Legality for Electronic Signatures in Implementing Electronic Medical Records

I Wayan Dody Putra Wardana1*, Ni Ketut Supasti Dharmawan2, Ni Luh Gede Astariyan3

*Correspondence Author: dodyputra01@gmail.com
1Magister Hukum Kesehatan, Universitas Udayana, Denpasar, Bali, Indonesia
23Fakultas Hukum, Universitas Udayana, Denpasar, Bali, Indonesia

ABSTRACT

An electronic signature is an authentic marker to show a person's responsibility. Electronic signatures also ensure confidentiality, integrity, authorization, access control, and non-repudiation of information in electronic medical records. Therefore, this research was conducted to determine the legal aspects of electronic signatures in administering electronic medical records. This research used a qualitative method with a normative juridical approach. The research sources were based on laws, government regulations, journals, and other tertiary related sources to electronic signatures and electronic medical records in health facilities. Research findings illustrated that Minister of Health Regulation Number 24 of 2022 concerning medical records only defined electronic signatures as an authentication and verification of the security and privacy of medical record information. Electronic signatures are specifically regulated by Constitution Number 11 of 2008 concerning Information and Electronic Transactions and Government Regulation Number 71 of 2019 concerning Electronic Systems and Transaction Operators. Both certified and uncertified electronic signatures have legal legitimacy in their application in electronic medical records. However, how they are supported by evidence is what makes them different.

Certified electronic signatures are more trustworthy than uncertified electronic signatures.

INTRODUCTION

In this era, technological transformation provides progress in the health sector, resulting in several information systems emerging to improve the quality of health services in healthcare facilities. One of the implications of current technological advances is the shift...
from conventional medical records to electronic medical records. The government's commitment, as stated in the 2020-2024 vision of the NMTDP (National Medium Term Development Plan), requires all health service facilities to transform health information technology, like electronic medical records, by the end of December 2023. This obligation is contained in Minister of Health Regulation Number 24 of 2022 concerning Medical Records.

An electronic medical record is an electronic-based health record that can be inputted, grouped, managed, and read by authorized individuals at the hospital (Febriyani, 2022). Moreover, electronic medical records can also be defined as a record of a patient's history of illness and treatment that is created electronically in the administration of medical records in a Health Facility, as stipulated in Article 1 Paragraph 2 of Minister of Health Regulation Number 24 of 2022 on Medical Records. From the two definitions above, electronic medical records are medical records made using an electronic system that can be accessed and intervened by an authorized person in a health facility. Implementing information systems in medical record management undoubtedly offers positive implications, including easy, accurate, and prompt access to patient data, thus enhancing the quality of services delivered by healthcare professionals in medical institutions.

The convenience provided by electronic medical records has a good impact. It poses a new challenge: threats to medical record information, including confidentiality, privacy, and security of patient medical data by irresponsible parties (Lestari, 2021). This problem arises because the quality of the medical record contents must be legally substantiated, ensuring the information therein is legally sound and safeguards the rights of healthcare facility personnel. Given that electronic medical records are not comprehensively regulated within Indonesia's criminal procedure system and are susceptible to data tampering and unauthorized access, considerations arise. Considering electronic medical records as testimony in court, we must prove that the official makes the data and cannot be manipulated (Basyarudin, 2022). Therefore, a strategy is needed to ensure the security of medical record information so that electronic medical records fulfill the aspects of confidentiality, integrity, non-repudiation, and authentication (Pangaribuan et al., 2023).

Determining the validity of electronic signatures to ensure accountability for completing electronic medical records lies in the authentication and verification of the signer's identity. This step is the key to identifying the individual responsible for filling out or entering the medical data into the patient's medical record, which is identified from their electronic signature (Noor, 2021). Identifying the signer within an electronic medical record involves cross-referencing the public key embedded in the original medical document with the private key possessed by the signer. This procedure confirms both the content and the authorship of the signature. Therefore, medical records that are made cannot be falsified or changed by people who do not have the authority to access them (Tandiahang et al., 2019).

An electronic signature is electronic information data used to identify someone who has signed a document to ensure the consent and information belong to the signatory (Fernando & Salam, 2023). In other words, electronic signatures are tools to validate and authenticate the ownership of a signature. An understanding of this matter can be observed from Article 31 Paragraph 2 of Minister of Health Regulation Number 24 of 2022 on Medical Records, which emphasizes the employment of verification and authentication in
affixing electronic signatures to electronic medical records to ensure the authenticity of the identity of the signatory or the individual responsible for completing the electronic medical records (Fitriyah et al., 2022). However, this article does not explain the types of signatures with legal validity that can be used to implement electronic medical records.

