ORIGINAL ARTICLE

Jurnal Dharmaputra Hukum Kesehatan (*JDHK*) 2026, Volume 2, Number 1: 7-14
E-ISSN: 3124-1840 ; P-ISSN: 3124-1964

Electronic medical records as legal evidence in Indonesian healthcare disputes: A review of authentication, confidentiality, and evidentiary challenges

Gede Krisna Udiana[1*], Ida Bagus Ngurah Tri Pramana[2], Ida Ayu Putu widya Indah Sari[3]

[1]Legal Unit, Wangaya Regional Hospital, Denpasar, Indonesia
[2]Media Content Department, Radio of The Republic of Indonesia, Denpasar, Indonesia
[3]News Program 1, Radio of the Republic of Indonesia

*Corresponding author:
Gede Krisna Udiana. Legal Unit, Wangaya Regional Hospital, Denpasar, Indonesia;
udiana.krisna@gmail.com

Received: 2026-02-19
Accepted: 2026-04-15
Published: 2026-05-22

ABSTRACT

Introduction: The nationwide implementation of electronic medical records in Indonesia has transformed clinical documentation into a digital legal artifact. Although electronic medical records improve continuity of care and administrative efficiency, their use as legal evidence in healthcare disputes raises complex questions regarding authenticity, confidentiality, integrity, and evidentiary reliability. This review aims to analyze the legal position of electronic medical records as evidence in Indonesian healthcare disputes, with particular attention to authentication, confidentiality, audit trails, chain of custody, and practical evidentiary barriers.

Methods: A normative-juridical narrative review was conducted by synthesizing Indonesian health law, electronic information law, personal data protection law, procedural law, and scholarly literature on electronic health records, digital evidence, cybersecurity, and health data governance.

Results: Electronic medical records have a legal basis as electronic documents and may support civil, criminal, administrative, ethical, disciplinary, and insurance-related proceedings. Their probative value depends on reliable electronic systems, user-specific authentication, certified electronic signatures, immutable audit trails, accurate timestamps, metadata preservation, confidentiality safeguards, and controlled extraction procedures. Current Indonesian regulation provides a strong normative basis, but operational gaps remain in system certification, shared-account prevention, forensic readiness, interoperability, and medico-legal disclosure protocols.

Conclusion: Electronic medical records can function as important legal evidence in Indonesian healthcare disputes. Their evidentiary strength requires integrated governance that combines legal compliance, clinical documentation discipline, technical security, and ethical protection of patient confidentiality.

Keywords: electronic medical records, legal evidence, authentication, confidentiality, healthcare disputes, Indonesia.
Cite This Article: Udiana, G.K., Pramana, I.B.N.T. 2026., Sari, I.A.P.W.I. Electronic medical records as legal evidence in Indonesian healthcare disputes: A review of authentication, confidentiality, and evidentiary challenges. *Jurnal Dharmaputra Hukum Kesehatan.* 2(1): 7-14

INTRODUCTION

Indonesia's healthcare system is moving from paper-based clinical documentation toward an integrated digital health information ecosystem. This shift is not merely administrative; it changes how clinical information is created, stored, exchanged, audited, and produced as legal evidence. Minister of Health Regulation No. 24 of 2022 positions electronic medical records (EMR) as the standard method for medical record management in healthcare facilities, including hospitals, primary health centers, clinics, independent medical practices, pharmacies, health laboratories, and other regulated healthcare facilities. The same regulation emphasizes the need for electronic systems that ensure the security, confidentiality, integrity, and availability of medical record data.[1]

In healthcare practice, medical records serve functions that extend far beyond clinical note-taking. They support continuity of care, quality evaluation, reimbursement claims, internal audit, health reporting, education, research, and ethical and legal accountability. In healthcare disputes, medical records frequently become the primary documents for assessing whether diagnosis, informed consent, medical procedures, monitoring, risk communication, referral, and follow-up were performed in accordance with professional standards and standard operating procedures. Therefore, the quality of medical record documentation may strengthen or weaken the legal position of patients, physicians, healthcare workers, and healthcare institutions.[2,3]

