Volume 8 Nomor 2, July 2024: pg. 103-112.
Fakultas Hukum, Universitas Lampung,
Bandar Lampung, Lampung, Indonesia.
E-ISSN: 2598-3105 P-ISSN:2723-2581
http://jurnal.fh.unila.ac.id/index.php/cepalo

THE ETHICAL AND LEGAL ASPECTS OF HEALTH POLICY ON ELECTRONIC MEDICAL RECORDS IN INDONESIA

Ta Larasati[1], Ahmad Irzal Fardiansyah [2], Dwi Saketi[3], Azelia Nusa Dewiarti[4].

[1]Universitas Lampung, Indonesia, Email; ta.larasati@fk.unila.ac.id
[2]Universitas Lampung, Indonesia, Email; ahmad.irzal@fh.unila.ac.id
[3]Universitas Lampung, Indonesia, Email; dwijim@gmail.com
[4]Universitas Lampung, Indonesia, Email; azelia.nusadewiarti@fk.unila.ac.id

Submitted: August 12, 2024; Reviewed: September 18, 2024; Accepted: October 9, 2024
DOI: 10.25041/cepalo.v8no2.3634

Abstract

The government has addressed the development of electronic medical records (RME) through Minister of Health Regulation (Permenkes) No. 24 of 2022, ensuring their legality in healthcare facilities across Indonesia. The primary goal is to integrate all patient data, enabling the Ministry of Health to map the health status of Indonesian citizens, including information about various diseases. However, principles related to medical records, particularly confidentiality, must be observed to prevent violations and guarantee the privacy of patient data, reflecting healthcare professionals' ethical responsibilities. The use of electronic medical records raises concerns about potential data leaks, necessitating the establishment of security measures and identification of responsible parties in case of breaches. Research indicates that challenges remain in implementing RME across healthcare facilities, including limited internet access and the lack of preparedness among practitioners, clinics, health centers, and hospitals. Therefore, the Ministry of Health must undertake extensive outreach and training initiatives to address these issues and enhance internet connectivity throughout the country.

***Keywords**: Etich; Legal aspect; Implementation; Electronic; Medical Record*

A. Introduction

Medical records creation by healthcare providers within hospital settings is not yet efficient due to the absence of a universal regulation.[1] In response to evolving healthcare needs, a specific regulation regarding medical records was established in 2008, requiring the records to be written in comprehensive, and clear formats on paper or electronically. This regulatory framework has facilitated the adoption of electronic medical records in Indonesia.

In August 2022, the Minister of Health issued the Regulation No. 24 of 2022 concerning Medical Records to amend the prior health ministerial regulation aimed at enhancing the quality of health services provided to the community. Electronic medical records are positioned as a pivotal component in the transformation of healthcare services. From the perspective of patient care, these records are anticipated to enhance the accuracy of information, support clinical decision-making processes, and improve information accessibility, thereby ensuring continuity

[1] See J. Guwandi, *Trilogi Rahasia Kedokteran* (Jakarta: UI Press, 1992).

of care. The viability of electronic medical records is bolstered by advancements in information technology, which are increasingly embraced by healthcare professionals, clinics, and hospitals.

The advantages of comprehensive and clearly articulated electronic medical records for healthcare practitioners include serving as a foundational tool for disease planning and analysis. They also facilitate the planning of treatment, care, and medical interventions provided to patients, thereby enhancing the quality of services and protecting healthcare workers in their pursuit of optimal public healthcare outcomes. For patients, electronic medical records provide essential information regarding service cost calculations and insight into disease progression, treatment options, and medical interventions.

Consequently, the maintenance of accurate, complete, and confidential electronic medical records is crucial as they serve as vital information for patients. The absence or inaccuracy of such records can result in significant legal implications. From a juridical standpoint, electronic medical records constitute evidence of the therapeutic relationship between healthcare providers and patients, thus underscoring their necessity in both health service practices and legal frameworks.

