Irine Diana Sari W, Manajemen Rekam Medik, STIKES Surya Global, Yogyakarta, 2006,p.15.

person's health information is recorded using electronic media by one or more integrated health professionals. Relevant health care workers must be able to re-access electronic medical records using computers so that this system can provide care and health services efficiently and effectively.[6]

Medical records have an important role and function in the world of law, especially in the field of proving medical dispute cases. Medical records can be used as evidence and help litigants to be able to recall events that occurred.[7]In legal cases, the absence of medical records can corner or harm health workers and hospitals. Because if there is no medical record, it can be assumed that there is no evidence of the implementation of the medical action, so that both conventional medical records and electronic medical records must be used as valid evidence.[8]

Based on the scope of civil law in accordance with Article 1866 of the Civil Code (BW) it is explained that the means of evidence are valid and especially written evidence. Whereas in criminal law, a letter (writing) is also one of the five legal pieces of evidence. This is stated in Articles 183 and 184 of the Criminal Procedure Code (KUHAP), which say that in proving a case a minimum of 2 valid pieces of evidence and a judge's conviction are needed. What applies based on these regulations is Conventional Medical Records so that it can raise new questions about the validity of Electronic Medical Records.

Based on the elucidation of Article 46 paragraph (3) of the Medical Practice Law, it is stated that what is meant by officers are doctors or dentists or other health workers who provide direct services to patients. If the recording of medical records uses electronic information technology, the obligation to affix a signature can be replaced by using a personal identification number (here in after referred to as a PIN/Personal Identification Number). However, this personal identification number can only carry out the function of verification, not authentication of a person, so that the PIN cannot be used as an authentication value in proving an Electronic Medical Record.[9]

Law No. 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as the ITE Law) it is explained that this Law does not recognize the existence of Electronic Medical Records. The ITE Law only recognizes electronic documents, namely any electronic information that is forwarded, sent, received, or stored in analog, digital, electro-magnetic, optical, or the like, which can be seen, displayed, and/or heard through a computer or electronic system. Based on this understanding, Electronic Medical Records can be equated as electronic documents in the ITE Law which will be declared valid if using the Electronic System in accordance with the provisions stipulated in the ITE Law. Electronic documents are also equipped with electronic signatures. An electronic signature is a signature filled with electronic information that is attached to, associated with, or related to other electronic information that is used as a means of verification and authentication. This examines the legal basis of electronic medical records when used as evidence.

Article 30 paragraph (1) of the 2022 Permenkes Medical Record states that in the context of security and protection of RME data, the head of the Health Service Facility

[6] Potter dan Perry, Fundamental of Nursing 7 th Edition, Missouri, St.Louis, 2009, p, 15.

[7] Sri Siswati, Etika dan Hukum Kesehatan, Rajawali Pers, Jakarta, 2017, p.110.

[8] Septi Nabora Lababan, et al., Rekam Medis Konvensional dan Elektronik sebagai Alat Bukti dalam Perkara PIdana, dalam *Al'Adl Jurnal Hukum* Vol.12, No. 22, Juli 2020, p.257.

[9] Chodijah Febriyani, Pentingnya Mengetahui Perbedaan dan Fungsi PIN, Password, dan OTP, dalam Pentingnya Mengetahui Perbedaan dan Fungsi PIN, Password,... (industry.co.Id),, accessed on August 27 2022, at 15.09 WIB.

grants access rights to health workers and/or other workers at health service facilities. In addition to granting these access rights in the framework of data security and protection, the implementation of RME can be equipped with electronic signatures. Based on this, two options emerged to replace the doctor's signature in RME, namely PIN and electronic signature as a function of verification and authentication of the health worker concerned.

This study aims to determine the legality and strength of proof of PIN and Electronic Signature as a substitute for a doctor's signature in electronic medical records.