The transition from paper medical records to EMR changes the evidentiary character of medical documentation. In conventional records, authentication is often assessed through wet signatures, initials, institutional stamps, visible corrections, or the physical existence of the document. In EMR, the evidentiary object includes not only the clinical content displayed on the screen or printed on paper, but also metadata, user logs, timestamps,

audit trails, access controls, electronic signature status, and data modification history. These digital dimensions can improve evidentiary precision when the system is properly governed. Conversely, systems without audit trails, systems that permit shared accounts, systems that fail to record data changes, or systems that cannot preserve metadata may reduce the probative value of EMR even when the electronic document can formally be printed.[4,5]

The position of EMR as legal evidence in Indonesia must be read through the interaction of several legal regimes. Health law governs documentation duties, confidentiality, patient rights, and the responsibility of healthcare facilities. Electronic information and transaction law recognizes electronic information, electronic documents, and their printed outputs as valid legal evidence when they meet procedural requirements and standards for electronic system operation.[6,7] Personal data protection law classifies health data and health information as specific personal data, meaning that processing, disclosure, storage, and transfer must comply with the principles of legality, transparency, legitimate purpose, security, and accountability.[8]

The main problem arises when evidentiary needs intersect with the duty to preserve medical confidentiality and protect patient data. Courts, investigators, disciplinary assemblies, reimbursement auditors, and legal representatives may require access to EMR to reconstruct the chronology of care. However, excessively broad disclosure of medical information may violate patient confidentiality, particularly when disclosed information is unrelated to the dispute. This situation requires lawful, limited, proportionate, and documented disclosure procedures.

This review analyses the position of EMR as legal evidence in Indonesian healthcare disputes. The discussion focuses on the positive legal framework, the concept of EMR as electronic evidence, authentication challenges, confidentiality and data protection issues, practical evidentiary barriers, comparative perspectives, and governance recommendations for healthcare facilities and legal stakeholders.

METHODS

Search Strategy

This article used a normative-juridical narrative review design. The normative-juridical approach was used to examine legal norms, principles, and relationships between regulations governing EMR implementation, electronic evidence, medical confidentiality, personal data protection, and healthcare dispute resolution. The narrative approach was used to synthesize scientific literature and technical documents concerning health information security, audit trails, digital authentication, chain of custody, and health data governance.

Primary legal materials included Minister of Health Regulation No. 24 of 2022 on Medical Records, Law No. 17 of 2023 on Health, Government Regulation No. 28 of 2024 as the implementing regulation of the Health Law, Law No. 27 of 2022 on Personal Data Protection, the Electronic Information and Transactions Law and its amendments up to Law No. 1 of 2024, Government Regulation No. 71 of 2019 on Electronic System and Transaction Operation, and relevant procedural law instruments.[1,6–11]

Secondary sources were obtained from journal articles, books, institutional reports, technical guidelines, and international documents relevant to EMR, digital evidence, healthcare cybersecurity, data protection, and health data governance. Searches were conducted through official government regulation portals, PubMed, Google Scholar, GARUDA, SINTA, and international institutional sources. Search terms included electronic medical records, electronic health records, legal evidence, digital evidence, authentication, audit trail, chain of custody, confidentiality, data protection, cybersecurity in healthcare, rekam medis elektronik, alat bukti elektronik, sengketa medis, tanda tangan elektronik, pelindungan data pribadi, and kerahasiaan medis.

Eligibility Criteria

Included materials consisted of current and relevant Indonesian regulations, academic articles discussing EMR and electronic evidence, literature on electronic health record security and privacy, and health data governance documents. Excluded materials were popular sources without a clear legal basis, unsupported opinions, revoked regulations, except where used for historical context, and articles without a direct relationship to EMR or healthcare dispute evidence.

Data Extraction and Synthesis

Data were extracted by identifying the legal basis, evidentiary function, authentication requirements, confidentiality duties, implementation barriers, and governance implications of EMR. The synthesis was performed thematically by grouping findings into legal validity, authentication, confidentiality, probative value, implementation challenges, and governance recommendations. Legal provisions were interpreted alongside technical and institutional literature to identify the gap between formal recognition of EMR as evidence and its practical reliability in dispute resolution.

