

Criminal Liability Analysis of Healthcare Professionals in Malpractice Cases Based on Digital Evidence in the Era of Electronic Medical Records

¹Faisal Lutfi, ²Sumarno, ³Mhd. Azhali Siregar

^{1,2,3}Universitas Pembangunan Panca Budi, Medan, Indonesia

¹faisal.lutfi.dr@gmail.com, ²sumarno@dosen.pancabudi.ac.id

³azhalisiregar@dosen.pancabudi.ac.id

Article History

Submission : 25-03-2026
Received : 30-03-2026
Revised : 28-04-2026
Accepted : 30-04-2026

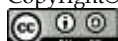
Abstract

The digitalization of healthcare services through the implementation of Electronic Medical Records (EMR) has important legal implications for proving medical malpractice cases. This study aims to analyze the construction of criminal liability for healthcare workers in malpractice cases using EMR-based digital evidence, as well as assess the strength of the evidence and its legal implications in the Indonesian criminal justice system. The method used is normative juridical research with a statutory, conceptual, and analytical approach to related doctrines and decisions. The results show that the criminal liability of healthcare workers remains based on the principles of actus reus and mens rea, with an emphasis on proving the element of fault in the form of intent or negligence. EMR as an electronic document is recognized as valid evidence under the Health Law No. 17 of 2023, Law No. 1 of 2024 as the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions, and derivative regulations, but its evidentiary strength is highly dependent on the fulfillment of the principles of data authentication, integrity, and validity. The findings also indicate that the use of EMR-based digital evidence has the potential to strengthen the proof of fault through digital forensic support, while also raising challenges related to personal data protection and the risk of criminalization of healthcare workers. This study concludes that harmonization of regulations and technical guidelines for digital evidence is necessary so that EMR can function optimally as evidence that ensures legal certainty, substantive justice, and balanced legal protection for patients and healthcare professionals.

Keywords: Criminal Liability, Criminal Evidence, Digital Evidence, Electronic Medical Records, Medical Malpractice,

Abstrak

Digitalisasi layanan kesehatan melalui implementasi Rekam Medis Elektronik (EMR) memiliki implikasi hukum yang penting untuk pembuktian kasus malpraktik medis. Studi ini bertujuan untuk menganalisis konstruksi tanggung jawab pidana bagi tenaga kesehatan dalam kasus malpraktik menggunakan bukti digital berbasis EMR, serta menilai kekuatan bukti dan implikasi hukumnya dalam sistem peradilan pidana Indonesia. Metode yang digunakan adalah penelitian yuridis normatif dengan pendekatan hukum, konseptual, dan analitis terhadap doktrin dan keputusan terkait. Hasil penelitian menunjukkan bahwa tanggung jawab pidana tenaga kesehatan tetap berdasarkan prinsip actus reus dan mens rea,



dengan penekanan pada pembuktian unsur kesalahan berupa kesengajaan atau kelalaian. Rekam Medis Elektronik (EMR) sebagai dokumen elektronik diakui sebagai bukti yang sah berdasarkan Undang-Undang Kesehatan No. 17 Tahun 2023, Undang-Undang No. 1 Tahun 2024 sebagai Amandemen Kedua Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan peraturan turunannya, tetapi kekuatan pembuktiannya sangat bergantung pada pemenuhan prinsip-prinsip otentikasi, integritas, dan validitas data. Temuan juga menunjukkan bahwa penggunaan bukti digital berbasis EMR berpotensi memperkuat pembuktian kesalahan melalui dukungan forensik digital, sekaligus menimbulkan tantangan terkait perlindungan data pribadi dan risiko kriminalisasi tenaga kesehatan. Studi ini menyimpulkan bahwa harmonisasi peraturan dan pedoman teknis untuk bukti digital diperlukan agar EMR dapat berfungsi optimal sebagai bukti yang menjamin kepastian hukum, keadilan substantif, dan perlindungan hukum yang seimbang bagi pasien dan tenaga kesehatan.

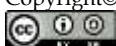
Kata kunci: Bukti Pidana, Bukti Digital, Rekam Medis Elektronik, Tanggung Jawab Pidana, Malpraktik Medis

Introduction

Healthcare professionals are the primary actors in the delivery of professional and safe medical services. Medical malpractice arises when established standards of healthcare services are violated, resulting in harm to patients. Within the context of Indonesian criminal law, the criminal liability of healthcare professionals for malpractice continues to face both substantive and implementation challenges, particularly following the enactment of Law Number 17 of 2023 on Health, which introduces new criminal provisions related to medical malpractice. Normative juridical research indicates that existing regulations have not explicitly regulated standards of proof for malpractice in the digital era, thereby complicating law enforcement authorities' efforts to assess elements of fault and negligence that require strong and reliable evidence.

The development of health information technology has encouraged the widespread adoption of Electronic Medical Records (EMRs) across healthcare facilities. EMRs contain patients' clinical data in digital form, which potentially serve as sources of evidence in medical malpractice disputes. However, the utilization of such digital evidence in criminal law practice presents new complexities concerning the authentication, integrity, and validity of digital data, all of which must be satisfied for such evidence to be admissible in court proceedings. Empirical studies reveal that Indonesian criminal procedural law and regulations governing digital evidence are not yet fully harmonized, thereby weakening the legal standing of EMRs as strong evidentiary instruments in criminal malpractice cases.