RESEARCH PROBLEMS

The formulation of problem in this research included 1) what are the provisions and functions for implementing PINs and electronic signatures as a substitute for a doctor's signature on the RME; 2) What is the legality of PIN / biometric verification / electronic signature as a substitute for a doctor's signature on electronic medical records as evidence in court

METHOD

This type of research used a normative juridical approach.This research approach uses a statutory approach (statute approach) and a conceptual approach (conceptual approach). The method of analysis uses the method of legal analysis of deductive legal materials. This researchby conducting an assessment of the legality and strength of evidence of electronic medical records, especially with regard to PINs and electronic signatures as a substitute for a doctor's signature. The legal materials used include:

a. Primary Legal Materials
   1. Law of the Republic of Indonesia Number 29 of 2004 concerning Medical Practice..
   2. Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions.
   3. Law of the Republic of Indonesia Number 36 of 2009 concerning Health amendment to law no. 17 of 2023 concerning health.
   4. Law of the Republic of Indonesia Number 44 of 2009 concerning Hospitals.
   5. Regulation of the Minister of Health of the Republic of Indonesia Number 269 / MENKES / PER / III / 2008 concerning Medical Records.
   6. Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records.
   7. Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions.

   This research was conducted in 2022 so at that time the research study still used Law No. 36 of 2009 concerning health. Currently the Health Law has changed to Law No. 17 of 2023. The normative study uses the legal basis that was in effect at the time the research took place and was completed before 2023. This makes the legal basis for this normative study still use Law No. 36 of 2009 concerning Health which has now become Law no. 17 of 2023 about health.

b. Secondary Legal Materialsr
   Secondary legal materials used in writing this thesis are text books about law that are relevant to the legal issues raised and written about in this thesis, such as related literature and books. The method of analyzing legal materials used is a deductive

method, which is guided by basic principles and then presenting the object to be studied, so moving from general principles to specific principles

DISCUSSION

Provisions and Functions of Implementing PIN and Electronic Signature as a Substitute for Doctor's Signature in RME

The Hospital Law, Article 29 paragraph (1) letter h states that every hospital has the obligation to maintain medical records, but there are no provisions in the implementation of these medical records. In his explanation what is meant by the implementation of medical records is carried out in accordance with standards which are gradually being endeavored to reach international standards, but it is not written that the provisions for organizing medical records are regulated by a ministerial regulation.

Provisionapplication of a PIN and electronic signature as a substitute for a doctor's signature on RME. According to the 2022 Regulation of the Minister of Health on Medical Records, it is explained that electronic medical records are required for all health service facilities, starting from hospitals, health centers, clinics, pharmacies, health laboratories, halls, independent practice places for doctors and dentists, as well as other health service facilities stipulated by Minister. The implementation of electronic medical records is carried out from the time the patient enters until the patient returns, is referred or dies.

The function of implementing a PIN/biometric verification/electronic signature in lieu of a doctor's signature in an electronic medical record is explained that pthere are conventional medical records, there is a security system that regulates how medical records are made and stored. This conventional medical record security system is influenced by the workflow system of health care facilities, as well as the health workers concerned. After the patient registers, a new medical record is made or a previous medical record is found, if any. The officer concerned searches for and retrieves medical record documents and then takes them to the examining doctor's table. After the doctor examines it, the doctor writes the medical record information, then the document is returned to the medical record document storage room. Based on this, there are two important security systems, namely the security of the medical record document storage space and the security of medical record information written by doctors.

The security of the medical record document storage room regulates how these documents are resistant to anything that can physically damage the medical record documents, including who is responsible for and holds the key to the room. The security of medical record information written by doctors on conventional medical records depends on the character of the doctor's writing, including the full name, date of service and doctor's signature.

In RME, the security of the medical record document storage space is replaced by a computer device where the RME digital-based storage media system is in the form of a cloud computing platform server that has been approved and certified according to laws and regulations, and/or other digital storage media developed using information and technology. approved.

Article 46 paragraph (3) of the Medical Practice Law, the obligation to sign can be replaced by using a PIN, but the PIN as a substitute for the signature function in RME is very inappropriate, because the PIN only performs the verification function, which is a kind of challenge code, and cannot be categorized as something unique and inherent that reflects

a person's authentication function. The authentication function must be able to ensure that only the person concerned owns/uses it, so that a PIN alone is not strong enough to be used as authentic evidence in proving an Electronic Medical Record.