RESULTS AND DISCUSSION

Conceptual Framework of Electronic Medical Records

EMR is a health information system that stores records of patient care in electronic format. Functionally, EMR is not identical to scanned paper documents. It covers the creation of data, entry of clinical information, storage, processing, display, exchange, correction, audit, retention, and destruction of data through an electronic system. Its core elements include patient identity, history taking, physical examination, diagnosis, therapy, procedures, laboratory results, radiology results, prescriptions, integrated progress notes, informed consent, discharge summaries, referral data, metadata, and access history.[1,6–12]

EMR has a dynamic character. Information may be created by different professional groups at different times and may be connected to registration, pharmacy, laboratory, radiology, inpatient, outpatient, reimbursement, telemedicine, and national interoperability modules. This dynamic structure provides a more comprehensive clinical chronology, but it also produces new evidentiary questions. The legal assessment of EMR depends not

only on the visible content, but also on the reliability of the system that records and preserves the data.[12,13]

From the perspective of evidentiary law, the information displayed on a screen or printed on paper is not the only important component. Metadata and audit trails may show who accessed the data, when the data were entered, what changes were made, whether previous entries were preserved, and whether corrections were performed in a traceable manner. These elements are crucial because healthcare disputes often concern chronology, attribution, and consistency between clinical action and documentation.[4,5,14,15]

Table 1. Evidentiary characteristics of conventional medical records and electronic medical records[1,6–12]

Aspect	Conventional medical records	Electronic medical records
Medium	Physical paper files.	Electronic data is stored on local servers, cloud platforms, or hybrid systems.
Authentication	Wet signatures, initials, institutional stamps, and handwriting identity.	User ID, electronic signatures, electronic certificates, timestamps, and metadata.
Correction	Cross-out corrections with initials and dates, provided that the original entry remains visible.	Versioning and audit trails that preserve values before and after modification.
Traceability	Dependent on loan books or manual tracking records.	Can be recorded automatically through access logs and system activity logs.
Risk	Loss, physical damage, fire, illegibility, or misfiling.	Digital manipulation, unauthorized access, metadata loss, downtime, and cyberattacks.
Evidentiary strength	Determined by physical integrity, signatures, and consistency of content.	Determined by system reliability, authentication, audit trails, data integrity, and chain of custody.

Indonesian Legal Framework for Electronic Medical Records

The legal framework for EMR in Indonesia is formed by the intersection of health law, electronic information law, personal data protection law, and procedural law. Minister of Health Regulation No. 24 of 2022 is the principal technical regulation governing medical record management. It requires healthcare facilities to implement EMR, regulates record keeping, confidentiality, security, storage, transfer, and utilization, and establishes minimum retention requirements. This regulation is the operational starting point for recognizing EMR as the standard form of healthcare documentation.[1]

Law No. 17 of 2023 on Health and Government Regulation No. 28 of 2024 strengthen the broader governance of health information systems. These instruments situate health data and service documentation within the institutional obligations of healthcare facilities, while also reinforcing patient rights and the duties of healthcare providers. In the digital context, these provisions support the view that EMR is not merely an internal administrative product but part of the accountability infrastructure of healthcare delivery.[9,10]

The Electronic Information and Transactions Law, as amended up to Law No. 1 of 2024, provides the general legal basis for recognizing electronic information, electronic documents, and their printed outputs as valid legal evidence. Government Regulation No. 71 of 2019 further governs the operation of electronic systems and transactions, including requirements for reliability, security, responsibility, and system accountability. These provisions are essential for evaluating whether an EMR system can produce reliable electronic documents in legal proceedings.[6,7]

Law No. 27 of 2022 on Personal Data Protection adds a distinct layer of protection by classifying health data and health information as specific personal data. As a result, EMR processing and disclosure must observe lawful basis, purpose limitation, security, transparency, and accountability. The legal function of EMR as evidence must therefore be balanced against the patient's right to privacy and the duty of medical confidentiality.[8]

Electronic Medical Records as Legal Evidence in Healthcare Disputes

EMR may be relevant in civil, criminal, administrative, ethical, disciplinary, and reimbursement-related proceedings. In civil malpractice claims, EMR can help demonstrate the existence of a therapeutic relationship, the chronology of care, compliance with professional standards, informed consent, and the causal relationship between alleged negligence and harm. In criminal cases, EMR may support the reconstruction of events and assist in assessing whether conduct amounted to negligence, gross deviation from standards, or intentional wrongdoing. In disciplinary proceedings, EMR is central to evaluating whether medical or healthcare personnel complied with professional standards, service standards, and standard operating procedures.[2,3]