Another legal issue arises from the lack of clear and comprehensive guidelines governing the collection, storage, and verification of digital evidence derived from EMRs within the context of criminal law enforcement. The regulatory framework for Electronic Medical Records in Indonesia is multilayered and integrated. Law Number 17 of 2023 on Health serves as the foundation for the digital transformation of the health sector by recognizing EMRs as part of the national health information system, further reinforced by Government Regulation Number 28 of 2024, which regulates the national implementation of Law Number 17 of 2023. Operationally, Minister of Health Regulation Number 24 of 2022 on Medical Records mandates all healthcare facilities to maintain electronic medical records that comply with standards of interoperability, system security, and service governance, while also being integrated with national platforms such as SATUSEHAT. From the



perspective of patient legal protection, Law Number 27 of 2022 on Personal Data Protection, particularly Article 4 paragraph (2) letter (a), Articles 20, and Articles 35 to 39, classifies health data as sensitive personal data that must be managed in accordance with principles of confidentiality, consent, and data processing security. Furthermore, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions provides legal certainty by recognizing electronic medical records as valid electronic documents that may serve as legal evidence, while obligating electronic system providers to ensure the integrity, reliability, and security of EMR data throughout healthcare service processes.

Normative legal research in Indonesia identifies that although Law Number 1 of 2024 expands the definition of electronic evidence, ambiguities remain in the mechanisms for verification and judicial assessment of digital evidence. These uncertainties raise concerns regarding the weakness of proof in malpractice cases based on digital evidence, ultimately affecting the effectiveness of prosecution and the legal protection afforded to both patients and healthcare professionals.

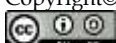
The evidentiary strength of medical records as criminal evidence has also been discussed in national legal literature, which demonstrates that traditional criminal procedural law continues to emphasize physical and written evidence. In contrast, digital evidence requires additional interpretation to attain equivalent evidentiary weight. Normative studies emphasize the urgency of regulatory reform to accommodate the rapid development of digital health technologies and to ensure that digital evidence can be lawfully and fairly processed within the criminal justice system.

The gap between advancements in health technology and criminal law regulation has created a significant research gap. Existing national and international studies tend to focus on medical technical aspects or general discussions of malpractice, without holistically examining the role and legal standing of digital evidence in determining the criminal liability of healthcare professionals. There is no clear consensus regarding the mechanisms for proving EMR-based digital evidence within the Indonesian criminal justice system. This gap highlights the need for an in-depth juridical analysis of the position of digital evidence in the era of electronic medical records.

The urgency of this research is further heightened by the ongoing digitalization of healthcare services, which is likely to increase the complexity of malpractice cases involving electronic evidence. International studies on digital health technology also indicate that such technologies may generate new forms of malpractice risk, thereby necessitating adaptations within the criminal law framework to ensure appropriate accountability and the protection of both patients and healthcare professionals. An empirical approach to digital evidence is therefore essential in developing criminal law standards of proof that are responsive to innovations in digital health technology.

This research is significant due to the need for legal reform that bridges the disparity between digital medical practice and criminal legal processes. EMR systems should be viewed not merely as administrative tools but also as sources of evidence that require a clear and systematic legal framework to ensure effective evidentiary processes. Yustiarta et al. argue that strengthening the regulatory framework governing digital evidence within the criminal justice system is expected to enhance substantive justice for both patients and healthcare professionals affected by malpractice cases in the digital era.

The formulation of research problems in this study is directed toward examining the legal regulation and construction of the criminal liability of healthcare professionals in



medical malpractice cases, particularly when the evidentiary process relies on digital evidence derived from electronic medical records within the Indonesian criminal law system. Additionally, this study focuses on analyzing the evidentiary strength and legal implications of using EMR-based digital evidence in determining elements of fault (*mens rea*) and criminal liability in medical malpractice cases.

Accordingly, the objectives of this study are to systematically analyze the legal framework and concept of criminal liability of healthcare professionals in medical malpractice cases involving the use of digital evidence in the era of electronic medical records. Furthermore, this study aims to examine the evidentiary strength and juridical impact of EMR-based digital evidence on proving criminal elements and on the effectiveness of law enforcement in medical malpractice cases.

Methods Research

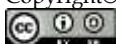
This study employs a normative juridical research method, focusing on the examination of legal norms, legal principles, and legal doctrines related to the criminal liability of healthcare professionals in malpractice cases based on digital evidence in the era of electronic medical records. A statutory approach is utilized to analyze the interrelationship and consistency among criminal law provisions, health law regulations, and laws governing electronic information and electronic documents. A conceptual approach is applied to examine theories of criminal liability, fault, evidentiary theory, and legal protection as the analytical foundation of the study. In addition, a case approach is employed to review relevant court decisions in order to understand the application of legal norms in criminal judicial practice.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials, which are systematically collected through a comprehensive literature review. The collection of legal materials is conducted by examining statutory regulations, scholarly literature, and expert opinions relevant to the research topic. The analysis of legal materials is carried out qualitatively through grammatical, systematic, and teleological interpretation to obtain a comprehensive legal understanding. This research methodology is designed to produce a logical and relevant analysis capable of explaining the legal position and evidentiary strength of digital evidence in establishing the criminal liability of healthcare professionals.