Another option for this second factor is the use of biometrics (biometric verification) such as fingerprints or eyeballs (iris or retina), known as the Something You Are factor. Information that can only be provided by the second factor is absolutely necessary in the authentication process

This is stated in the Elucidation of the Medical Practice Law Article 46 paragraph (3). The PIN is used to protect access to the electronic medical record, so it is hoped that only the health worker concerned can access it. The use of a PIN is not explained in more detail by law. According to the 2022 Medical Record Regulations, there is no further mention of the specific use of PINs in electronic medical records. The 2022 Regulation of the Minister of Health on Medical Records provides a wider scope, namely giving authority to the heads of health service facilities to determine and independently regulate the type of use of the medical record security and authentication system. This is manifested in granting access rights to the health workers concerned, so that the use of a PIN is not mandatory for electronic medical records. In article 31,

The 2022 Regulation of the Minister of Health on Medical Records states that the regulation of medical records aims to ensure the security, privacy, reliability and accessibility of Medical Record data. Electronic medical record storage must guarantee the security, integrity, confidentiality and availability of electronic medical record data. Standards of data security, information confidentiality, integrity and availability must be met in Electronic Medical Records. The term confidentiality refers to the guarantee of data and information security from internal or external intrusion by parties who do not have access rights to prevent the use and dissemination of data and information in the Electronic Medical Record.

Legality of PIN / Biometric Verification / Electronic Signature Substitute for Doctor's Signature in Electronic Medical Records as Evidence in Court

Electronic evidence must meet the requirements both formally and materially as evidence that can be declared valid and used in court. These provisions and requirements are to guarantee legal certainty and function as a test tool in determining the validity of evidence so that judges can be sure of the legal facts presented through electronic evidence. Electronic evidence has a wide scope and various types. Each type of electronic evidence has characteristics that technically require separate handling in determining its legal validity.[10]

One of the requirements for electronic evidence can be accepted in court by fulfilling the formal and material requirements. In this case, electronic evidence in its original form as well as the printed results have the same value. This is in accordance with Article 5 paragraph (1) of the ITE Law which states that Electronic Information and/or Electronic Documents and/or their printouts are valid legal evidence.

Law Number 19 of 2016 concerning Amendments to Law No. 11 of 2008 (UU ITE), in the elucidation section of Article 5, states that the existence of Electronic Information and/or Electronic Documents is binding and recognized as valid evidence to provide legal certainty for the Implementation of the System and Electronic Transactions, especially in proving and all matters relating to legal actions carried out through Electronic Systems.

[10] Eddy Army, *Bukti Elektronik dalam Praktik Peradilan*, Sinar Grafika, Jakarta, 2020, p.117.

Thus, to guarantee the fulfillment of the requirements referred to, a scientific method supported by special technology is needed to examine electronic evidence. Formal requirements regarding electronic evidence are regulated in Article 5 paragraph (4) and Article 43 of Law Number 19 of 2016 which states that:

a. Such Electronic Information or Documents are not letters which according to law must be made in written form, and letters and their documents which according to law must be drawn up in the form of notarial deeds or deed made by the official making the deed.
b. A search or confiscation of an Electronic System must be carried out with the permission of the chairman of the local district court.
c. A search or seizure of an Electronic System must maintain the maintenance of public service interests.[11]

The material requirements for electronic evidence are regulated in article 5 paragraph (3) of the ITE Law, namely electronic information or documents are declared valid when using an electronic system in accordance with the provisions stipulated in the ITE Law. Furthermore, it is regulated in Articles 15 and 16 of the ITE Law that can obtain more detailed requirements, namely that the electronic system must:

a. Reliable, safe and responsible.
b. Can display information or electronic documents back in its entirety.
c. Can protect the availability, integrity, authenticity, confidentiality and accessibility of Electronic Information.
d. Equipped with procedures or instructions and can operate according to the procedures or instructions that have been set.[12]

In addition, Article 6 of the ITE Law also provides material requirements regarding the validity of electronic evidence, namely that electronic information or documents are considered valid as long as the information contained therein can be accessed, displayed, guaranteed for integrity, and can be accounted for so as to explain a situation. The ITE Law does not regulate the means or methods used to collect, secure, display or guarantee the integrity of electronic evidence information. Because basically the ITE Law adheres to a technology-neutral principle, which means that methods or methods for collecting and securing electronic evidence can use available technology, as long as it can meet the requirements for the validity of electronic evidence.[13]

Association of Chief Police Officers(ACPO) provides four principles in handling electronic evidence.[14]First, all handling of electronic evidence carried out by law enforcement officials must not result in changes or damage to data so that it can be accepted in court, thus the data obtained during an investigation is the same as the data presented at trial. Damage, deletion or modification of data can occur by improper data handling.