The evidentiary position of EMR should be distinguished between admissibility and probative value. Admissibility concerns whether the relevant forum may accept the evidence. Probative value concerns the persuasive strength of that evidence in proving a disputed fact. EMR may be admissible as an electronic document, but its probative value may be weak if the system cannot establish authenticity, attribution, chronology, integrity, and completeness. Conversely, EMR supported by reliable audit trails, certified electronic signatures, preserved metadata, and documented extraction procedures may carry substantial probative weight.[2,3,5]

In practice, EMR has the potential to serve both patients and healthcare providers. For patients, a complete EMR may help prove delayed diagnosis, lack of informed consent, medication error, inadequate monitoring, or failure to refer.

Table 2. Indonesian legal framework relevant to electronic medical records[9,10]

Regulation	Scope	Relevance to EMR	Evidentiary implication
Minister of Health Regulation No. 24/2022	Medical record management.	Requires and regulates EMR, security, confidentiality, retention, and utilization.	Defines minimum standards for clinical documentation and retention of clinical evidence.
Law No. 17/2023 and Government Regulation No. 28/2024	Health and health information systems.	Places health data and care documentation within healthcare facility governance.	Strengthens institutional duties and patient rights.
Electronic Information and Transactions Law jo. Law No. 1/2024	Electronic information, electronic documents, electronic transactions, and electronic certification.	Recognizes electronic documents and printed outputs as legal evidence.	Provides the basis for the admissibility of EMR as electronic evidence.
Government Regulation No. 71/2019	Electronic system and transaction operation.	Regulates reliability, security, and accountability of electronic systems.	Serves as a technical-legal parameter for assessing EMR system reliability.
Law No. 27/2022	Personal data protection.	Classifies health data as specific personal data.	Limits and regulates EMR disclosure for legal purposes.
Procedural law	Rules of evidence in judicial forums.	Determines the form, relevance, and assessment of evidence.	Determines how EMR is admitted and evaluated in disputes.

For physicians and hospitals, a complete EMR may demonstrate compliance with standard operating procedures, adequate risk communication, proper monitoring, and timely clinical response. Therefore, EMR is not inherently pro-plaintiff or pro-provider; its legal effect depends on the quality and integrity of the documentation.[2,3]

EMR also has specific importance in administrative and reimbursement disputes. In the context of national health insurance and hospital claims, EMR may be used to verify diagnosis coding, procedures, length of stay, medication, and service eligibility. Poorly maintained EMR may expose facilities to allegations of upcoding, phantom billing, or inappropriate claims, while reliable EMR may support billing accountability and fraud prevention.[1,16]

Authentication and Integrity Challenges

Authentication is the central requirement for making EMR legally persuasive. It answers whether the record is what it purports to be and whether the person attributed to the entry actually created, modified, or approved it. Authentication in EMR depends on user-specific accounts, access rights, electronic signatures, timestamps, metadata, audit logs, and system security architecture. When these components are weak, the opposing party may challenge the authenticity or integrity of the record.[4,5,14,15]

The use of shared accounts represents one of the most serious authentication risks. If several physicians, nurses, or administrative staff use the same login credentials, the system cannot reliably identify who created or modified a clinical entry. This undermines attribution and weakens the non-repudiation function of the record. It also creates personal data protection risks because unauthorized access becomes difficult to trace. For this reason, healthcare facilities should prohibit password sharing, implement individual user IDs, enforce automatic logout, and apply role-based access control.[4,5]

Audit trail reliability is equally important. A robust audit trail should record the user, date, time, location or device where relevant, type of activity, data before modification, and data after modification. Corrections must not erase earlier entries. Instead, the system should preserve historical versions so that investigators, auditors, or courts can distinguish contemporaneous documentation from retrospective correction. In disputes, this distinction may determine whether a record is viewed as routine documentation or post-event reconstruction.[15]