Results and Discussion

Legal Construction of the Criminal Liability of Healthcare Professionals in Digital Evidence-Based Malpractice Cases the Concept of Criminal Liability of Healthcare Professionals under Indonesian Criminal Law

The criminal liability of healthcare professionals within the Indonesian legal system refers to a legal concept whereby medical practitioners may be subject to criminal sanctions for actions that fulfill the elements of a criminal offense, whether in the form of intent (*dolus*) or negligence (*culpa*) that result in harm to patients. The most recent health legislation, namely Law Number 17 of 2023 on Health, explicitly incorporates provisions that expand the scope of criminal liability for healthcare professionals, including articles addressing medical malpractice that violates professional standards or established healthcare service procedures. Under these provisions, healthcare professionals who are proven to have committed acts resulting in serious injury or the death of a patient may be held criminally accountable in accordance with the relevant articles of the Health Law.



The fundamental principle underlying criminal liability is the doctrine of *geen straf zonder schuld* (no punishment without fault), which signifies that criminal sanctions may only be imposed when an element of fault exists, either in the form of intent or negligence. This principle is firmly established in Indonesian criminal law practice, ensuring that healthcare professionals are not automatically subjected to criminal liability merely due to unfavorable medical outcomes experienced by patients. Instead, criminal liability requires proof of a violation of professional standards or established medical procedures. In line with the findings of Wardhana and Sulisty, criminal liability in healthcare malpractice cases arises only when the element of fault meets the criteria prescribed by criminal law, including deviations from applicable medical service procedures, non-compliance with professional competency standards, or violations of professional regulations that result in harm to patients.

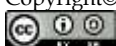
It is also important to note that, within the criminal evidentiary process, healthcare professionals are protected by the presumption of innocence until proven guilty by a court of law, which constitutes a key aspect in maintaining a balance between law enforcement interests and the protection of the medical profession. The application of the presumption of innocence serves to prevent the criminalization of medical actions that are fundamentally performed within the framework of professional practice and medical ethics. This principle requires careful and objective proof of the element of fault, thereby ensuring that professional errors are not automatically equated with criminal wrongdoing.

Elements of Criminal Acts and Fault in Medical Malpractice

There are two essential elements that must be fulfilled in the context of medical malpractice in order to qualify an act as a criminal offense, namely: (1) the element of an unlawful act, and (2) the element of fault on the part of the perpetrator. These elements reflect the manner in which medical actions that deviate from established standards may be transformed into criminal conduct when the requirements of criminal law are satisfied. The element of the criminal act in malpractice cases generally refers to acts or omissions by healthcare professionals that result in physical harm, psychological injury, or the death of a patient.

Deviations from healthcare service standards, serious misdiagnosis, or the failure to implement safety procedures constitute examples of conduct that may be categorized as criminal acts when proven before a court of law. The principle of *culpa* (negligence) represents the most frequently applied form of fault in medical malpractice cases. Negligence occurs when healthcare professionals fail to demonstrate the level of skill, prudence, and professionalism required by prevailing professional standards, thereby causing harm to patients. Although distinct from intent, negligence may nevertheless give rise to criminal liability provided that such fault can be proven lawfully and convincingly in judicial proceedings. In certain circumstances, the element of *dolus* (intent) may also be present, particularly when healthcare professionals knowingly perform high-risk medical actions without a sound medical basis or deliberately disregard established safety procedures. To satisfy this element, strong evidence must demonstrate that the perpetrator was aware of the risks associated with the conduct and nevertheless proceeded intentionally.

The proof of fault in medical malpractice cases often involves an assessment of professional service standards, documentary evidence, and expert opinions demonstrating that the medical services provided did not comply with established professional standards. This evidentiary process becomes increasingly complex when digital evidence, such as electronic medical records, is employed to demonstrate procedural deviations. Such



complexity arises because electronic medical records encompass not only clinical data but also time stamps, user authorization logs, and data modification histories, all of which must be examined for authenticity and integrity. Each digital component of electronic medical records must be verified through digital forensic mechanisms to ensure that no data manipulation or misuse has occurred. The validity of such proof also depends on healthcare facilities' compliance with electronic system governance standards as regulated under health and information technology laws.

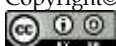
The Relevance of Criminal Liability Theory in the Context of Digital Medical Malpractice

Criminal Liability Theory is a legal doctrine that provides a conceptual framework for determining how and under what circumstances an individual may be held criminally responsible for acts committed. The core focus of this theory lies in the examination of the elements of a criminal act (*actus reus*) and fault (*mens rea*), as well as the proof of a causal relationship between the act and the resulting harm. Within the context of medical malpractice, this theory offers a foundational basis for law enforcement authorities to assess whether a medical action may be classified as a criminal offense based on these established criteria.

The relevance of this theory in malpractice cases based on digital evidence has increased significantly due to the advancement of health information technologies, particularly the widespread use of electronic medical records (EMRs) as a primary source of evidence. EMRs function as digital evidence capable of documenting the timing, content, and decision-making processes underlying medical actions in a detailed manner. Consequently, EMRs play a crucial role in evaluating the existence of unlawful conduct and the element of fault on the part of healthcare professionals. In this regard, the validity, authentication, and integrity of digital evidence become essential prerequisites for the accurate application of Criminal Liability Theory.