Electronic signatures in electronic medical records are important to prevent falsification of patient medical data, for example, a falsifying rapid results case by falsifying a doctor's signature and stamping a letter allegedly issued by one of the Community Health Centers around the Port of Tanjung Perak, Surabaya (Kompas.com, 2020). Another case is doctors falsifying patient signatures on patient consent forms (informed consent) when performing medical procedures on critical patients (Syarifah, 2013). These cases show that the signature verification and authentication process was not carried out, resulting in signature falsification cases, which led to lawsuits against implicated health workers. Such scenarios are not precluded from managing electronic medical records in healthcare facilities. Falsifying medical records in legal proceedings, as examined through Article 278 Paragraph 1 of Law Number 1 of 2023 within the Criminal Code, constitutes a grave offense warranting a maximum prison sentence of 7 years. This regulation is the legal foundation for holding individuals accountable for falsifying medical records (Semara & Purwani, 2019).

Based on the mentioned cases, electronic signatures for electronic medical records are highly important to ensure data accuracy, information integrity, and accountability for the content of these records. Moreover, clear legal guidelines are necessary to define who has the authority to verify digital signature authenticity. This issue has prompted researchers to research how to regulate electronic signature legality arrangements in electronic medical records and how to prove the law of electronic signatures as authentication in implementing electronic medical records.

### RESEARCH METHOD

#### Types of research

This research used qualitative methods with a normative juridical approach. The normative juridical approach focuses on legal norms, legal principles, and legal doctrines that align with each other to understand their substance and describe the problems regarding regulating electronic signatures as authentication in administering electronic medical records (Benuf & Mahmudah, 2020). This legal research is based on statutory regulations from the perspective of statutory hierarchy (vertical) and harmonious statutory relations (horizontal). This method provides prescriptive justification regarding legal issues that make it a norm system (Muhaimin, 2020). In a vertical hierarchy of laws, lower regulations must not conflict with higher regulations. Likewise, in a horizontal legal hierarchy, legal provisions governing the same thing must not conflict with norms or one another (Hasan, 2017; Wahab & Surya, 2023).

#### Sources of legal materials

This research's sources of legal materials consist of primary, secondary, and tertiary sources. The distribution of legal material sources is as follows.
Primary legal material sources are the main sources in this research. Secondary legal material sources provide explanations or instructions to primary legal material sources. Meanwhile, tertiary sources of legal materials are used to explain or guide primary and secondary legal materials.

Data collection
Data collection in this research used literature and document study techniques. Document studies include laws and regulations issued by government agencies, while literature studies include books, scientific journals, and other publications related to this research topic.

Data analysis
Research objects from legal sources collected and identified systematically are then carried out qualitative juridical analysis with the following stages:
1. Classifying criteria according to the problem topic;
b. Classifying results are then organized;
c. After organizing, an evaluation is carried out, arguments are given, and conclusions are
drawn to answer the research problems (Purwati, 2020).

RESULTS AND DISCUSSION

Legality Arrangements for Electronic Signatures in Electronic Medical Records

Placing a signature on the medical record is mandatory. The necessity of signing medical records is explicitly outlined in Articles [16][26] of Minister of Health Regulation Number 24 of 2022 concerning Medical Records and Article 46 of Law Number 29 of 2004 concerning Medical Practice. These stipulate that every health worker practicing must record a complete and clear medical record and include the health worker's name, the time when the medical record was made, and the signature of the health service provider. Signatures must be given to every medical record recording because they are original and authentic data as accountability for data and information in electronic medical records (Prasetya, 2022).

An electronic signature is a composite of various electronic information affixed to, connected with, or associated with other electronic data utilized for verification and authentication as stipulated in Article 1 Paragraph 12 of Constitution Number 11 of 2008 concerning Information and Electronic Transactions. The role of electronic signatures is to avoid someone's denial of electronic documents or the contents of electronic documents sent or created so that the authenticity of electronic documents can be trusted (Pangaribuan et al., 2023). Proving the authority of medical record-filling officers can be proven by affixing an electronic signature to each medical record. Talking about electronic medical records as legal evidence will drag health workers who fill out electronic medical records on suspicions of malpractice. Hospital doctors and patients have a medical and legal relationship (Amir, 2019). In allegations of malpractice, the validity of the signature is the main responsibility of the doctor in his defense before the court because the signature must be able to identify the signatory and medical record documents signed to avoid falsification or alteration (both signed and signed) documents can be identified (Tandiabang et al., 2019).