Despite the potential benefits, the utilization of electronic medical records in Indonesia remains limited. A significant number of healthcare providers, including doctors, clinics, and hospitals, have yet to implement electronic systems. Challenges persist, primarily due to inadequate internet connectivity and the varying levels of proficiency among human resources.

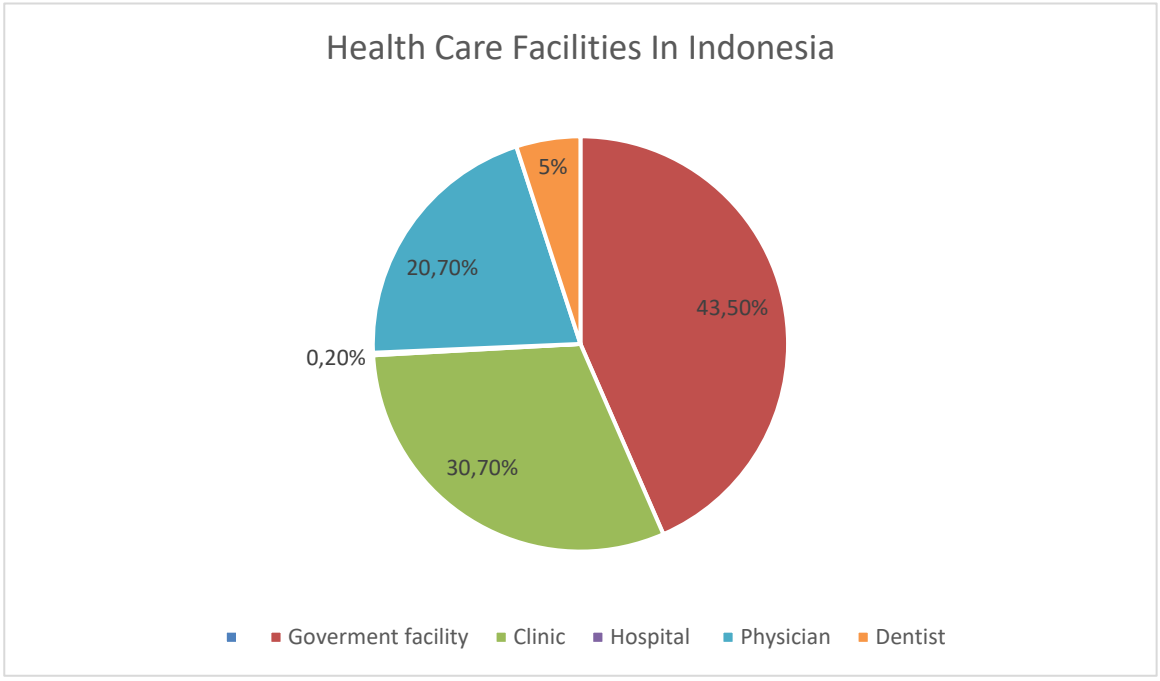

Figure 1 : Health care facilities in Indonesia, November 2022

As of November 2022, Indonesia has over 23,000 healthcare facilities. However, more than 11,000 of these facilities are concentrated in just five provinces on the island of Java, despite Indonesia having a total of 38 provinces. Additionally, over 12,000 healthcare facilities are located in a limited number of cities, with many situated in rural areas or smaller towns that lack reliable internet connectivity. Given this context, the implementation of an Electronic Medical Record (EMR) system across all healthcare facilities nationwide is likely to face significant challenges.

This situation raises several critical questions: What guarantees exist regarding medical confidentiality, integrity, and availability in the application of electronic medical records in Indonesia? What are the legal implications and benefits associated with the use of electronic medical records in the country?.

This research employs doctrinal qualitative methods to conduct an in-depth examination of various regulatory aspects related to electronic medical records and their implementation in Indonesia. As a contribution to the existing body of knowledge, this study aims to analyze potential outcomes of implementing electronic medical records across Indonesia and to provide recommendations to the government for mitigating potential adverse effects.