Timestamp integrity is essential because healthcare disputes often depend on precise chronology. The timing of assessment, medication administration, referral, monitoring, resuscitation, informed consent, and operative decisions may be central to liability analysis. If server time can be altered without a trace, or if time synchronization is poor, the EMR chronology may be challenged. Technical safeguards should include restricted administrator privileges, synchronized server time, logging of time-setting changes, and periodic system audits.[4,15]

Certified electronic signatures can improve document authenticity, particularly for informed consent, discharge summaries, medical certificates, operative notes, and other documents with legal consequences. However, electronic signature implementation must be integrated into the clinical workflow rather than treated as a decorative image attached to a document. A scanned signature or pasted image does not provide the same non-repudiation value as a certificate-based electronic signature linked to the identity of the signer and the integrity of the document.[6,7]

Another major issue is the chain of custody. When EMR is extracted for investigation, litigation, audit, or disciplinary proceedings, the facility must be able to show how the data were identified, collected, exported, preserved, transferred, and submitted. Screenshots, informal PDF exports, or photographs of computer screens are vulnerable to authenticity challenges because they may omit metadata and can be easily edited. A legally safer approach requires authorized extraction, preservation of metadata,

Table 3. Authentication risks and minimum mitigation measures for electronic medical records[4,5,14,15]

Risk	Legal impact	Minimum mitigation	Priority
Shared accounts	Unclear attribution of clinical entries.	Individual user IDs, password-sharing prohibition, and automatic logout.	Very high
Absence of detailed audit trails	Data modification becomes difficult to prove.	Access logs and change logs with pre-image and post-image preservation.	Very high
Editable timestamps	Chronology of care can be disputed.	Server time synchronization and restriction of administrator privileges.	High
Uncertified electronic signatures	Weak non-repudiation for important documents.	Certified electronic signatures for consent forms, discharge summaries, and medical certificates.	High
Evidence export without metadata	The authenticity of printouts or PDF files can be challenged.	Extraction protocol, hash verification, official minutes, and metadata preservation.	Very high
Downtime without standard procedure	Continuity of documentation becomes incomplete.	Downtime forms, reconciliation, and verified scanning or transcription.	Moderate-high

hash verification where feasible, official documentation of the process, secure transfer, and retention of the source record.[5,14,15]

Confidentiality and Personal Data Protection Issues

The evidentiary use of EMR must be balanced with the obligation to protect patient confidentiality. Medical records contain information about diagnosis, treatment, reproductive health, mental health, infectious disease status, genetic data, medication history, and other sensitive information. Under the Indonesian Personal Data Protection Law, health data and health information are classified as specific personal data, requiring stronger safeguards than ordinary personal data.[8]

Healthcare facilities function as personal data controllers or processors, depending on the context of data processing. They are responsible for ensuring a lawful basis, purpose limitation, access restriction, data security, accountability, and prevention of unauthorized disclosure. This responsibility extends to internal access by staff, sharing with referral facilities, transmission to national platforms, use for insurance claims, research, audit, and disclosure for legal proceedings.[8,16]

The duty of medical confidentiality is not absolute. Disclosure may be permitted or required for lawful purposes such as court orders, criminal investigations, professional disciplinary review, public health obligations, patient safety, reimbursement audit, or the patient's own request. However, disclosure must remain limited to the purpose for which access is granted. Over-disclosure of irrelevant medical history may violate patient rights even when disclosure of the disputed episode is lawful.[8,9]

In medico-legal disclosure, healthcare facilities should apply principles of legality, necessity, proportionality, and accountability. Legality means that disclosure must have a valid legal basis. Necessity means that the data disclosed must be needed for the stated legal purpose. Proportionality means that disclosure should be limited to relevant information. Accountability means that the facility must document who requested the data, what data were disclosed, who authorized the disclosure, how the data were transmitted, and what safeguards were applied.[8,17]

Patient access to EMR also requires careful governance. Patients have legitimate interests in obtaining information about their own health, especially when they suspect harm or wish to seek a second opinion. A defensive institutional posture that obstructs patient access may generate additional legal risk. At the same time, facilities must ensure that the released record is accurate, complete within the requested scope, and protected from disclosure of third-party information or unrelated sensitive data.[1,8]