Regulations regarding electronic medical records regulate electronic signatures in the electronic medical record system as stipulated in Article 31 Paragraph [1][2] of Minister of Health Regulation Number 24 of 2022 on medical records. However, these regulations do not specifically regulate electronic signatures to documents of medical records; they only explain that electronic signatures can be used for the security and protection of medical information data, as well as for the rules for the function of electronic signatures as a tool for verifying and checking the authenticity of health workers. Suppose we view medical records as electronic documents based on Article 60 Paragraph 2 of Government Regulations 71 of 2019 on Electronic System and Transaction Operators. In that case, two types of digital signatures can be used in electronic documents: certified and non-certified. Certified electronic signatures have electronic certificates made using the services of electronic certificate providers. In contrast, non-certified electronic signatures do not have electronic certificates and are made without the services of electronic certificate providers. As stipulated in Article 11 Paragraph 1 of Constitution Number 11 of 2008 concerning Information and Electronic Transactions, Government Regulations Number 71 of 2019 concerning Electronic System and Transaction Operators, and Minister of Communication and Information
Regulation Number 11 of 2018 concerning Electronic System Organizers, they have stipulated that electronic signatures for electronic medical record documents have validity, legal force, and legal consequences.

The electronic or digital signature must guarantee the integrity of the electronic medical record document and identify the health worker who has signed it. Guaranteed data integrity in an electronic signature can be obtained using asymmetric cryptographic techniques (Disemadi & Prasetyo, 2021). Asymmetric cryptographic techniques are a type of contemporary cryptography in which encryption and decryption are carried out using complex algebraic, algorithmic, and mathematical theories using two key combinations, namely a public key and a private key (Vardhan & Narad, 2018). The private key is made specifically for individual health workers with limited properties known only to that individual. In contrast, the public key is open (public) and contains public information used to match signatures (Kementerian Komunikasi dan Informatika, 2021). The private key must have a public key because, in asymmetric cryptographic techniques, it results from changing the code of the two keys bound to each other. This attachment allows the private key to open a code change resulting from the public key and vice versa. When the private key cannot open the code change from the public key, these two keys are not bound to each other (Cahyadi, 2020). Installing the private key and public key on the electronic certificate can indicate a change by moving or removing one of the characters in the electronic medical record document. According to Article 62, paragraph 6b of Government Regulation Number 71 of 2019 concerning Electronic Systems and Transaction Operators, a signature is changed after the signature is affixed, the process of verifying the suitability of the two keys becomes invalid so that the recipient of the document can know that the document is not original (Pangaribuan et al., 2023).

The latest United States and European Union laws have been implemented and state that they can accept certified digital signatures in their legal proceedings. America uses the DSS (Digital signature standard) method, while European Union countries use the PKI (Public Key Infrastructure) method. Both methods are similar to code changes from the public and private keys, which will later be compared as electronic signature requirements used as authentic proof (Noor, 2021). Certified electronic signatures or signatures that have electronic certificates in developed countries have been legally recognized as authentic means of identifying a person. Based on the positive law in force in Indonesia, signatures that have electronic certificates are signatures released by the BSSN (National Cyber and Crypto Agency) or Indonesian electronic certificate providers (PSrE) that have successfully gone through the strict selection stages by the government, in this case by The Ministry of Communication and Information (Kementerian Komunikasi dan Informatika, 2021). The legal certainty of an electronic certificate under Article 1 Paragraph 9 of Constitution Number 11 of 2008 concerning Information and Electronic Transactions states that it designates the legal subject of the parties conducting therapeutic transactions in electronic medical record documents, both medical personnel and patients. Electronic certificates are also able to ensure the right party's identity, the integrity of electronic medical record information, and the non-repudiation of the parties involved in therapeutic transactions in electronic medical records so that this certainty can prevent abuse and violations that may occur in electronic medical records (Kementerian Komunikasi dan Informatika, 2023).
The usage of certified or unauthorized electronic signatures has been acknowledged in the ITE Law. Electronic signatures, as authentication in medical practice, are outlined in Article 46 Paragraph 3 of Law Number 29 of 2004 concerning Medical Practice, specifying that electronic medical records should be affixed with a signature that can be substituted using a personal identification number (PIN). However, relying on a PIN as a replacement for a signature, as stated in the mentioned provisions, is not appropriate because a PIN cannot serve as genuine evidence linked to an individual; rather, it functions as a verification tool (Lestari, 2021). Consequently, using a PIN to substitute electronic signatures in medical records management fails to provide legal certainty due to its inability to identify signatures genuinely.