Second, in cases where a person has to access original data on a computer or storage medium, that person must be competent to do so and be able to explain the relationship of the action to the data and what will happen as a result of that activity.

[11] *Ibid*. p.118
[12] *Ibid*. p.119.
[13] *Ibid*. p.
[14] Janet Williams, ACPO Good Practice Guide for Digital Evidence, Association of Chief Police Officers of England, Wales & Northern Ireland, 2012, p.6.

The third principle is that there must be proper protocols for collecting and examining electronic evidence. The process in question includes finding evidence containing electronic evidence, wrapping evidence, examining, analyzing, and reporting. Thus, any interested party can examine the processes and procedures in question and obtain the same results. The fourth principle is that there must be a party or official who is responsible for ensuring that the implementation of activities is in accordance with laws and regulations as well as the entire process and procedure referred to.

According to Eddy Army, the steps that must be passed to determine the validity of an electronic evidence are as follows:

1. Electronic documents or recording devices must comply with standardization.
2. Must read by experts.
3. The expert must be certified.
4. The tools used to read electronic evidence comply with the standards.
5. The process of reading electronic evidence must be correct.
6. Laboratory or place for reading electronic evidence in accordance with standardization.[15]

The validity of an electronic evidence greatly determines the verification process to determine whether or not a perpetrator of a crime is guilty. Thus, whether or not the electronic evidence that will be presented before the court is valid or not will determine the level of validity of the evidence in evidence before the court. When the system used is issued by an accurate and reliable electronic system, the existence of electronic documents is also accurate and reliable. An electronic system must be validated before being used, so that the documents produced from it can be trusted. Electronic evidence is different from non-electronic evidence, because electronic evidence has characteristics that can be easily manipulated, so there are often doubts about the validity of electronic evidence.[16]

Authentic deed is evidence that has perfect evidentiary power. According to a legal perspective, authenticity is generally understood only if a process of creating information is carried out with strict procedures. Initially, the medical record, when it was still in a conventional form, required a signature, the name of the officer and the date as proof of verification and authentication that the health worker had actually written it. In conventional medical records, it can be proven more easily by looking at the signature of the health worker. In the electronic medical record the name, signature and date are made depending on the electronic medical record program used. The electronic medical record program used depends on the leadership of the health care facility.[17]

PIN and biometric verification here play an important role. The PIN used in electronic medical records is a PIN for accessing medical records. It is also possible that there is an electronic medical record program that provides double protection. For example, when filling in the action it is asked again regarding the access key to save the action data. However, the use of a PIN is said to be weaker because it still uses a single factor authentication system. This security system is a traditional authentication system that relies on mutual trust between the user and the medical record service provider. The PIN depends on the user how strong he is to create and store the PIN and protect it from hackers.

Electronic signatures can be used on electronic medical records. This aims to improve security and data protection. In the 2022 Permenkes Medical Record Article 31, electronic

[15] Eddy Army, Supra 10., p.128.
[16] *Ibid*. p.129
[17] Janet Williams. Supra 14. p.8

signatures are intended as a means of verification and authentication of the contents of the Electronic Medical Record and also function as the identity of the signer. Furthermore, it is determined that an electronic signature has legal validity and legal consequences as long as it meets the requirements as specified in Article 11 of the ITE Law, namely as follows:

a. Electronic signature creation data is related only to the signers.
b. The data on making an electronic signature during the electronic signing process is only in the power of the signatory.
c. All changes to the electronic signature that occur after the time of signing can be known.
d. All changes to electronic information related to the electronic signature after the time of signing can be known.
e. There is a certain way used to identify who signed it.
f. There are certain ways to show that the signatory has given an consent to the relevant Electronic Information.