Practical Evidentiary Challenges in Healthcare Disputes

The first practical challenge is incomplete documentation. In a dispute, an act that was clinically performed but not documented may be difficult to prove. Conversely, a record that appears formally complete may still be questioned if it relies heavily on templates, automatic population, or copied entries. The legal problem is not only whether a note exists, but whether the note accurately represents the clinical reasoning and action taken at the relevant time.[2,3]

Delayed charting is another recurrent problem. Busy clinical environments may lead physicians and nurses to enter notes at the end of a shift or after several patients have been treated. Delayed entry is not automatically unlawful, but it should be transparent. EMR should distinguish the time of the clinical event from the time of documentation. If this distinction is absent, the record may produce an inaccurate chronology and become vulnerable to challenge.[5,15]

Copy-paste and auto-populate functions create a particular evidentiary risk. These features may improve efficiency, but they can also create cloned notes that do not reflect the patient's changing condition. In malpractice disputes, repetitive notes with identical findings across multiple days may be interpreted as evidence of inadequate assessment. Healthcare facilities should regulate template use, require verification of copied content, and discourage copying without clinical review.[5,14]

Downtime management is equally important. Electronic systems may fail due

to network problems, server interruptions, cyber incidents, maintenance, or power disruption. During downtime, facilities may use temporary paper forms or offline modules. These records must later be reconciled with the EMR in a traceable manner. Without a downtime standard operating procedure, the continuity and completeness of the record may be questioned.[5,15]

Interoperability remains a major implementation challenge. EMR data may be distributed across hospital information systems, laboratory systems, radiology information systems, pharmacy modules, reimbursement systems, and national platforms such as SATUSEHAT. Dispute reconstruction may require data from multiple modules. If systems are poorly integrated, records may be fragmented, inconsistent, or difficult to export in a legally reliable form.[16]

Cybersecurity also affects evidentiary credibility. Data breaches, ransomware, unauthorized access, and system manipulation can compromise confidentiality and integrity. Even when a particular dispute does not arise from a cyber incident, weak cybersecurity can undermine institutional claims that the record is reliable. Therefore, EMR governance requires not only legal compliance but also information security management, access monitoring, incident response, backup, and disaster recovery planning.[5,13,14,18]

Comparative Perspective

International experience shows that EMR governance depends on the integration of privacy, security, accountability, and evidentiary reliability. The Health Insurance Portability and Accountability Act (HIPAA) in the United States focuses on protected health information within covered entities and their business associates, with administrative, physical, and technical safeguards. The European General Data Protection Regulation (GDPR) regulates personal data more broadly. It treats health data as a special category requiring strict lawful processing, accountability, minimization, and data protection by design. These frameworks are not directly applicable in Indonesia, but they provide useful benchmarks for strengthening EMR governance.[18,19]

Table 4. Comparative perspective on health data and electronic medical record governance

Aspect	HIPAA	GDPR	Indonesia
Protected object	Protected Health Information held by covered entities and business associates.	Personal data, including health data as a special category.	General personal data and specific personal data, including health data and health information.
Main focus	Privacy and security of health information in treatment, payment, and healthcare operations.	Data subject rights, lawful basis, minimization, accountability, and cross-border transfer.	A combination of personal data protection, health law, and electronic system operation.
Implication for EMR	Administrative, physical, and technical safeguards.	Data protection by design, lawful processing, and transfer control.	Mandatory EMR, confidentiality, electronic system reliability, and electronic evidence basis.
Implementation challenge	Compliance audits and breach reporting.	Cross-organizational compliance and documentation of processing basis.	System certification, audit trails, interoperability, and digital forensic readiness.

Indonesia's model combines elements of health-sector regulation, general personal data protection, and electronic system governance. This combination is appropriate for a digital health ecosystem that connects healthcare facilities, national platforms, reimbursement systems, and legal forums. However, the Indonesian framework still requires more operational standards for audit trails, electronic signatures, forensic extraction, system certification, and disclosure protocols. Comparative analysis suggests that enforceable technical safeguards and institutional accountability must accompany formal legal recognition.[6–8,17,19,20]

Practical Implications and Policy Directions

For hospitals and clinics, EMR implementation should be treated as legal and clinical risk management rather than as a mere information technology project. Institutional leaders must allocate resources for secure infrastructure, backup, disaster recovery, access control, audit trail monitoring, staff training, and legal disclosure procedures. Medical record units, information technology teams, legal units, and clinical governance committees should work together rather than operate separately.[1,13,18]