As per Article 11 Paragraph 1 of Constitution Number 11 of 2008 concerning Information and Electronic Transactions, the PIN cannot fulfill the stipulated requirements because it is categorized as an electronic signature and lacks an electronic certificate. Therefore, utilizing a PIN as a replacement for a signature on an electronic medical record will entail legal implications. This notion is reaffirmed by Article 60 Paragraph 2 of Government Regulation Number 71 of 2019 concerning Electronic Systems and Transaction Operators that the legal consequences of electronic signatures lie in the strength of the proof. Proof in legal disputes plays an important role because the aspect of proof determines the truth of the defense of legal facts, which is the subject of justice (Saruji & Martana, 2015). Proof serves to eliminate objections to evidence submitted in court. Of course, the evidence must have a strong legal aspect of proof. The legal proof of an electronic signature that is not certified is still not strong enough as an electronic medical record authentication tool. However, this signature, based on the perspective of the ITE Law, still has a legal force that is legally recognized by the regulation (Lestari, 2021). Therefore, electronic signatures with legal consequences that guarantee health workers’ use in electronic medical records are certified electronic signatures (PSrE).

The Legal Proof of Electronic Signatures as Authentication in Electronic Medical Records

The understanding of medical records, as emphasized in Minister of Health Regulation Number 24 of 2022 on medical records, explains that the completeness and clarity of medical record filling is legal for every medical record recording to provide legal protection and firmness when electronic medical records are used as legal evidence. Legal proof is the disclosure of a fact to support or disprove an argument made by a party to convince the judge about the truth in a dispute (Hakim, 2022). The proof aspect is the most important factor in electronic medical records when used as evidence in a case, considering that electronic documents are very easy to change, falsify, or duplicate. Article 6 of Constitution Number 11 of 2008 concerning Information and Electronic Transactions states that information contained in an electronic document is recognized as valid before the law as long as the information can be accessed, displayed, accounted for, and remains intact so that it can explain how a problem can occur.

Per the principle of legal certainty, using electronic signatures in electronic medical records can provide legal assurance for health workers in health facilities. Based on Article 36 Paragraph 1, Minister of Health Regulation Number 24 of 2022 on Medical Records, law enforcement, electronic medical record documents can be used as evidence before the court.
The perspective of electronic documents as legal evidence has been regulated in article [5][11] of Constitution Number 11 of 2008 concerning Information and Electronic Transaction Law stipulating that as an extension of procedural law in Indonesia, legally electronic and printed documents can be recognized and used as evidence in court cases. In addition, the regulation states that electronic documents signed with electronic signatures have legal certainty, legal force, and legal consequences as long as they comply with this regulation. These provisions include: (a) the issuance of an electronic/digital signature is only related to the individual, (b) the individual signing has the authority to carry out the process, (c) all changes that occur can be known after the issuance of the electronic signature, (d) there is a method to find out the identity of the signatory, (e) there is a method to show the correctness of the agreement given by the signatory.

The legality of an activity must be regulated in applicable law, in this case, electronic signatures, because it can have legal implications in court claims caused by actions that cause material or material losses to someone (Hapsoro, 2023). So, the legality of an electronic signature can be seen from how the signature has been regulated in the laws applicable in that region. The legal perspective in Indonesia is that electronic signatures have clear legality as regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions and Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Operators and has the legal force and consequences of the use of electronic signatures on electronic documents, in this case, electronic medical record documents (Yuniati & Sidiq, 2020).

Electronic medical records are one of the pieces of evidence in court. In litigation, electronic signatures serve as signature authentication. Every record in the electronic medical record must have an electronic signature as legality, proving that the medical data created and stored is correct (Lestari, 2021). Therefore, a change in electronic medical record documents creates uncertainty and injustice in determining whether or not the party is guilty at trial (Semara & Purwani, 2019).

Electronic signatures can be used in litigation to ensure the authenticity of the signatory and the accuracy and validity of the information in digital medical records (Disemadi & Prasetyo, 2021). Asymmetric cryptographic techniques in electronic signatures demonstrate signature authentication on electronic documents by combining private and public keys to prove that affixing a signature is within the power of the signature owner (Disemadi & Prasetyo, 2021).

Asymmetric cryptography and blockchain techniques can provide a fairly high level of security (Akanksha et al., 2018). In cryptographic techniques, every transaction history or change to medical records data is carried out with an electronic signature to identify, store, validate, and share, recorded permanently, and cannot be changed by anyone unauthorized (Latif, 2023).
Picture 2 illustrates that the medical record kept by private A will be encrypted using the public key he owns and the private key to describe the electronic medical record data contained in the electronic signature to prove the integrity of the recorded data medical (Puspitasari & Permanasari, 2020; Suma, 2019). Private and public keys are asymmetric cryptographic technical infrastructures interconnected and bound to one another (Akshatha et al., 2018).

The integrity of electronic medical record data can be determined in the electronic signature verification process to ensure whether the medical record data has undergone data changes or not. Using the verification calculation \( v \mod n \) (V=D) can interpret that the electronic medical record data is still authentic (without changes); the electronic medical record data has changed so that it becomes inauthentic (Ilyas & Karyati, 2018). In the flowchat, the electronic signature verification process is shown in Picture 3.
Asymmetric and blockchain cryptography techniques are only found in electronically certified signatures. So, certified electronic signatures have a higher evidentiary value than uncertified ones. The certified electronic signatures can be issued by The National Cyber and Crypto Agency or Indonesian Electronic Certificate Providers (PSrE), which have been recognized by the government, including PrivyID, Solusi Net, Peruri, Vda, BPPT, BSrE, and DTB with several steps, including application, verification and publication step (Kementerian Komunikasi dan Informatika, 2022).

An electronic certified signature can provide legal certainty because it has been issued by an institution recognized by the government in Indonesia. In addition, electronic certificates provide authentication, confidentiality, integrity, authorization, access control, and non-repudiation functions. Suppose there is even the slightest change in the information in the electronic medical record. It changes the hash value algorithm on the electronic medical record document to identify authenticity easily and can reduce denial in court if electronic medical records are used as legal evidence (Gokulraj et al., 2021; Vardhan & Narad, 2018).

Presumption of reliability (Presumption de fiabilite) can be used in electronic signatures by fulfilling the minimum requirements in Article 11 of Constitution Number 11 of 2008 concerning Information and Electronic Transactions Law, which are believed to provide certainty, strength, and legal consequences themselves. The difference between the two types of electronic signatures lies in the principle of proof. Article 1875 of the Indonesia Civil Code, where whether or not a signature is legally determined, is largely determined by the recognition of the signer himself. Electronic signatures guarantee trust and legal certainty for users of electronic signatures in administering electronic medical records per these regulations. The guarantee of trust (non-denial) lies in a certified electronic signature, the guarantee of trust is in data authenticity (can designate the owner of the certificate), integrity of information (electronic documents that have been signed can be monitored) and proof of truth (avoiding the indisputability of documents made) (Hakim, 2022). Electronic medical records with certified signatures cannot be denied the accuracy of the information because they can already designate the person who made it and what documents were made. The most important aspect is to have authentication and non-repudiation.

CONCLUSION

The electronic signature arrangement for maintaining electronic medical records has legal legality or legitimacy, as demonstrated by regulations on electronic signatures in some regulations, including Constitution Number 11 of 2008 concerning Information and Electronic Transactions, Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Operator, and Minister of Communication and Information Regulation Number 11 of 2018 concerning Electronic System Organizer. Specifically, Minister of Health Regulation Number 24 of 2022 on Medical Records has also regulated the application of electronic signatures in the maintenance of electronic medical records where it legally indicates that using an electronic signature as an authentication has clear legality.

Generally, two types of electronic signatures are used in Indonesia: certified electronic signatures and uncertified digital signatures. They are different in the value of proof. The
certified electronic signatures have a higher proof value (precision) compared to the uncertified electronic signatures due to the certified signature using asymmetrical cryptography and blockchain techniques as a method of authenticating electronic medical records data, as well as the certificate signature has been issued by an agency recognized by the government in Indonesia. Although the uncertified electronic signatures have less proof value, their use is still valid for use in the maintenance of electronic medical records under Government Regulation No. 71 of 2019 concerning Electronic System Operators and Transactions.

ACKNOWLEDGMENT

The authors thank all parties who have helped during this research. In particular, the Postgraduate Study Program for the Master of Health Law at Udayana University has allowed us to conduct this research.

REFERENCES