Digital evidence is difficult to accept as evidence if it follows the classic theory of evidentiary law, which is called the "best evidence rule", which states that valid evidence is original evidence that can be brought to court, unless it is does not exist, and its non-existence does not occur due to serious mistakes on the part of those who have to prove it. Therefore, based on the best evidence doctrine, a copy of the letter (not the original) has no value as evidence in court. As with digital evidence such as e-mail, fax letters and electronic signatures, the failure to bring the originals to court can lead to serious legal problems in the field of evidentiary law.[18]

Several basic criteria or provisions that need to be considered in relation to the recognition of digital evidence are as follows:

a. The treatment of electronic data by law
   It was decided that no one including the courts may object to the legal effect, its legality or its implementation on the grounds that it relates solely to electronic data. In addition, if it is absolutely impossible for the parties to access the original text of the document, then the court should also not deny the legal effect of the document.[19]
b. Presumption of Authenticity
   The principle of presumption of authenticity is a provision that is often used to prove the legitimacy/authenticity of digital documents/data or the authenticity of digital signatures.
c. Signature issues in medical records
   Based on the law of evidence, the signature on a document has an important role. It's the same as the signature of a health worker on a medical record. In the 2022 Permenkes Medical Record, Article 16 that the recording and documentation of the results of examinations, treatment, actions and other health services that have been provided to patients must be complete, clear and carried out after the patient receives health services by including the name, time and signature of the health worker providing health services.
d. Period of obligation to keep Electronic Medical Records
   Based on the 2022 Regulation of the Minister of Health on Medical Records, the period for storing electronic medical records is at least 25 (twenty five) years from the date of

[18] Munir Fuady, Teori Hukum Pembuktian PIdana dan Perdata, Citra Aditya Bakti, Bandung, 2020, p.151.

[19] *Ibid*. p.153

the patient's last visit. After the time limit expires, if the data is still to be used, the Electronic Medical Record data may not be destroyed.

e. Recognition only in certain ways and formats
There are various types and formats of electronic data. Not all electronic data is reliable and appropriate to be used as evidence in court. For this reason, the law of evidence should strictly limit which electronic data and in what format can be admissible in court.
Electronic Medical Records can also be used as evidence for Instructions. Clues are actions, events or circumstances, which because of their correspondence, both between one and the other, as well as with the crime itself, indicate that a crime has occurred and who is the perpetrator.

The application of Article 188 paragraph (1) of the Criminal Procedure Code by judges is aimed at strengthening the judge's conviction whether a crime has occurred and whether the defendant is the perpetrator. Guidance evidence can not only convict the defendant but also conversely can free the defendant from lawsuits, where the judge with his conviction connects all the evidence available during the trial process.

In civil cases, according to Article 1866 of the Civil Code (BW), the means of proof include written evidence, witness evidence, presumptions, confessions and oaths. Written evidence is the main evidence. In Civil Law, what is meant by written evidence is anything that contains punctuation marks that can be understood and contains a certain thought and is used as evidence. Written evidence that applies to civil procedural law is based on the agreement of both parties. RME cannot be included in written evidence because the nature of RME is a recording and documentation only, not an agreement, so it cannot include conditions in written evidence, namely there are signatures from the parties.[20]

RME can be included in a presumption, which is indirect evidence. Prejudice is a conclusion that by law or by a judge is drawn from an event that is publicly known to an event that is not publicly known. Allegation alone is the same in nature as a "signal" or "appointment", namely nothing other than a conclusion drawn by a judge from an event or situation that has been proven, thus explaining an event or situation that is not proven. The evaluation of the strength of the allegation evidence is left to the discretion and opinion of the judge, so that mere presumption is free evidence, not absolute evidence. In the context of using electronic documents,

CONCLUSION

The legality of PIN/Biometric Verification/Electronic Signature as a substitute for Signatures on Electronic Medical Records is regulated in Law Number 29 of 2004 concerning Medical Practice Article 46 paragraph (3), Minister of Health Regulation 24 of 2022 concerning Medical Records, and the Information and Transaction Law Electronic Number 11 of 2008 Article 11. Under the Medical Practice Law, a PIN can replace the signature requirement in an Electronic Medical Record. Permenkes Medical Record 2022 states that Electronic Medical Records can be equipped with Electronic Signatures as verification and authentication of the signer's identity. Electronic Signatures are clarified in the ITE Law and must meet the requirements in accordance with applicable laws. Unspecified Biometric Verification can be a substitute for a signature,[21].

[20] Efa Laela Fakhriah, *Bukti Elektronik dalam Sistem Pembuktian Perdata*, Refika Aditama, Bandung, 2017. p.15.

[21] Id.

The strength of electronic medical record evidence depends on the judge's point of view and the judge's assessment of the evidence. The judge's point of view, namely first, as new evidence in the form of electronic information and/or documents, refers to Article 44 of the ITE Law; secondly as an extension tool of documentary evidence; thirdly as a support in evidence instructions; Fourth, Electronic Medical Records can produce expert evidence, namely Digital Forensics. The judge's assessment of the submitted evidence is influenced by the legitimacy of the Electronic Medical Record (Electronic Medical Record security system and the presence/absence of a PIN/Biometric Verification/Electronic Signature as a function of verification and authentication), as well as how to retrieve, store and deliver the evidence to to court (bewijsvoering).

SUGGESTIONS

Suggestions that can be submitted are explained that the leadership of Health Service Facilities can choose/create Electronic Medical Records that use PIN/Biometric Verification/Electronic Signature as a security system with conditions in accordance with applicable laws and regulations. The Bill on Civil Procedure Law relating to RME will be passed soon because proof can be carried out with all evidence, unless the law stipulates otherwise, so that RME can become one of the valid pieces of evidence.

REFERENCES

Chodijah Febriyani. The Importance of Knowing the Differences and Functions of a PIN. Passwords. and OTPs. In The Importance of Knowing the Differences and Functions of a PIN.Passwords.... (industry.co.id). accessed on August 27, 2022. at 15.09 WIB.

Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions. State Gazette of the Republic of Indonesia of 2019 Number 185. Supplement to the State Gazette of the Republic of Indonesia Number 6400.

Hafid Abbas. et.al. Handbook of Human Rights for Doctors and Patients in Preventing Medical MalpracticeHuman Rights Research and Development Agency Ministry of Law and Human Rights of the Republic of Indonesia. 2008

Irine Diana Sari W. Medical Records Management. Yogyakarta. STIKES Solar Global. 2006

Janet Williams. ACPO Good Practice Guide for Digital Evidence. Wales & Northern Ireland. Association of Chief Police Officers of England. 2012

Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions. State Gazette of the Republic of Indonesia of 2008 Number 58. Supplement to the State Gazette of the Republic of Indonesia Number 4843.

Law of the Republic of Indonesia Number 29 of 2004 concerning Medical Practice. State Gazette of the Republic of Indonesia of 2004 Number 116. Supplement to the State Gazette of the Republic of Indonesia Number 4431.

Law of the Republic of Indonesia Number 36 of 2009 concerning Health. State Gazette of the Republic of Indonesia of 2009 Number 144. Supplement to the State Gazette of the Republic of Indonesia Number 5063.

Law of the Republic of Indonesia Number 44 of 2009 concerning Hospitals. State Gazette of the Republic of Indonesia of 2009 Number 153. Supplement to the State Gazette of the Republic of Indonesia Number 5072.

Munir Fuady. Legal Theory of Criminal and Civil Proof. Bandung. Image Aditya Bakti. 2020

Nabil Atta Samandari. Wila Chandrawila S and Agus H. Rahim. The Proof of Conventional and Electronic Medical Records.in SOEPRA Journal of Health Law Vol. 2. No. 2. 2016.

Potter and Perry. Fundamentals of Nursing 7th Edition. Missouri. St. Louis. 2009

Regulation of the Minister of Health of the Republic of Indonesia Number 269 / MENKES / PER / III / 2008 concerning Medical Records.

Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records.

Septi Nabora Laban. et al.. Conventional and Electronic Medical Records as Evidence in Criminal Cases. in Al'Adl Journal of Law Vol.12. No. 22. July 2020

Sri Siswati. Health Ethics and Law. Jakarta. Rajawali Press. 2017