For physicians, nurses, and other healthcare workers, EMR changes the meaning of documentation discipline. Entries must be contemporaneous, complete, accurate, and attributable to the correct individual. Healthcare workers should avoid shared accounts, retrospective editing without explanation, unverified copy-paste entries, and informal communication that is not integrated into the official record when clinically relevant. Good documentation is both a patient safety measure and a legal safeguard.[2,5,15]

For EMR vendors and developers, legal readiness should be embedded into system design. Systems should include granular audit logging, role-based access control, tamper-evident logs, secure electronic signatures, metadata preservation, version control, export functions for medico-legal purposes, and downtime modules. Vendor contracts should clarify data ownership, access rights, security obligations, incident response duties, and support for legal evidence extraction.[4,5,13–15]

For regulators, more detailed technical standards are needed. These standards should specify minimum audit trail requirements, prohibited practices such as hard deletion of clinical entries, mandatory use of certified electronic signatures for selected documents, secure retention periods, interoperability standards, system certification, and protocols for producing EMR as legal evidence. Without such standards, implementation will vary

widely, and legal certainty will remain uneven.[1,6,7]

For courts, investigators, advocates, and disciplinary bodies, digital literacy is increasingly important. Legal actors should understand that printed EMR is not always equivalent to the original electronic record. Assessment of EMR should consider the reliability of the system, the existence of metadata, audit trail integrity, extraction method, chain of custody, and the possibility of tampering or incomplete disclosure. Expert assistance in health informatics or digital forensics may be necessary in complex disputes.[2,4,5,14,15]

Policy reform should prioritize four areas. First, harmonization between health law, personal data protection law, electronic evidence law, and procedural law should be strengthened. Second, a national technical standard for EMR evidentiary readiness should be issued. Third, healthcare facilities should be required to develop written protocols for medico-legal extraction and disclosure. Fourth, education on legal documentation, confidentiality, and cybersecurity should be incorporated into medical, nursing, health information management, and hospital administration training.[1,6–10,17]

CONCLUSION

Electronic medical records now occupy a central position in Indonesian healthcare governance and medico-legal accountability. They are no longer merely administrative documents but electronic clinical records with potential evidentiary value in civil, criminal, administrative, ethical, disciplinary, and reimbursement-related disputes. Indonesian law provides a substantial normative basis for this position through health regulation, electronic information law, personal data protection law, electronic system regulation, and procedural law.

However, the evidentiary strength of EMR depends on more than formal legal recognition. System reliability, user-specific authentication, certified electronic signatures, audit trail integrity, timestamp accuracy, metadata preservation, confidentiality safeguards, and documented chain of custody determine its probative value. Weak implementation, such as shared accounts, incomplete logs, delayed entries, copy-paste documentation, uncontrolled exports, and poor downtime procedures, can substantially weaken EMR in legal proceedings.

The central challenge for Indonesia is to integrate legal validity, clinical documentation quality, technical security, and ethical confidentiality into a coherent governance framework. Healthcare facilities should treat EMR as both a patient safety infrastructure and a legal evidence infrastructure. A reliable EMR system must be clinically useful, technically secure, legally defensible, and ethically protective of patient privacy. Strengthening these dimensions is essential to ensure legal certainty for patients, healthcare professionals, and healthcare institutions in Indonesia's digital health era.

DISCLOSURES

AUTHORS CONTRIBUTION

[Initials] conceptualized the study, designed the review framework, and wrote the original draft. [Initials] conducted legal material extraction and contributed to the review and editing of the manuscript. [Initials] supervised the project and provided critical revisions. All authors have read and approved the final version of the manuscript.

FUNDING

None.

CONFLICT OF INTEREST

The authors declare no conflict of interest related to this study.

ETHICAL CONSIDERATION

Not applicable.