B. Discussion

1. Guarantee of Confidentiality, Integrity, and Availability of Electronic Medical Records in Indonesia

Article 46, Paragraph (1) of Law No. 29 of 2004 concerning Medical Practice defines medical records as files that include archives and documents pertaining to patient identities, examinations, treatments, actions, and other services provided to patients. Additionally, Regulation of the Minister of Health Number 24 of 2022 regarding Electronic Medical Records elaborates that medical records consist of files containing patient identities, examination results, previous treatments, and other actions and services rendered to patients, all of which are recorded using an electronic system designed for medical record management.

A fundamental aspect of the doctor-patient relationship is the ethical obligation to maintain the confidentiality of all patient information. This principle is enshrined in the Indonesian Medical Code of Ethics, which mandates that “every doctor is obliged to keep everything he knows about a patient confidential, even after the patient has passed away.” Consequently, all information obtained by a doctor from a patient must be adequately safeguarded.

This confidentiality is crucial as it protects sensitive patient information. A patient's medical record encompasses at least two critical components that must remain confidential: documentation regarding current and past health conditions, as well as information about past, present, and future treatments proposed by healthcare professionals.[2]

Based on these essential elements, medical information within a patient's medical record must include five key components:[3] details about the patient and healthcare providers, the patient's complaints, the duration of pain, the symptoms experienced, and the methods employed to receive medical treatment. Additionally, the record must reflect the outcomes or impacts of the medical actions and treatments administered to the patient. It is imperative that the data containing these elements be accurate and comprehensive, as omissions or inaccuracies could have severe repercussions for patient safety and well-being.[4]

The implementation of electronic medical records (EMRs) allows hospitals to exercise discretion in the form and method of data storage, focusing on three key criteria: confidentiality, visual readability, and data integrity. According to the Minister of Health Regulation Number 24 of 2022, the foundational principles governing EMRs encompass confidentiality, integrity, and availability, all of which must be maintained in a secure environment. The security of authenticity places the onus on third parties to ensure the accuracy of records, necessitating proactive measures to prevent the intentional or inadvertent entry of incorrect data, as well as the alteration, deletion, or misrepresentation of information. Furthermore, the principle of visual

[2] Clifford Goodman, “Savings in Electronic Medical Record Systems? Do It for the Quality,” *Health Affairs (Project Hope)* 24, no. 5 (2005), https://www.healthaffairs.org/doi/abs/10.1377/hlthaff.24.5.1124.

[3] John Ludwick D.A, Doucette, “Adopting Electronic Medical Records in Primary Care: Lessons Learned from Health Information Systems Implementation Experience in Seven Countries,” *International Journal of Medical Informatics* 78, no. 1 (2009): 22–31, https://doi.org/10.1016/j.ijmedinf.2008.06.005.

[4] Jacqueline Ross, “Electronic Medical Records: The Promises and Challenges,” *Journal of Perianesthesia Nursing* 24, no. 5 (2009): 327–29.

readability mandates that records must be easily legible to the naked eye and capable of being printed when required, while the security of property storage underscores the importance of data being recoverable at any time, thereby preserving its authenticity and legibility. Consequently, these principles highlight the critical need for robust protocols to ensure secure data storage and management.

2. Confidentiality

In medical practice, every doctor creates medical records right away and complete them after a patient receives care. This includes recording the results of examinations, treatments, and other services provided to the patient. Each entry must include the name, date, and signature of the doctor or healthcare worker who provided the service. If there is an error in the medical record, corrections can be made by crossing out the mistake without deleting the original notes, and the doctor or healthcare worker must initial the correction.[5]

The contents of medical records can be explained as needed for legal enforcement regarding medical and dental ethics. Information in medical records, such as a patient's identity, diagnosis, medical history, and examination results, may be disclosed to law enforcement officials if required by a court order.[6] According to the medical code of ethics, doctors must keep all information obtained from patients confidential.

The law requires every hospital to maintain medical records, and these records must be managed appropriately to meet international standards. The World Health Organization (WHO) states that patient medical records are confidential documents that hospitals must protect.[7] These regulations ensure the confidentiality of medical records and are being applied in Indonesia. Therefore, it is crucial to uphold the confidentiality of these records. If there is a misuse of records, violations can result in administrative penalties, including warnings, fines, or the loss of hospital licenses.

To address these needs, the government has taken steps to guarantee confidentiality. Every healthcare worker providing individual health services must create a patient's medical record immediately after treatment. Each patient's record must include the name, date, and signature or initials of the healthcare worker who provided the service. Additionally, healthcare workers and facility leaders are required to keep patient records confidential. These documents belong to the healthcare facility, and patients can request a summary of their medical records when needed.

Despite the linkage, the ownership of medical records is separated between the physical files and their contents. From a civil law perspective, medical records can be defined as documents, whether on paper or in electronic format, that contain meaningful information about a situation, event, or action.[8]

Recent developments have led to the introduction of new regulations by the government to facilitate the use of electronic medical records. These regulations were established based on three key considerations: the integration of health data systems, the development of health service application systems, and the creation of a health technology ecosystem. While these factors are essential for current healthcare needs, it is crucial to prioritize the principles of data confidentiality and security. To ensure the confidentiality of electronic medical records, healthcare facilities must protect the security, integrity, confidentiality, and availability of the

[5] Sudjana Sudjana, "Aspek Hukum Rekam Medis Atau Rekam Medis Elektronik Sebagai Alat Bukti Dalam Transaksi Teurapetik," *Veritas et Justitia* 3, no. 2 (2017): 359–83, https://doi.org/10.25123/vej.2685.

[6] Hanafiah Jusuf & Amir Amri, *Etika Kedokteran Dan Hukum Kesehatan* (Jakarta: Buku Kedokteran EGC, 1999).

[7] "Guidelines Medical Record Practice," *World Health Organisation*, 1980.

[8] Fransiska FH Novita Eleanora Univ MPU Tantular Jakarta Jl Cipinang Besar No and Jakarta Timur, "Analisis Yuridis Rekam Medis Sebagai Alat Bukti Surat," *Analisis Yuridis Rekam Medis Sebagai Alat Bukti Surat Forum Ilmiah* 10 (2013): 387.

data.[9] Digital storage solutions may include servers and certified cloud computing systems that comply with relevant laws and regulations, along with other certified technologies. The confidentiality of these medical records is further assured by health service facilities through digital storage media that require data backups.

However, the new regulations introduce certain factors that may threaten the confidentiality of electronic medical records. For instance, electronic medical records stored by healthcare facilities must connect and interoperate with an interoperability service platform that integrates health data managed by the Ministry of Health. According to another regulation, healthcare facilities are required to grant the Ministry of Health access to all contents of patients' electronic medical records. While this requirement is framed in the context of data collection and research, it raises concerns about confidentiality. Linking this information to specific agencies could create vulnerabilities, as it increases the risk of unauthorized access by hackers and the potential for unrestricted access by the agency itself.

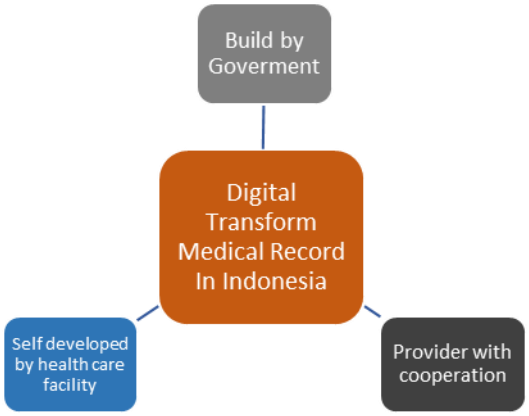

Figure 2. Digital transform of medical record in Indonesia

Christina Rosario highlighted that the primary issue in the implementation of electronic medical records is the security risk posed by criminal hackers.[10] Ben Walker emphasized that healthcare facilities and physician practices are legally obligated to implement security measures to safeguard patient information. For instance, access to patient data should be restricted to authorized individuals only. Most computer hardware and software programs come equipped with built-in security features to protect patient records from unauthorized access.[11]

This indicates that as more parties gain access to the contents of medical records, which should remain confidential, the risk of data misuse increases. Consequently, the Ministry of Health should not have access to the entirety of medical records, as this could lead to potential breaches of confidentiality due to the handling of larger volumes of sensitive documents. To uphold the confidentiality of medical records—an essential right of patients—it is crucial to categorize the information needs of the Ministry of Health. Even when data collection is conducted for research purposes, it must adhere to the requirements stipulated in the Medical Practice Act.

3. Integrity

[9]Regulation of the Minister of Health Number 24 of 2022 concerning Electronic Medical Records
[10] Christina Rosario, "4 Problems With Electronic Health Records," *Advance Data Systems Corporation*, 2019.
[11] Ben Walker, "Problems With Electronic Health Records," *Ditto*, 2021, https://www.dittotranscripts.com/blog/problems-with-electronic-health-records/.

Integrity ensures the accuracy and reliability of data and information in electronic medical records. Changes to this data may only be made by individuals with authorized access rights.[12] According to ISO 15489-1, the integrity of an archive pertains to its completeness and stability, meaning it should not be altered.[13] To uphold the integrity of health records, electronic systems must allow providers to make changes, track corrections, and clearly indicate when original entries have been modified.[14] It is essential to adhere to the principle of integrity when making changes; each alteration must be justified, with safeguards in place to maintain the integrity of electronic medical records.

The integrity issue is particularly significant when related to governmental authority, specifically the Ministry of Health, which can access medical records stored electronically on the server. Regulations impose restrictions on the possibility of changing data, stating that corrections are to be made only when errors occur in the input of administrative and clinical data. These corrections can only be performed by healthcare workers and administrative staff, including medical recorders, within a maximum timeframe of two days from the initial data input. If administrative errors are identified after this period, corrections can only proceed with the approval of the medical recorder and health information officer or the head of the healthcare facility. These regulations serve as a safeguard against potential discrepancies in medical record data.

Maintaining the integrity of electronic documentation is vital for preventing fraud, waste, misuse, and improper payments. Electronic systems must incorporate software capabilities designed to ensure integrity. Key aspects of this integrity principle include user authentication and access management or authorization. It also involves maintaining audit trails and resisting intrusions through mechanisms such as connection logs and encryption status, which record who made changes and when. Furthermore, optimal security settings should be established by default, preventing modification, overwriting, or deletion of events. The system should also be able to detect changes in the audit log and restrict access after a period of inactivity.[15]

4. Availability

Availability ensures that the data and information contained in electronic medical records can be accessed and utilized by individuals who have been granted access rights by the head of the healthcare facility.[16] Accessing data refers to the activities performed by internal staff at health service facilities to retrieve information related to electronic medical records for service or administrative purposes. The allocation of access rights is governed by the policies set by the head of the healthcare facility, taking into account the principles of data and information security.

Furthermore, availability means that information may become inaccessible if the system is hacked or overloaded. To ensure availability, electronic health record systems typically incorporate redundant components, often referred to as fault-tolerant systems.[17] ` This means

[12] Minister of health regulation number 24 of 2022 Article 29 paragraph (3)

[13] MIM Saleh, "Standards Organisation, Geneva. See Also in Salleh, Mohd, at All, Records Policy and Integrity Used in Electronic Medical Records: Evidence from the Malaysian Healthcare Industry," *Science Seires Data Report* 5, no. 9 (2013).

[14] "Integrity of the Healthcare Record: Best Practices for EHR Documentation," 2013, https://flbog.sip.ufl.edu/risk-rx-article/integrity-of-the-healthcare-record-best-practices-for-ehr-documentation/.

[15] Software Features, "Documentation Integrity in Electronic Health Records," 2011, 6–8.

[16] Minister of Health Regulation No. 24 of 2022 Article 29 paragraph (4)

[17] PMP Laurinda B. Harman, PhD, RHIA, Cathy A. Flite, MEd, RHIA, and Kesa Bond, MS, MA, RHIA, "Electronic Health Records: Privacy, Confidentiality, and Security," *AMA Journal of Ethics® Illuminating the Art of Medicine*, n.d., https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209.

that if one component fails or encounters issues, the system can seamlessly switch to a backup component. The principle of availability should be a central focus in the implementation of electronic medical records, as data availability is susceptible to hacking or corrupt storage files. To address this vulnerability, regulations mandate that healthcare facilities using digital storage media must have a data backup system in place.

There is a need for clarification regarding what constitutes data backup, particularly when healthcare facilities develop electronic medical records applications independently. The requirement for integration with the Ministry of Health's system implies that data backups must also be included in this process. This indicates that once all medical record applications are integrated with the Ministry of Health's system, individual healthcare facilities may not be required to perform automatic data backups. However, this has not been explicitly confirmed in the relevant health ministerial regulations.

5. Legality and Benefits of Electronic Medical Records

The issuance of the Minister of Health's regulation on electronic medical records solidifies the legal framework for their implementation. Health facilities that are considering or currently operating an electronic medical records system can be reassured, as this regulation provides a guarantee for its use. According to the World Health Organization (WHO), electronic medical records (EMRs), as well as automated health records, refer to automated systems based on document imaging that have been developed for medical practice and public health centers. General practitioners in many countries have widely adopted this method, which includes detailed information about patient identification, medications, prescriptions, and laboratory results. In many cases, all healthcare information is recorded by physicians during each patient visit.[18]

However, several challenges remain, particularly concerns about the potential leakage of medical records. In electronic medical records systems, access is not limited to doctors or health facilities; third-party providers may also have access. This raises important considerations for data protection, necessitating additional legal provisions regarding the entities authorized to create electronic medical record systems. Consequently, if there is an inappropriate leak of medical information, those responsible can be held legally accountable.

Medical records serve other legal functions as well, including data collection and research for law enforcement purposes. They can be utilized as evidence in criminal cases related to healthcare errors.[19] For instance, all or part of the medical information may be presented as evidence to support the defense of hospitals and healthcare workers, particularly physicians, in legal proceedings.

6. Medical Records as Legal Evidence

Medical records can be accessed under specific circumstances, such as for law enforcement purposes. In these cases, electronic medical records must meet several requirements:[20] they should not be written in pencil, contain no deletions or scribbles, and any corrections must be made contemporaneously and initialed. Additionally, records should be clear and legible, including the signature and name of the officer, along with the date and time of examinations and actions, as well as a medical action consent form.

Key elements essential for law enforcement efforts should be upheld, including authority to access medical record data, create and modify content, and maintain accurate timestamps.

[18] WHO, "Electronic Health Records: Manual for Developing Countries," *World Health Organisation* 15, no. 44 (2012): 64.

[19] Nabil Atta Samandari, Wila Chandrawila S, and Agus H. Rahim, "Kekuatan Pembuktian Rekam Medis Konvensional Dan Elektronik," *Soepra* 2, no. 2 (2017): 154, https://doi.org/10.24167/shk.v2i2.818.

[20] Tjen D.W, "Rekam Medis Alat Bukti Hukum," *Jurnal Ilmiah Kesehatan* 5, no. 3 (2013).

This information is crucial for tracing accountability in instances of discrepancies within medical records.

In Indonesia, medical records can serve as evidence as outlined in Article 1866 of the Civil Code and Article 184 of the Criminal Procedure Code. Article 1866 of the Civil Code states that evidence includes written documentation, witness testimony, suspicions, confessions, and oaths. Conversely, Article 184, Paragraph (1) of the Criminal Procedure Code defines legal evidence in criminal law to include witness and expert testimony, documents, instructions, and statements from the defendant. The Minister of Health's regulation also reinforces that police officers may request the use of electronic medical records in law enforcement.

According to Articles 5 and 6 of the Law on Information and Electronic Transactions, electronic medical records, electronic documents, and their printed results are considered legal evidence. Furthermore, electronic medical records and documents are deemed valid when created using an electronic system compliant with the provisions established in this law.

Article 6 of the Information and Electronic Transactions Law includes additional stipulations beyond those in Article 5, Paragraph (4), which require that medical records be in written or original form. Electronic medical records and documents are considered valid when their contents can be accessed, displayed, and guaranteed for integrity, accurately reflecting a given situation.[21] This should be taken into account by those managing electronic medical records to enhance their application in supporting law enforcement processes.

The existence of electronic medical records and other related documents is recognized as legal evidence, providing certainty for the operation of electronic systems and transactions. This recognition extends to their use in legal matters, particularly concerning evidence in legal actions conducted through electronic systems. The collection of electronic medical records and documents, including interception, wiretapping, and related recordings, must occur within the framework of law enforcement, involving police, prosecutors, and other legally authorized institutions. However, a significant challenge in the evidentiary process arises concerning expert testimony, as outlined in Article 186 of the Criminal Procedure Code.

Expert testimony may be provided during examinations by investigators or public prosecutors in the form of reports, adhering to the oath taken upon assuming their position. If this testimony is not provided, the investigator or public prosecutor must still furnish information, which is recorded in the official examination report. This testimony is offered only after the expert has taken an oath or made a promise before the court to speak truthfully. It is important to distinguish this oath from the oath of office taken upon accepting the position.

In the context of the relationship between a doctor or dentist and a patient, the expert testimony referenced in Article 186 of the Criminal Procedure Code can be presented in both written and unwritten forms. Written expert testimony may include electronic medical records. The legal function of electronic medical records is twofold: they serve as evidence in disputes or claims from patients and provide legal protection for healthcare professionals. These records also contain informed consent for medical procedures, as no actions can proceed without the patient's consent. When these multifunctional medical records are connected to Article 184 of the Criminal Procedure Code, they function as both written evidence and expert testimony.[22]

The contents of medical records can only be disclosed by the doctor or dentist who treated the patient, and only with the patient's written consent. However, the head of the health service facility can explain the contents of electronic medical records in writing or in person to the

[21] Kimberly D. Schenarts PhD MD, Paul J. Schenarts, "Educational Impact of the Electronic Medical Record," *Journal of Surgical Education* 69, no. 1 (2012): 105–12, https://doi.org/https://doi.org/10.1016/j.jsurg.2011.10.008.

[22] Hatta Gemala, "Rancangan Rekam Kesehatan Elektronik" (Jakarta: Sub. Dit. Keterapian Fisik Direktorat Keperawatan dan Keteknisan Medik Direktur Jenderal Pelayanan Medik Departemen Kesehatan RI, n.d.).

applicant without requiring the patient's permission. In cases involving a court order, doctors, dentists responsible for patient care, or hospital leadership may provide photocopies of medical records, along with a conclusion reflecting their professional opinion.[23]

This indicates that judges can utilize medical records as evidence in court, but their use is not binding and ultimately depends on the judge's discretion. Thus, medical records can serve as proof of potential errors or negligence by a doctor or dentist in their professional duties. Therefore, electronic medical records are valuable for defending healthcare professionals against lawsuits and claims made against them.

C. Conclusion

With the implementation of regulations regarding electronic medical records, all health facilities in Indonesia are required to utilize electronic medical records accurately and responsibly in therapeutic transactions, adhering to the principles of confidentiality, integrity, and availability. Maintaining these things is a code of ethics for health workers. The absence of electronic medical records in health facilities can lead to the imposition of administrative sanctions. In maintaining the principle of confidentiality, electronic medical records should be owned by health facilities and patients. Current regulations also grant the Ministry of Health the right to access electronically created medical records. The government must exercise caution when handling patient medical record data, establishing specific criteria for individuals granted access to these records. Additionally, it is essential to carefully select providers permitted to collaborate with healthcare facilities in developing electronic medical record applications to prevent violations of confidentiality. In therapeutic transactions, electronic medical records serve as both written evidence (submitted outside of court) and expert testimony (presented during court hearings). However, for law enforcement purposes, the evidential weight of these records is not absolute, as judges retain the discretion to assess their validity.

REFERENCES

A. Book

Hanafiah Jusuf & Amir Amri. *Etika Kedokteran Dan Hukum Kesehatan*. Jakarta: Buku Kedokteran EGC, 1999.

Hatta Gemala. “Rancangan Rekam Kesehatan Elektronik.” Jakarta: Sub. Dit. Keterapian Fisik Direktorat Keperawatan dan Keteknisan Medik Direktur Jenderal Pelayanan Medik Departemen Kesehatan RI, n.d.

See J. Guwandi. *Trilogi Rahasia Kedokteran*. Jakarta: UI Press, 1992.

B. Journal

Christina Rosario. “4 Problems With Electronic Health Records.” *Advance Data Systems Corporation*, 2019.

Clifford Goodman. “Savings in Electronic Medical Record Systems? Do It for the Quality.” *Health Affairs (Project Hope)* 24, no. 5 (2005). https://www.healthaffairs.org/doi/abs/10.1377/hlthaff.24.5.1124.

Features, Software. “Documentation Integrity in Electronic Health Records,” 2011, 6–8.

“Integrity of the Healthcare Record: Best Practices for EHR Documentation.” 2013. https://flbog.sip.ufl.edu/risk-rx-article/integrity-of-the-healthcare-record-best-practices-for-ehr-documentation/.

[23] *ibid*

Jacqueline Ross. "Electronic Medical Records: The Promises and Challenges." *Journal of Perianesthesia Nursing* 24, no. 5 (2009): 327–29.

Laurinda B. Harman, PhD, RHIA, Cathy A. Flite, MEd, RHIA, and Kesa Bond, MS, MA, RHIA, PMP. "Electronic Health Records: Privacy, Confidentiality, and Security." *AMA Journal of Ethics® Illuminating the Art of Medicine*, n.d. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209.

Ludwick D.A, Doucette, John. "Adopting Electronic Medical Records in Primary Care: Lessons Learned from Health Information Systems Implementation Experience in Seven Countries." *International Journal of Medical Informatics* 78, no. 1 (2009): 22–31. https://doi.org/10.1016/j.ijmedinf.2008.06.005.

MD, Paul J. Schenarts, Kimberly D. Schenarts PhD. "Educational Impact of the Electronic Medical Record." *Journal of Surgical Education* 69, no. 1 (2012): 105–12. https://doi.org/https://doi.org/10.1016/j.jsurg.2011.10.008.

MIM Saleh. "Standards Organisation, Geneva. See Also in Salleh, Mohd, at All, Records Policy and Integrity Used in Electronic Medical Records: Evidence from the Malaysian Healthcare Industry." *Science Seires Data Report* 5, no. 9 (2013).

Novita Eleanora Univ MPU Tantular Jakarta Jl Cipinang Besar No, Fransiska FH, and Jakarta Timur. "Analisis Yuridis Rekam Medis Sebagai Alat Bukti Surat." *Analisis Yuridis Rekam Medis Sebagai Alat Bukti Surat Forum Ilmiah* 10 (2013): 387.

Samandari, Nabil Atta, Wila Chandrawila S, and Agus H. Rahim. "Kekuatan Pembuktian Rekam Medis Konvensional Dan Elektronik." *Soepra* 2, no. 2 (2017): 154. https://doi.org/10.24167/shk.v2i2.818.

Sudjana, Sudjana. "Aspek Hukum Rekam Medis Atau Rekam Medis Elektronik Sebagai Alat Bukti Dalam Transaksi Teurapetik." *Veritas et Justitia* 3, no. 2 (2017): 359–83. https://doi.org/10.25123/vej.2685.

Tjen D.W. "Rekam Medis Alat Bukti Hukum." *Jurnal Ilmiah Kesehatan* 5, no. 3 (2013).

Walker, Ben. "Problems With Electronic Health Records." *Ditto*, 2021. https://www.dittotranscripts.com/blog/problems-with-electronic-health-records/.

WHO. "Electronic Health Records: Manual for Developing Countries." *World Health Organisation* 15, no. 44 (2012): 64.

World Health Organisation. "Guidelines Medical Record Practice." 1980.