Criminal proof in the digital era no longer relies solely on witness testimony and physical documents but increasingly depends on electronic evidence that must be processed in accordance with legal provisions governing digital evidence. The Indonesian legal framework on electronic evidence, including the integration of the Electronic Information and Transactions Law (ITE Law) and the reformed Criminal Procedure Code (KUHAP), provides the normative basis for the admissibility and use of digital evidence such as electronic medical records in criminal proceedings. These provisions are critical to ensuring that digital evidence can effectively contribute to the assessment of both *mens rea* and *actus reus* in medical malpractice cases.

The application of Criminal Liability Theory within the context of digital evidence underscores that the mere existence of digital evidence is insufficient. Such evidence must undergo a rigorous process of legal validation to qualify as a legitimate basis for either conviction or acquittal, in line with the principles of human rights protection embedded in modern criminal justice systems. This validation process includes the examination of the legality of the evidence, its relevance to the alleged conduct, and its capacity to accurately represent the element of fault attributable to the accused. Without stringent validation procedures, digital evidence may lead to erroneous legal assessments that adversely affect both defendants and victims. In medical malpractice cases, misinterpretation of electronic medical records may result in disproportionate legal conclusions regarding the degree of fault attributable to healthcare professionals. Therefore, the application of Criminal Liability



Theory necessitates judicial and law enforcement prudence in objectively and fairly evaluating the evidentiary weight of digital evidence.

The Legal Status of Electronic Medical Records as Digital Evidence in the Criminal Evidentiary System, Electronic Medical Records as Electronic Documents and Legal Evidence

Electronic Medical Records (EMRs) constitute electronic documents containing comprehensive data on patient identity, diagnoses, medical procedures, treatments, and other clinical notes, which are created and stored digitally within healthcare facilities. Within the Indonesian legal system, EMRs are fundamentally recognized as valid legal evidence, as they fall within the category of electronic information and/or electronic documents. This recognition is explicitly regulated under the Law on Electronic Information and Transactions (ITE Law), which stipulates that electronic information and/or electronic documents, along with their printouts, constitute lawful legal evidence in the resolution of criminal cases. This provision establishes a legal foundation whereby digital data that satisfies requirements of authenticity and integrity may be submitted as evidence in criminal proceedings.

Electronic medical records do not merely function as administrative health documents but may also transform into digital evidence within criminal evidentiary processes, particularly in medical malpractice cases. In juridical practice, EMRs hold an evidentiary position equivalent to conventional written evidence, provided that such evidence fulfills both the formal and material requirements of proof.

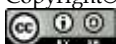
More specifically, in addition to the provisions of the ITE Law, the legal status of electronic medical records is further reinforced by healthcare regulations in Indonesia. For instance, the Minister of Health Regulation on Medical Records affirms that medical records may be utilized as evidentiary instruments in law enforcement, professional disciplinary proceedings, and the enforcement of medical ethics. These regulatory provisions further strengthen the legal standing of electronic medical records as evidence in criminal proceedings related to medical malpractice.

Requirements for the Validity and Probative Value of Digital Evidence

Although electronic medical records are recognized as digital evidence, their validity and probative value are not automatic but must satisfy specific legal requirements. The first requirement concerns the authentication of digital evidence, namely the ability to ensure that the data presented genuinely originates from a legitimate source and has not been manipulated since its creation. This authentication process often involves verification through digital transactions, such as the use of electronic signatures, as regulated under the Electronic Information and Transactions Law (ITE Law) and electronic system standards.

The second requirement relates to the integrity of digital evidence, which requires that the data contained in electronic medical records remain intact and unaltered from the time they were first recorded. Integrity is a crucial element in criminal proof, as evidence that is damaged, altered, or inconsistent may diminish or even negate its evidentiary weight in the eyes of the law. To safeguard integrity, electronic medical record systems must implement adequate technical mechanisms for data logging, backup, and protection against unauthorized access.

Furthermore, the probative value of digital evidence also depends on compliance with applicable criminal procedural law, particularly the evidentiary rules set forth in the Criminal Procedure Code (KUHAP) concerning types of evidence and methods of presenting evidence



before the court. Although the ITE Law has expanded the definition of admissible evidence by recognizing electronic documents as lawful evidence, the strength of such evidence ultimately depends on the presenting party's ability to demonstrate the validity, relevance, and causal connection of the digital evidence to the alleged criminal act.

Integrity, Authentication, and Validity of Electronic Medical Records in the Evidentiary Process

The integrity, authentication, and validity of electronic medical records constitute three fundamental aspects that determine the extent to which such digital evidence may be regarded as strong and reliable evidence within criminal proceedings. The integrity of digital evidence relates to the wholeness and consistency of data, meaning that electronic medical records must remain complete, accurate, and unaltered from the moment of their creation until their submission as evidence in court. Without assurance of integrity, digital evidence may be challenged by opposing parties in criminal cases on grounds of unreliability.

Authentication refers to the ability to verify the identity and origin of electronic medical records and to ensure that they are not forged or fabricated. This is typically achieved through technical mechanisms such as the use of electronic signatures or digital identification systems capable of linking the data to the healthcare professional or healthcare facility responsible for its creation. In the absence of clear authentication, electronic medical records may be rejected by judges due to uncertainty regarding their provenance.

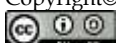
Validity concerns the conformity of electronic medical record data with actual medical facts and events. In the context of criminal proof in medical malpractice cases, data validity must be capable of demonstrating a causal relationship between the actions of healthcare professionals and the harm suffered by patients. This requirement often necessitates the support of medical expert testimony and digital forensic analysis to accurately interpret electronic data within a legal framework.

In practical terms, the application of integrity, authentication, and validity requirements not only strengthens the legal standing of electronic medical records as digital evidence but also addresses the technological challenges inherent in increasingly complex criminal proof in the digital era. This situation demands that law enforcement institutions and judicial authorities possess robust technical and methodological competence in handling electronic evidence, ensuring that both conviction and acquittal are carried out objectively and based on lawful and reliable evidence.

An Analysis of the Probative Value of Electronic Medical Record-Based Digital Evidence in Determining the Element of Fault, Proving Intent and Negligence of Healthcare Professionals

The proof of intent (*dolus*) and negligence (*culpa*) in medical malpractice cases constitutes a crucial point in determining the criminal liability of healthcare professionals. In criminal law, *dolus* refers to a mental state in which the perpetrator consciously and deliberately violates legal norms or performs acts that are known to potentially produce legal consequences, whereas *culpa* reflects a lack of due care, inaccuracy, or inadvertence arising from the failure to observe applicable professional standards. These elements must be proven lawfully and convincingly before the court in order to satisfy the prevailing principles of criminal liability.

Electronic medical records, which contain medical notes and chronological documentation of medical actions, hold strategic value in proving both elements of fault.



Time-stamped medical orders, records of procedural implementation, and digitally stored clinical annotations may serve as critical evidence in demonstrating whether a medical action was performed with deliberate intent to deviate from established procedures or merely resulted from negligence. Nevertheless, such digital data must undergo authentication and integrity verification processes before they can be relied upon as evidence supporting the element of fault. Incomplete data or manipulated information may lead to erroneous interpretations of the intent or conduct of healthcare professionals in the performance of medical actions.

Legal scholars emphasize that proving *dolus* is generally more difficult than proving *culpa*, as intent involves the perpetrator's internal motives and subjective awareness of the potential consequences of their actions. Within the context of digital evidence, electronic data such as electronic medical records must therefore be corroborated with other forms of evidence, including witness testimony or expert opinions, in order for judges to conclude that the conduct in question genuinely reflects either intent or negligence in a legal sense. Without such corroboration, digital evidence alone may be insufficient to convincingly distinguish between deliberate misconduct and negligent behavior.

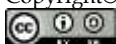
The probative value of digital evidence in determining the element of fault ultimately depends on the quality of the data, as well as on how such data are interpreted and linked to applicable professional standards and medical procedures. The use of digital evidence without proper verification carries the risk of producing legal decisions that fail to reflect substantive justice.

The Role of Digital Forensics in Proving Medical Malpractice Cases

The role of digital forensics in the evidentiary process of medical malpractice cases has become increasingly significant alongside the growing use of electronic systems for recording and managing health data. Digital forensics encompasses the methodological and legally accountable processes of collecting, preserving, examining, analyzing, and presenting electronic evidence. The application of digital forensic techniques ensures that digital evidence, such as electronic medical records, is handled in a manner that minimizes data contamination and alteration, thereby preserving its credibility as legal evidence in judicial proceedings.

A digital forensic expert bears the responsibility of ensuring that evidence extracted from electronic medical record systems accurately reflects the original condition of the data at the time of the incident and that there are no indications of data modification or deletion. The forensic process may include metadata examination, access path analysis, and digital activity log audits, all of which may assist in revealing the intent, timing, and scope of healthcare professionals' actions toward patients. These techniques are essential in providing judges with a comprehensive understanding of the context surrounding the disputed medical actions.

Digital forensics also serves as a critical basis for assessing the reliability of digital evidence in terms of its validity and direct relevance to the alleged criminal act. Through forensic analysis, it is possible to determine whether a medical record entry was created after the relevant event, whether data alterations were performed by specific parties, or whether there is evidence of deliberate manipulation. This aspect supports judges in objectively evaluating the evidentiary weight of electronic evidence, thereby facilitating the proof of both *actus reus* and *mens rea*. The role of digital forensics is therefore not merely technical but also strategic within the framework of criminal proof based on digital evidence, particularly



in reinforcing justice and accuracy in the legal assessment of healthcare professionals accused of medical malpractice. Without the involvement of a valid forensic process, electronic medical records risk being regarded as secondary or weak evidence in the eyes of the court.

Implications of Electronic Medical Records on Judicial Assessment in Criminal Cases

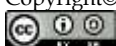
The use of electronic medical records (EMRs) as digital evidence carries significant implications for how judges assess legal facts in criminal medical malpractice cases. Judges are required to possess an adequate understanding of the characteristics of digital data, including how such evidence is generated, stored, and maintained within the electronic systems of healthcare institutions. This understanding is essential to ensure that judges do not rely solely on normative legal reasoning but also engage with the technical aspects that may affect the credibility and relevance of electronic evidence. Electronic medical records provide detailed audit trails, enabling judges to reconstruct the chronology of medical actions with greater temporal precision than conventional written records. This allows judges to more accurately evaluate whether healthcare professionals acted within the scope of their professional authority or deviated from applicable medical standards. Nevertheless, judges must exercise caution in interpreting digital evidence, as electronic information is often dispersed across multiple data entries that must be logically synthesized to produce a coherent and legally accountable factual narrative.

Another important implication is that judges are increasingly required to collaborate with digital forensic experts and medical experts when evaluating evidence, given the technical complexity that electronic evidence may present compared to traditional documentary proof. Interaction between judges and experts becomes crucial to ensure that evidentiary assessments are grounded in information that is both valid and aligned with medical and criminal law contexts. This multidisciplinary approach helps prevent misinterpretation of evidence that could undermine the quality and fairness of criminal judgments.

Juridical Implications of the Use of Digital Evidence for the Legal Protection of Patients and Healthcare Professionals, Legal Protection for Patients in EMR-Based Malpractice Evidence

The utilization of electronic medical records (EMRs) as digital evidence in medical malpractice cases has significant implications for the legal protection of patients. As the injured party, patients are entitled to access objective and accurate evidence to support malpractice claims brought before the court. EMRs can function as evidentiary instruments that comprehensively document medical events, including the timing of healthcare services, medical instructions, and records of patient progress throughout the course of treatment. This strengthens the patient's legal position in judicial proceedings, as digital data tend to be more complete and systematically structured than conventional handwritten medical records. In addition to their level of detail, EMRs also contribute to reducing interpretative errors commonly associated with traditional written documents, since each digital entry typically contains real-time information that can be traced and verified. This feature is particularly important when patients must demonstrate a causal relationship between the medical actions of healthcare professionals and the harm or risks incurred.

However, the effective use of EMRs as evidentiary tools must be accompanied by strict safeguards for patient data protection and privacy standards, in accordance with personal data protection regulations and medical ethics. The validity and transparency of EMR data are essential to ensuring that their evidentiary value benefits patients without compromising their right to privacy. The use of EMRs in criminal proceedings must therefore be balanced with



guarantees of data security and confidentiality, so that the evidence presented does not violate fundamental rights and remains consistent with the principle of legal certainty. Such certainty forms the foundation for patients to obtain justice through strong and reliable digital evidence in court proceedings.

Legal Protection for Healthcare Professionals Against the Risk of Criminalization

Another critical dimension of the use of electronic medical records (EMRs) as digital evidence is the potential risk of criminalization faced by healthcare professionals. EMRs, which comprehensively document every stage of medical intervention, may function as a double-edged sword. If not analyzed with due caution, digital data may be interpreted narrowly, leading to assumptions that healthcare professionals have committed criminal misconduct, when in fact their actions remain within legitimate professional standards. This risk is particularly evident when electronic evidence is presented without proper contextualization based on professional expertise and the complex dynamics of clinical decision-making.

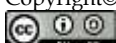
To protect healthcare professionals from unwarranted criminalization, clear legal boundaries are required to determine which circumstances genuinely fulfill the elements of criminal liability in medical malpractice cases. Law enforcement authorities and judges must carefully distinguish between professional errors that fall within the scope of disciplinary or administrative accountability and criminal acts that justify penal sanctions. This distinction constitutes an essential component of legal protection for healthcare professionals, ensuring that criminal penalties are not imposed solely due to suboptimal medical outcomes that do not amount to unlawful conduct.

Healthcare professionals are also entitled to fair and proportional evidentiary procedures, including the right to present expert witnesses, digital forensic specialists, and medical experts capable of explaining the technical aspects of EMRs. Such procedural safeguards help ensure that digital evidence is interpreted objectively and does not give rise to unfounded assumptions of criminal liability. In this context, the proper use of EMRs as digital evidence should serve the interests of justice rather than become an instrument of excessive criminalization.

Balancing Legal Certainty and Substantive Justice in Medical Criminal Cases

When electronic medical records (EMRs) are utilized as digital evidence in medical criminal cases, a fundamental need arises to balance legal certainty and substantive justice. Legal certainty requires that every piece of evidence presented before the court rests upon a solid legal basis, fulfills all requirements of authentication, integrity, and validity in accordance with applicable regulations, and can be clearly understood by judges as decision-makers. Conversely, substantive justice demands that judicial decisions go beyond formal compliance and genuinely reflect the realities of events, the complexity of medical circumstances, and the multifaceted nature of electronic medical records.

This balance is essential to ensure that criminal judgments are not based solely on the formal strength of evidence but also consider fairness for all parties involved, both patients and healthcare professionals. If judges rely excessively on digital data without adequately considering scientific context and medical practice standards, judicial outcomes may become unjust toward healthcare professionals. On the other hand, if judges disregard strong electronic evidence due to technical considerations alone, patients' rights to justice may likewise be compromised.



Recent studies indicate that a multidisciplinary approach, involving medical experts, legal scholars, and digital forensic specialists, enhances the quality of judicial assessment of electronic evidence and contributes to achieving a fair balance in criminal proceedings. With an appropriate equilibrium between legal certainty and substantive justice, the use of digital evidence—such as electronic medical records—in medical criminal cases can strengthen the function of the judiciary as a mechanism for fair and effective law enforcement without undermining individual human rights.

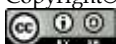
Conclusion

Electronic medical records (EMRs) hold a legitimate position as digital evidence within the Indonesian criminal evidentiary system, particularly in cases of medical malpractice. Their legal recognition as electronic documents provides a normative foundation for their use in assessing whether a healthcare professional has committed a criminal offense, provided that the requirements of authentication, integrity, and validity are fulfilled in accordance with applicable laws. Criminal liability of healthcare professionals remains grounded in the principles of unlawful conduct and the element of fault. EMRs play a significant role in revealing the chronology of medical actions, applicable standards of care, and the causal relationship between medical conduct and resulting harm. Nevertheless, proof of the element of fault cannot rely solely on digital data; it must be supported by professional standard analysis, expert medical opinions, and comprehensive digital forensic examinations. The evidentiary strength of digital evidence is largely determined by both legal and technical validation, including digital forensic verification to ensure data authenticity. Without adequate verification, the use of EMRs risks producing legal misjudgments that may either harm patients' interests or lead to unjust criminalization of healthcare professionals. Therefore, the involvement of digital forensic experts and medical experts is crucial in assisting judges to assess electronic evidence objectively.

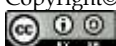
The juridical implications of using digital evidence in medical criminal cases demonstrate the necessity of balancing legal protection for both patients and healthcare professionals. While EMRs can strengthen patients' positions in evidentiary processes, they must also safeguard healthcare professionals who act in accordance with professional standards. Such a balance between legal certainty and justice can only be achieved if law enforcement is conducted cautiously, based on valid digital evidence, and with due consideration of the inherent complexity of medical practice.

Bibliography

- Bardaeni, Bardaeni, and Sudarto Sudarto. "Analisis Pertanggungjawaban Pidana Dan Faktor Penentu Dalam Kasus Malpraktek Medis." *Focus* 6, no. 2 (2025): 138–45. <https://doi.org/10.37010/fcs.v6i2.2060>.
- Daeng, Yusuf, Nelda Ningsih, Fatma Khairul, Sri Winarsih, and Zulaida Zulaida. "Pertanggungjawaban Pidana Rumah Sakit Dan Tenaga Medis Di Atas Tindakan Malpraktik Berdasarkan Undang-Undang Nomor 17 Tahun 2023 Tentang Kesehatan." *Innovative: Journal Of Social Science Research* 3, no. 6 (2023): 3453–61.
- Djatmiko, Devi Shalsabila Atika, Ahmad Yulianto Ikshan, and Muridah Isnawati. "Kekuatan Pembuktian Rekam Medis Sebagai Alat Bukti dalam Perkara Pidana." *ACADEMOS Jurnal Hukum dan Tataanan Sosial* 1, no. 1 (2022): 1–9. <https://doi.org/10.30651/aca.v1i1.14191>.



- Dmitrieva, A. A., and P. S. Pastukhov. "Concept of Electronic Evidence in Criminal Legal Procedure." *Journal of Digital Technologies and Law* 1, no. 1 (2023): 270–95. <https://doi.org/10.21202/jdtl.2023.11>.
- Fauziah, Yessy Andriani. "Malpraktik Kedokteran Gigi Dan Pertanggungjawaban Pidana : Tinjauan UU No. 17 Tahun 2023 Tentang Kesehatan." *Jurnal Hukum Dan Etika Kesehatan* 5, no. 1 (2025): 64–75. <https://doi.org/10.30649/jhek.v5i1.230>.
- Ginting, Edisa Putra, Yasmirah Mandasari Saragih, and Sumarno. "Legal Protection For Health Workers After The Implementation Of Electronic Medical Records (RME)." *International Journal of Synergy in Law, Criminal, and Justice* 1, no. 2 (2024): 118–25. <https://doi.org/10.70321/ijslcv.1i2.31>.
- Irwanto, Engga Lift, Syofirman Syofyan, and Yussy Adelina Mannas. "Urgensi Pembuktian Rekam Medis Elektronik Dalam Perspektif Hukum Di Indonesia." *UNES Law Review* 5, no. 4 (2023): 1641–53.
- Jeremia, Kevin Stevanus, and Abdul Rahman Maulana Siregar. "Kepastian Hukum Bagi Tenaga Kesehatan Dalam Kasus Malpraktik Akibat Pelanggaran Jam Kerja : Tanggung Jawab Dan Perlindungan Hukum." *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora* 2, no. 2 (2025): 11–16. <https://doi.org/10.62383/aliansi.v2i2.802>.
- Kembaren, Novalina Br, Marice Simarmata, and Riza Zarzani. "Legal Aspects of Digital Proof in Medical Criminal Cases in Healthcare Services in Hospitals." *Asian Journal of Healthcare Analytics* 4, no. 1 (2025): 141–52. <https://doi.org/10.55927/ajha.v4i1.14460>.
- Lee, Mingyu, Kyuri Kim, Yoojin Shin, Yoonji Lee, and Tae-Jung Kim. "Advancements in Electronic Medical Records for Clinical Trials: Enhancing Data Management and Research Efficiency." *Cancers* 17, no. 9 (2025): 1552. <https://doi.org/10.3390/cancers17091552>.
- Madan, R, Nileswar Das, Rahul Patley, Neeraj Nagpal, Yogender Malik, and Suresh B. Math. "Consequences of Medical Negligence and Litigations on Health Care Providers – A Narrative Review." *Indian Journal of Psychiatry* 66, no. 4 (2024): 317–25. https://doi.org/10.4103/indianjpsychiatry.indianjpsychiatry_799_23.
- Mandalika, Muhammad Sultan, Radjendra Al Fattah Banu, Rafli Achmad Irzaqie, and Vanessa Debora Muaja. "Digitalisasi Rekam Medis Dalam Pusaran Hukum Analisis Pertanggungjawaban Malpraktik Medis Dan Perlindungan Data Pasien." *Jurnal Kajian Hukum Dan Kebijakan Publik | E-ISSN: 3031-8882* 2, no. 2 (2025): 1362–69. <https://doi.org/10.62379/veegj712>.
- Mirza, Andi, Dahlan, and Teuku Muttaqin Mansur. "Criminal Liability of Perpetrators of Health Care Malpractice." *International Journal of Law and Society* 2, no. 3 (2025): 238–46. <https://doi.org/10.62951/ijls.v2i3.699>.
- Nasution, Erdi Effendi, and Abdul Rahman Maulana Siregar. "Juridical Review of Electronic Medical Records as Therapeutic Evidence in Health Law Practice." *Formosa Journal of Applied Sciences* 4, no. 1 (2025): 245–54. <https://doi.org/10.55927/fjas.v4i1.13211>.
- Nelson, Rivan. "Analisis Yuridis Mengenai Pembuktian Informasi Elektronik (Digital Evidence) Sebagai Alat Bukti Yang Sah Dalam Hukum Acara Pidana." *Lex Privatum* 10, no. 5 (2022): 1–13.
- Pemerintah RI. *Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 Tentang Kesehatan*. Sekretariat Negara, 2023.
- Putri, Renita Meidiana, Akhmad Munawar, and Sudiyono. "Pertanggungjawaban Hukum Pidana Terhadap Malpraktik Medis Pada Rumah Sakit." *Rewang Rencang : Jurnal Hukum Lex Generalis* 4, no. 7 (2023): 1–21.



- Rakha, Naeem Allah. "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations." *Mexican Law Review* 16, no. 2 (2024): 23–54. <https://doi.org/10.22201/ij.24485306e.2024.2.18892>.
- Rayyan, Rayga, and Abdul Rahman Maulana Siregar. "Kepastian Hukum Dalam Penerapan Teknologi Kesehatan: Perlindungan Data Pasien Dan Malpraktik." *Politika Progresif: Jurnal Hukum, Politik Dan Humaniora* 2, no. 1 (2025): 01–11. <https://doi.org/10.62383/progres.v2i1.1230>.
- Razak, Kaisar. "Analisis Yuridis Terhadap Rekam Medis Elektronik Sebagai Alat Bukti Sengketa Medis." *Citizen : Jurnal Ilmiah Multidisiplin Indonesia* 5, no. 3 (2025): 896–905. <https://doi.org/10.53866/jimi.v5i3.854>.
- Rokhim, Abdul. "Rekam Medis Sebagai Alat Bukti Dalam Penyelesaian Sengketa Layanan Medis." *Yurispruden* 3, no. 1 (2020): 61. <https://doi.org/10.33474/yur.v3i1.4863>.
- Sari, Indah. "Kekuatan Keabsahan Alat Bukti Elektronik Dalam Penyelesaian Perkara Pidana Di Indonesia." *Jurnal Sistem Informasi Universitas Suryadarma* 11, no. 2 (2024): 103–18. <https://doi.org/10.35968/jsi.v11i2.1245>.
- Subeki, Farlin, Abdul Rahman Maulana Siregar, and Rahmayanti Rahmayanti. "Analisis Normatif Penyelesaian Tindak Pidana Medis Dalam Program Pendidikan Dokter Spesialis Berdasarkan Undang-Undang Nomor 17 Tahun 2023 Tentang Kesehatan." *Jurnal Keluarga Sehat Sejahtera* 22, no. 1 (2024): 8–19. <https://doi.org/10.24114/jkss.v22i1.62338>.
- Syarifudin, Syarifudin. "Problematisa Pembuktian Dalam Tindak Pidana Malpraktik Dokter Ditinjau Dari Undang-Undang Nomor 17 Tahun 2023 Tentang Kesehatan." *Justitia et Pax* 40, no. 2 (2024): 295–330. <https://doi.org/10.24002/jep.v40i2.8262>.
- Vanessa, Vanessa, and Hery Firmansyah. "Analysis of the Validity of Electronic Evidence in Criminal Trial Proceedings and the Implementation of Its Admissibility (Judgment Study): Analisis Keabsahan Bukti Elektronik Dalam Pemeriksaan Persidangan Perkara Pidana Dan Implementasi Admisibilitasnya (Studi Putusan)." *Indonesian Journal of Law and Economics Review* 20, no. 4 (2025): 1–15. <https://doi.org/10.21070/ijler.v20i4.1395>.
- Wardhana, Encek Muhammad Rizky Kusuma, and Al Qodar Purwo Sulisty. "Legal Consequences of Malpractice in the Medical World for Medical Personnel." *PAMALI: Pattimura Magister Law Review* 5, no. 2 (2025): 330–34. <https://doi.org/10.47268/pamali.v5i2.3218>.
- Widjaja, Christine, and Adriano. "The Legal Power in Evidence of Electronic Medical Records As A Substitute for A Doctor's Signature | |." *Soepra. Jurnal Hukum Kesehatan* 10, no. 1 (2024): 17–28.
- Yustiarta, Ipan, T. Subarsyah, and Iyus G. Suhandi. "Perlindungan Hukum Bagi Pasien Atas Keberadaan Rekam Medis Sebagai Alat Bukti Hukum Dihubungkan Dengan Tindakan Malpraktik Ditinjau Dari Aspek Hukum Pidana." *Journal Evidence Of Law* 4, no. 2 (2025): 573–78. <https://doi.org/10.59066/jel.v4i2.1242>.