REFERENCES

1. Kementerian Kesehatan Republik Indonesia. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis [Internet]. Jakarta: Kementerian Kesehatan Republik Indonesia; 2022. Available from: https://jdih.kemkes.go.id/documents/peraturan-menteri-kesehatan-nomor-24-tahun-2022
2. Irwanto EL, Syofyan S, Mannas YA, Hukum F, Andalas U, Hukum F, et al. Urgensi pembuktian rekam medis elektronik dalam perspektif hukum di Indonesia. UNES Law Rev [Internet]. 2023;5(4):1641–53. Available from: https://doi.org/10.31933/unesrev.v5i4
3. Daud KR, Sagala P, Sutarno, Sutrisno. Analis Yuridis Kekuatan Hukum Rekam Medis Elektronik sebagai Alat Bukti dalam Suatu Sengketa Medis. Junal Cahaya Mandalika [Internet]. 2022;3(3). Available from: https://doi.org/https://doi.org/10.36312/jcm.v3i3.3660
4. Grassi PA, Garcia ME, Fenton JL. NIST Special Publication 800-63-3 Digital Identity Guidelines. Natl Inst Stand Technol [Internet]. 2017;800-63–3. Available from: https://doi.org/10.6028/NIST.SP.800-63-3
5. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egypt Informatics J [Internet]. 2020 Aug 1;22. Available from: https://doi.org/10.1016/j.eij.2020.07.003
6. Pemerintah Republik Indonesia. Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [Internet]. Jakarta: Kementerian Komunikasi dan Digital Republik Indonesia; 2008. Available from: https://peraturan.bpk.go.id/details/37589/uu-no-11-tahun-2008
7. Pemerintah Republik Indonesia. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik [Internet]. Jakarta: Kementerian Komunikasi dan Digital Republik Indonesia; 2019. Available from: https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019
8. Pemerintah Republik Indonesia. Undang-undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi [Internet]. Jakarta: Sekretariat Negara; 2022. Available from: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022
9. Pemerintah Republik Indonesia. Undang-undang Republik Indonesia Nomor 17 Tahun 2023 Tentang Kesehatan [Internet]. Jakarta: Kementerian Kesehatan Republik Indonesia; 2023. Available from: https://www.kemkes.go.id/id/undang-undang-republik-indonesia-nomor-17-tahun-2023-tentang-kesehatan
10. Pemerintah Republik Indonesia. Peraturan Pemerintah Republik Indonesia Nomor 28 Tahun 2024 tentang Peraturan Pelaksanaan Undang-undang Nomor 17 Tahun 2023 tentang Kesehatan [Internet]. Jakar: Kementerian Kesehatan Republik Indonesia; 2024. Available from: https://kemkes.go.id/id/peraturan-pemerintah-ri-no-28-tahun-2024-tentang-peraturan-pelaksanaan-uu-kesehatan
11. Pemerintah Republik Indonesia. Undang-undang Republik Indonesia Nomor 20 Tahun 2025 Tentang Kitab Undang-undang Hukum Acara Pidana [Internet]. Jakarta: Sekretariat Negara; 2025. Available from: https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025
12. World Health Organization. Global strategy on digital health 2020-2025. Geneva: World Health Organization (WHO); 2021.
13. International Organization for Standardization. Health informatics: Information security

management in health using ISO/IEC 27002 [Internet]. Geneva: ISO; 2016. Available from: https://www.iso.org/standard/62777.html
14. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security Techniques for the Electronic Health Records. J Med Syst [Internet]. 2017 Aug;41(8):127. Available from: https://doi.org/10.1007/s10916-017-0778-4
15. NIST. Guide to Computer Security Log Management. NIST Comput Secur Res Cent [Internet]. 2006;800–92. Available from: https://doi.org/10.6028/NIST.SP.800-92
16. Kementerian Kesehatan Republik Indonesia. Platform SatuSehat: Kebijakan pendukung dan interoperabilitas nasional. Jakarta: Kementerian Kesehatan Republik Indonesia; 2024.
17. OECD. Health Data Governance Privacy, Monitoring, and Research. OECD Heal Policy Stud [Internet]. 2015; Available from: http://dx.doi.org/10.1787/9789264244566-en
18. Badan Siber dan Sandi Negara Republik Indonesia. Lanskap keamanan siber indonesia 2024. Jakarta: BSSN RI; 2024.
19. U.S. Department of Health and Human Services. Summary of the HIPAA privacy rule [Internet]. Washington (DC): National Academies Press; 2009. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
20. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Off J Eur Union [Internet]. 2016; Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng