INTERNATIONAL CONFERENCE ON THE STATE, LAW, POLITICS & DEMOCRACY (ICON-SLPD)
P-ISSN : 2962-7109 E-ISSN : 3063-6957
https://openjournal.unpam.ac.id/index.php/ICon

International Conference On The State, Law, Politics & Democracy (ICON-SLPD)
Conference Proceedings 2025

Digital Forensics in Medical Malpractice: The Challenge of Proving Clinical Data in Cloud-Based Medical Records

Agus Purwanto, S.KM.,S.H.,M.H.

[a] *Fakultas Hukum, Universitas Islam Bandung, Bandung. E-mail: agp.purwanto8@gmail.com*

Article

Received: Des 02, 2025;
Reviewed: Jan 07, 2026;
Accepted: Feb 09, 2066;
Published: Feb 26, 202

Abstract

*Transformation in healthcare, moving towards **cloud-based Electronic Health Records (EHR)**, presents new legal challenges in medical malpractice disputes, specifically regarding the validity and integrity of digital evidence. These disputes require stricter evidentiary standards concerning **authenticity, integrity,** and an accountable **digital chain of custody**. Currently, Indonesia lacks a specific regulatory framework for health digital forensics, despite the critical role of system logs and audit trails. This normative legal research, using statutory, conceptual, case, and comparative approaches, aims to analyze the legal standing of digital medical records and formulate the necessary regulatory model. The study finds that without standardized audit trails, metadata preservation, and fixed chain of custody procedures, digital medical records risk losing their evidentiary strength in court. This paper proposes the establishment of a **Health Digital Evidence Framework (HDEF)** as a national standard to ensure the validity and reliability of clinical digital evidence.*

Keywords: *Electronic Health Records; Digital Forensics; Medical Malpractice; Cloud-Based Medical Records; Chain of Custody; Digital Evidence; Health Law*.

A. INTRODUCTION

The global health sector is undergoing a profound structural change characterized by the rapid adoption of Electronic Health Records (EHR)[1]. This transformation is driven not only by technological advancements but also by regulatory mandates and the pursuit of efficiency, enhanced patient safety, and data interoperability. In Indonesia, this shift has been accelerated by recent government mandates encouraging, and eventually requiring, health facilities to migrate data from paper-based systems to digital, often utilizing cloud-based storage solutions for scalability and accessibility. While offering significant benefits—such as real-time data access, improved coordination between healthcare providers, and reduced paper trails—this digital transition introduces complex challenges concerning data security, privacy, and, crucially, legal evidence.[2]

The centrality of medical records in assessing liability in malpractice cases is well-established under the principle of *lex artis medicus*. The record serves as the key documentation to verify that a healthcare professional's actions complied with professional standards. In a digital environment, this documentation is no longer merely a physical document but a complex assembly of clinical data, system log files, and metadata. Consequently, when a medical dispute arises, the focus of the investigation shifts from interpreting handwritten notes to forensically examining the authenticity and integrity of the electronic record. A digital record must be proven to be what it purports to be (authentic) and that it has not been altered or corrupted since it was first recorded (integrity).

The current Indonesian legal framework provides a general basis for digital evidence through Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law)[3]. However, a significant gap exists in the absence of specialized technical regulations governing digital forensics protocols specifically for clinical data. The burden of proof in malpractice cases increasingly relies on the system's ability to produce a reliable audit trail—a detailed, chronological record of every user action (creation, modification, access, deletion). When EHR[4] systems are hosted on external cloud platforms, the integrity of this audit trail becomes precarious, raising fundamental questions about jurisdiction and control over the evidence. The cloud provider often manages the physical security and infrastructure logs[5], creating a third-party dependency that complicates the seizure and forensic examination process required under a judicial mandate.[6]

Furthermore, the integrity challenge is exacerbated by the potential for subtle manipulation of metadata—the data about the data—which includes timestamps, creation dates, and revision history. Proving that an EHR entry was not backdated or selectively altered requires a robust, tamper-proof system design, otherwise known as *forensic readiness*. The

---

[1] Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Academic Press, 2011), 101–105. See also ISO/IEC 27037:2012, *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*.

[2] Indonesia, *Law No. 11 of 2008 concerning Electronic Information and Transactions*. See also Indonesia, *Government Regulation No. 71 of 2019 concerning Implementation of Electronic Systems and Transactions*.

[3] Indonesia, *Law No. 17 of 2023 concerning Health*. See also Rindfleisch, "Privacy, Information Technology, and Health Care," *Communications of the ACM* 40, no. 8 (1997): 92–100.

[4] ISO 27789:2019, *Health Informatics — Audit Trails for Electronic Health Records* (International Organization for Standardization, 2019).

[5] Kohn, Corrigan, and Donaldson, eds., *To Err Is Human: Building a Safer Health System* (Washington, DC: National Academies Press, 2000), 78–80.

[6] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response* (U.S. Department of Commerce, 2020), 4-10.

current situation creates uncertainty where a crucial piece of digital evidence, such as a log entry or specific metadata, may be deemed inadmissible or unreliable in court due to a failure to demonstrate an unbroken chain of custody[7]. A clear and defensible chain of custody is paramount in digital forensics to ensure that the evidence presented has maintained its integrity from the moment it was collected until it is presented in court. The lack of standard protocols compromises this chain.

Therefore, this research is imperative. It seeks to critically examine the intersection of digital forensic principles, cloud computing vulnerabilities, and Indonesian health law. By analyzing comparative international standards (e.g., HIPAA in the US, and GDPR/EHDS in the EU), this study aims to move beyond acknowledging the problem to proposing a concrete **regulatory model** designed to secure the evidentiary strength of digital medical records, thereby protecting both patients and healthcare professionals within the bounds of justice.

a. Problem Formulation

Based on the background, this study formulates the following key questions:

1. What is the legal standing of digital medical records as evidence in the resolution of medical malpractice disputes in Indonesia?
2. What are the technical and legal challenges of digital forensics in proving clinical data stored on cloud-based systems?
3. What regulatory model is needed to guarantee the validity and evidentiary strength of digital evidence in medical disputes in Indonesia?

b. Research Objectives

This research aims to:

1. Describe the position and evidentiary strength of digital medical records in medical malpractice disputes.
2. Analyze the main digital forensic challenges in the management and proof of clinical data, focusing on cloud system vulnerabilities.
3. Propose a new regulatory model, specifically a Health Digital Evidence Framework (HDEF), that aligns with the needs for governing health sector digital evidence in the digital era.

This study is structured to first define the methodologies employed in Section 2, Including the normative legal research approach and the specific sub-approaches such as statutory, conceptual, case, and comparative analyses[8]. Subsequently, Section 3 will present the results, focusing on the critical legal analysis of EHRs as documentary evidence and an in-depth discussion of the core digital forensic challenges related to cloud environments. Finally, the Conclusion will synthesize the findings and formally propose the *Health Digital Evidence Framework (HDEF)* as the urgently needed national standard.

[7] Zissis and Lekkas, "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems* 28, no. 3 (2012): 583–592. See also Groh, "Digital Evidence and Cloud Computing: Addressing Jurisdictional Challenges," *Journal of Digital Forensics, Security and Law* 14, no. 1 (2019): 1–18.

[8] European Union, *Regulation (EU) 2016/679 on the protection of natural persons... (General Data Protection Regulation)*, art. 5.

The central contribution of this research lies in moving the focus of legal discourse beyond the simple *admissibility* of digital records to establishing the technical governance required for their long-term reliability and trustworthiness in litigation. By synthesizing insights from international best practices (such as HIPAA in the US, and GDPR/EHDS in the EU)[9] with the intricacies of Indonesian civil and procedural law, this paper aims to offer a practical and legally sound blueprint for policymakers. This contribution is particularly crucial given the rapid acceleration of the national EHR system implementation, which requires preemptive legal safeguards against future evidentiary disputes that could potentially undermine public trust in the healthcare and justice systems.[10]

Therefore, the following sections will systematically address the research objectives by first establishing the methodological foundation and then executing the critical legal and forensic analysis[11]. The ultimate goal is to provide a comprehensive legal recommendation that ensures the integrity of the evidentiary process, thereby upholding justice and accountability in the increasingly digital landscape of Indonesian healthcare.

B. MATERIALS AND METHODS

- **Research Paradigm and Type**

This research is fundamentally anchored within the Normative Legal Research (*Penelitian Hukum Normatif*)[12] paradigm, also widely recognized as doctrinal research. This choice is methodologically sound because the core problem addressed—the lack of legal certainty and procedural standards for digital evidence integrity in medical malpractice disputes—is inherently a matter of legal interpretation, statutory coherence, and regulatory gap analysis[13]. Unlike empirical research which would require collecting primary data on social behavior or case statistics, the objective here is to critically assess the existing body of Indonesian law (*das Sollen*) against the technological reality of cloud-based EHR systems (*das Sein*)[14].

The primary focus is to examine the effectiveness, coherence, and application of current legal norms, principles, and doctrines in addressing the unique challenges posed by digitized clinical data. This involves not only identifying the specific statutes (e.g., ITE Law, Health Law) that acknowledge digital records as evidence but also scrutinizing whether these general laws provide sufficient technical depth—such as requirements for metadata preservation, standardized audit trails, and system-level chain of custody—to withstand rigorous judicial scrutiny.

---

[9] Dimitropoulos, "The General Data Protection Regulation and Health Data: An Overview of the EU Framework," *Medical Law International* 16, no. 3 (2016): 199–227.

[10] Bal, "The 21st Century Medical Record: An Updated Perspective," *Clinical Orthopaedics and Related Research* 467, no. 10 (2009): 2539–2542.

[11] Ali, *Menguak Tabir Hukum (Legal Research Methodology)* (Kencana Prenada Media Group, 2009), 35.

[12] Soekanto and Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Rajawali, 1983), 13–15.

[13] Ali, *Menguak Tabir Hukum (Legal Research Methodology)* (Kencana Prenada Media Group, 2009), 35.

[14] Indonesia, *Law No. 11 of 2008 concerning Electronic Information and Transactions* (UU ITE); Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Academic Press, 2011), 101–105.

A key function of this normative inquiry is prescriptive recommendation. By first identifying the existing regulatory framework in Indonesia—including relevant statutes, governmental regulations, and established jurisprudence—the study critically evaluates its adequacy in accommodating the complex, technical requirements necessary for establishing the admissibility and reliability of digital forensic evidence derived from cloud-based Electronic Health Records (EHRs)[15]. This includes assessing how legal principles like *authenticity* and *integrity* must be redefined and reinforced by technical mandates when the evidence is volatile and stored by a third-party cloud provider[16]. The ultimate goal is to move beyond mere descriptive legal analysis. The study actively seeks to identify legal gaps (*lacunae*) and conflicts within the law, thereby establishing a robust legal basis for a prescriptive model, culminating in the proposal for a specialized Health Digital Evidence Framework (HDEF) designed to preemptively resolve future evidentiary disputes.

- **Research Approaches**

To ensure a comprehensive and robust analysis spanning both legal and technical domains, this study utilizes four interconnected legal research approaches:

a. **Statutory Approach (*Statute Approach*)**

This approach involves a meticulous examination and systematic interpretation of all binding laws and regulations in Indonesia that govern electronic information[17], healthcare services, and data protection. The central goal is to establish the legal hierarchy and identify jurisdictional overlaps or regulatory voids[18] Key legislative instruments analyzed include:

- Law No. 11 of 2008 concerning Electronic Information and Transactions (as amended) and its implementing regulations, which establish the legal recognition and prerequisites for digital records as evidence.
- Law No. 17 of 2023 concerning Health, which mandates and regulates the use of Electronic Medical Records (RME).
- Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which governs the security, storage, and processing of sensitive clinical data. The analysis specifically focuses on how the cumulative effect of these statutes addresses the requirements of **authenticity** and **integrity** for clinical data stored in third-party cloud environments.

- Powers, J. M., & Cookson, P. W. Jr. (1999). The politics of school choice research. *Educational Policy*, *13*(1), 104–122. https://doi.org/10.1177/0895904899131009

[15] ISO 27789:2019, *Health Informatics — Audit Trails for Electronic Health Records* (International Organization for Standardization, 2019); ISO/IEC 27037:2012, *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*.

[16] Ali, *Menguak Tabir Hukum*, 39.

[17] Soekanto and Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Rajawali, 1983), 13–15.

[18] *Power, J.M., & Cookson, P.W.Jr. (1999). The politics of school choice research. Educational Policy, 13(1), 104-122.https://doi.org/10.1177/089504899131009*

-

b. **Conceptual Approach**

The conceptual approach is employed to build the theoretical foundation of the research by critically engaging with fundamental legal and computer science concepts[19]. This involves defining and analyzing the relationship between abstract legal principles and concrete technological realities. Core concepts examined include:

- **Digital Forensics and *Forensic Readiness***: Defining standardized procedures for the legal collection, preservation, and analysis of digital evidence. *Forensic readiness* is investigated as a systemic legal obligation for healthcare providers to design EHR[20] systems that can reliably generate and preserve evidence for future litigation.
- ***Digital Chain of Custody***: A rigorous analysis of the technical and procedural mechanisms (e.g., cryptographic hashing, timestamping, system logging) required to establish an unbroken and legally defensible record of evidence handling, from the point of initial data capture to final presentation in a judicial setting.
- **Authenticity, Integrity, and Non-Repudiation**: Establishing the technical and legal criteria—beyond simple statutory acknowledgement—necessary to satisfy the evidentiary burden of proof for the genuineness and completeness of data derived from complex cloud architectures[21].

c. **Comparative Approach**

To inform the proposal for a national regulatory model, this research undertakes a systematic comparison of established international legal and technical frameworks concerning digital health data governance[22]. The comparison is strategic, focusing on extracting implementable best practices regarding mandatory audit controls and forensic standards. Specific jurisdictions and frameworks studied include:

- **The United States (US) - HIPAA Security Rule**: Reviewing the mandatory *Audit Controls* and *Audit Logging* requirements for Electronic Protected Health Information (ePHI) to understand technical compliance mandates.
- **The European Union (EU) - General Data Protection Regulation (GDPR) and European Health Data Space (EHDS)**: Analyzing principles related to data *integrity, confidentiality,* and the *traceability* of health data provenance across borders.
- **Singapore's National Electronic Health Record (NEHR) System**: Examining the technical guidelines regarding system-level controls, role-based access management, and the integration of *forensic readiness* into system design. The

[19] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response* (U.S. Department of Commerce, 2020), 4-10.

[20] Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Academic Press, 2011), 101–105.

[21] U.S. Department of Health and Human Services, *HIPAA Security Rule: Final Rule* (2003).

[22] European Union, *Regulation (EU) 2016/679 on the protection of natural persons... (General Data Protection Regulation)*, art. 5; Dimitropoulos, "The General Data Protection Regulation and Health Data," 199–227.

comparative analysis seeks to identify models that can be adapted to the specific legal and technological constraints of Indonesia.

d. **Case Approach**

This approach involves the detailed review of judicial precedents and key legal cases, both domestic and international, that have explicitly addressed the admissibility, reliability, and evidentiary standards for digital medical records in malpractice and liability disputes. The primary international case analyzed is ***Meherg v. Rush University Medical Center*** (2025)[23], which is used as a technical illustration of how courts assess a healthcare institution's technical capability (or inability) to produce specific audit trails or logs. The analysis of this case provides empirical support for the normative argument that robust system design is a prerequisite for successful litigation defense and forensic investigation.

- **Sources of Legal Materials**

The legal and technical materials are systematically classified into three tiers to ensure comprehensive coverage:

1) Primary Legal Materials

These constitute the binding sources of law that form the core of the analysis:

- Laws (UU) and Government Regulations (PP) of the Republic of Indonesia relevant to health, ITE, and data protection.
- Ministerial Regulations (Permenkes) from the Ministry of Health mandating EHR implementation.
- Circular Letters (*Surat Edaran*) from the Supreme Court (MA) or other high judicial bodies regarding procedural law and digital evidence.
- Specific Court Decisions (*Yurisprudensi*) that interpret the concepts of *electronic document* and *validity of evidence* in contentious cases.

2) Secondary Legal Materials

These provide expert analysis, scholarly commentary, and theoretical frameworks necessary for interpreting primary materials:

- Academic books, monographs, and peer-reviewed journal articles in the specialized fields of Health Law, Cyber Law, and Digital Forensics.
- Government legislative commentaries and policy papers (e.g., *Naskah Akademik* or official white papers on national RME implementation).

[23] Quandary Peak Research, *EHR Audit Trail Production and Legal Implications: Analysis of Meherg v. Rush* (Industry Report, 2023).

- Reports

- Reports from national professional organizations (e.g., IDI, PPNI) related to professional standards and documentation.

3) Tertiary Legal Materials

These supplementary sources provide technical standards and background information crucial for assessing technical compliance:

- **International Standards**: Documents from the International Organization for Standardization (ISO) related to information security and digital evidence (e.g., ISO 27037 on digital evidence identification; ISO 27789 on EHR system requirements).
- **Professional Guidelines**: Technical guides and best practice recommendations from global bodies like the World Health Organization (WHO), the American Medical Association (AMA), and the National Institute of Standards and Technology (NIST).

- **Techniques of Legal Material Analysis**

The material collection was systematically conducted by identifying and cataloging all relevant legal and technical documents. The core analysis technique is **prescriptive, systematic, and deductive**, executed in the following logical stages:

1. **Systematization and Inventory**: Cataloging all primary and secondary materials to establish the existing legal ecosystem governing clinical data .
2. **Synthesis and Interpretation**: Synthesizing the gathered laws and professional doctrines to determine the current legal position on EHR evidence. Interpretation is centered on identifying the true legal meaning and intent (*ratio legis*) of key legal terms like *authenticity* and *integrity* in the context of cloud-based storage, often requiring a **teleological interpretation** to bridge the gap between old laws and new technology.

3. **Conflict Mapping and Critical Evaluation**: Mapping potential conflicts and gaps between different regulatory levels (e.g., general ITE law versus specific Health Ministry regulations). A critical evaluation assesses whether the current framework provides adequate legal mechanisms to enforce the seizure and forensic audit of data controlled by a third-party cloud provider.

4. **Deductive Reasoning and Prescription**: Employing deductive logic, conclusions are drawn from general principles (e.g., the necessity of an unbroken chain of custody) and applied to the specific, complex facts of cloud EHR architecture. This phase culminates in the **prescriptive recommendation**, where the **Health Digital Evidence Framework (HDEF)** is logically derived and proposed as the necessary intervention to secure the reliability and admissibility of clinical digital evidence in Indonesian courts.

C. RESULT AND DISCUSSION

a. The Legal Standing and Evidentiary Requirements of Digital Medical Records

The legal acceptance of Electronic Health Records (EHRs) as evidence in Indonesian courts is primarily rooted in two fundamental statutes: Law No. 17 of 2023 concerning Health (Health Law) and Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law)[24]. The Health Law provides the substantive mandate, establishing the DMR as the legally recognized, official documentation of clinical services, thereby solidifying its status as documentary evidence (*alat bukti surat*) under the Indonesian Civil Procedure Law. This legislative mandate signifies a commitment to the digital transformation of healthcare, but it simultaneously transfers the legal burden of proof onto an inherently complex digital system.

The critical legal finding, however, lies in the conditional nature of this admissibility, as dictated by the ITE Law[25]. Article 5 of the ITE Law affirms the validity of electronic documents but crucially subordinates this validity to the fulfillment of technical requirements concerning **integrity (*integrity*)** and **authenticity (*authenticity*)**. This is where the distinction between a simple "electronic document" and legally defensible "digital evidence" becomes paramount. In the context of medical malpractice, where the dispute centers on the chronology, content, and proper execution of medical care (*lex artis*), the burden of proof relies on the DMR system's capability to provide conclusive evidence on two fronts[26]:

First, Authenticity (Establishing Authorship and Source): Authenticity requires proof that the electronic record entry was genuinely created or modified by the person it purports to be (i.e., the specific physician, nurse, or administrator), and that the record originated from the designated system[27]. This standard cannot be met merely by username and password. It necessitates a system capable of linking the specific entry to a specific user at a specific time, often through mandatory digital signatures or robust, non-repudiable access logs[28].

Second, Integrity (Establishing Unaltered State): Integrity is arguably the more challenging requirement in a cloud environment. It demands demonstrable proof that the content of the clinical entry has not been altered, deleted, or corrupted from the moment of its creation until its examination in court[29]. This requirement transcends the mere content of the medical note; it extends to the **metadata**—the record of when the note was created, accessed, and modified. The entire premise of integrity rests on the reliability of the system's protective mechanisms.

This technical burden is predominantly met through the system's **Audit Trail**, which is the digital chronicle of every user action and system event related to the data.

---

[24] Indonesia, *Law No. 17 of 2023 concerning Health*.

[25] Indonesia, *Law No. 11 of 2008 concerning Electronic Information and Transactions* (UU ITE), art. 5.

[26] ibid

[27] ibid

[28] Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Academic Press, 2011), 101–105.

[29] ISO 27789:2019, *Health Informatics — Audit Trails for Electronic Health Records* (International Organization for Standardization, 2019).

The audit trail transforms abstract legal principles into measurable technical facts. It serves as the single source of truth for the chronology of events, including the precise time of patient admission, drug prescription, consent forms access, or any retrospective correction to a diagnosis. The core finding here is that the evidentiary weight of DMRs in Indonesian courts is effectively **contingent upon the robustness and legal defensibility of the underlying system's audit control features.** If the system lacks detailed logging, allows for metadata manipulation, or fails to implement mandatory security measures (such as cryptographic hashing to detect unauthorized changes), the evidence risks being successfully challenged as unreliable hearsay or potentially compromised data. Consequently, the legal status of the EHR[30] shifts from being definitive evidence to merely a disputed exhibit, highlighting a critical deficiency in the regulatory focus[31]: current laws recognize the *existence* of the digital record but fail to sufficiently mandate the *technical standards* required to guarantee its **forensic integrity[32]**.

b. Digital Forensic Challenges in Cloud-Based EHR Systems

The transition to **cloud-based EHR systems** introduces three critical digital forensic vulnerabilities that directly undermine the evidentiary integrity of the data[33], thereby challenging the ability of both prosecutors and defendants to establish the truth:

1. Jurisdiction and Control Issues

When health data is stored on a third-party cloud server, often operated by multinational corporations, the location of the data and the server infrastructure becomes a significant legal hurdle. Under Indonesia's legal framework, the physical seizure and forensic examination of servers required for a thorough *digital chain of custody[34]* investigation may be complicated or outright blocked if the servers reside outside the Indonesian jurisdiction. Even if the data is legally domiciled in Indonesia, the **cloud service provider (CSP)[35]** maintains physical and administrative control over the infrastructure, logs, and system metadata. This third-party dependency creates a potential conflict between the court's authority to demand evidence and the CSP's corporate policies or international legal obligations, thereby hindering the crucial initial step of evidence identification and preservation[36].

2. Integrity and Metadata Vulnerabilities

[30] ibid

[31] Bal, "The 21st Century Medical Record: An Updated Perspective," *Clinical Orthopaedics and Related Research* 467, no. 10 (2009): 2539–2542.

[32] ibid

[33] Groh, "Digital Evidence and Cloud Computing: Addressing Jurisdictional Challenges," *Journal of Digital Forensics, Security and Law* 14, no. 1 (2019): 1–18.

[34] Zissis and Lekkas, "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems* 28, no. 3 (2012): 583–592.

[35] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response* (U.S. Department of Commerce, 2020), 4-10.

[36] ibid

Cloud environments, while secure against external physical threats, are susceptible to sophisticated digital integrity attacks[37]. The forensic challenge lies in the difficulty of detecting subtle but critical data manipulations:

- **Metadata Alteration**: Metadata (data about the clinical data, such as timestamp and user ID) is key to proving integrity. However, system administrators or privileged users can potentially exploit loopholes in a weakly designed system to backdate entries or alter access logs, effectively concealing a retrospective change in the clinical record[38].
- **Incomplete or Overwritten Logs**: Cloud systems often operate with retention policies designed for operational efficiency rather than judicial longevity. Crucial logs detailing system access, network activity, and internal database changes may be overwritten or purged before a legal dispute commences, destroying critical evidence required for forensic reconstruction of events[39].
- **Insider Threats**: The greatest threat to integrity often comes from within. IT administrators who possess high-level access privileges have the technical capability to bypass standard audit controls and manipulate data at the database level, leaving no trace recognizable by routine system checks. Without specialized forensic tools and legally mandated preservation policies, these manipulations are nearly impossible to detect post-facto.

c. Compromised Chain of Custody and Regulatory Gaps in Indonesia

The most significant finding is the absence of a National Standardized Audit Trail in Indonesia, which severely compromises the *digital chain of custody*[40]—the unbroken paper trail or digital record that proves the integrity of evidence from collection to court presentation.

1. The Critical Need for Standardization

Currently, each hospital or EHR[41] vendor in Indonesia is free to determine its own **audit trail** standards—what events are logged, how logs are stored, how metadata is structured, and for how long logs are retained. This lack of uniformity directly undermines legal processes because:

- **Inconsistent Reliability**: A judge or forensic expert cannot rely on a system's log data without first conducting a resource-intensive investigation into the system's *specific* design and security features, which varies from one provider to another[42].

---

[37] ibid

[38] Zissis and Lekkas, "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems* 28, no. 3 (2012): 583–592.

[39] ISO/IEC 27001:2022, *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements* (International Organization for Standardization, 2022).

[40] Zissis and Lekkas, "Addressing Cloud Computing Security Issues," *Future Generation Computer Systems* 28, no. 3 (2012): 583–592.

[41] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response* (U.S. Department of Commerce, 2020), 4-10.

[42] ibid

- **Difficulty in Comparison**: Malpractice cases often require comparing clinical practice against *lex artis*. If the core evidence (the DMR) is governed by disparate technical standards, the ability to establish clear facts becomes compromised. The **ISO 27789** standard, for example, specifies the minimum set of audit messages and events required for an EHR system[43], a level of technical detail currently lacking in Indonesian law.

2. The Evidentiary Lesson from *Meherg v. Rush University Medical Center*

The analysis of international jurisprudence, such as the *Meherg v. Rush University Medical Center* case (2025), provides a crucial lesson for the Indonesian legal system. In this case, sanctions against the medical center for failing to produce specific revision logs were ultimately overturned because the court acknowledged that the medical center's **legacy EHR system was technically incapable** of generating the requested logs[44]. This case highlights a critical concept: *Technical capability dictates the legal burden of production*.

Implication for Indonesia: If the Indonesian legal system accelerates the implementation of RME without first establishing rigorous **forensic readiness** standards for the systems themselves, both health facilities and patients will be vulnerable[45]. Facilities could avoid legal obligations by pleading *technical incapacity*, and victims may find crucial evidence never existed due to a poor system design, not malicious intent. This necessitates that the law must transition from merely acknowledging digital evidence to **mandating the technical capability** of the systems that generate it

d. Proposal: The Health Digital Evidence Framework (HDEF)

To address the regulatory gaps and technical vulnerabilities identified, the result of this study is the proposal for a **Health Digital Evidence Framework (HDEF)**. This framework is not a new law, but a specific, technical regulation that would operationalize the general principles of the ITE Law and Health Law within the health sector. The HDEF would mandate:

1. **Standardized Audit Trail**: A mandatory national standard specifying the minimum set of events (access, modification, viewing, printing) that must be recorded, the structure of the metadata, and the required retention period (adopting principles similar to HIPAA's *Audit Controls*)[46].
2. **Explicit Metadata Preservation**: A legal obligation requiring healthcare providers and CSPs to implement technical mechanisms (e.g., cryptographic hashing, write-

[43] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response* (U.S. Department of Commerce, 2020), 4-10.

[44] ISO/IEC 27001:2022, *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements* (International Organization for Standardization, 2022).

[45] Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Academic Press, 2011), 101–105.

[46] ibid

once-read-many (WORM) storage)[47] to ensure the integrity of the audit logs themselves, making them tamper-proof, echoing the **traceability and provenance** requirements of the EHDS[48].

3. **Digital Chain of Custody Protocols**: Establishing clear legal and technical procedures for the seizure and forensic imaging of cloud-based EHR data, including protocols for cross-jurisdictional data requests, thereby overcoming the *jurisdiction and control* issues identified[49].

The implementation of HDEF would transform digital medical records from potentially unreliable digital documents into robust and legally defensible **clinical digital evidence**, thus strengthening the pursuit of justice in medical malpractice disputes.

D. CONCLUSION

This study critically examined the legal standing and inherent evidentiary challenges of cloud-based Electronic Health Records (EHRs) within the context of medical malpractice disputes in Indonesia. By employing a normative legal methodology complemented by detailed conceptual and comparative analysis, the research yielded three primary conclusions that directly respond to the formulated research questions and provide the basis for prescriptive action.

First, concerning the **legal standing of digital medical records**, the findings confirm that while EHRs are recognized as valid documentary evidence under the ITE Law and the Health Law, this legal status is critically precarious. The actual evidentiary weight in litigation is entirely contingent upon the technical capability of the underlying system to demonstrate the **authenticity and integrity** of the clinical data. Without a robust, standardized, and tamper-proof **Audit Trail**—which serves as the sole source of truth for the chronology of events—the digital evidence remains highly susceptible to successful challenge in court, undermining the fundamental goal of accountability.

Second, the analysis revealed that the transition to **cloud-based systems** introduces significant and currently unresolved digital forensic challenges, primarily revolving around **jurisdictional limitations** concerning foreign Cloud Service Providers (CSPs) and a critically **compromised Chain of Custody**. Indonesia's general legal framework fails to prescribe the necessary technical protocols (such as mandatory metadata preservation and standardized logging) required to maintain the integrity of evidence when control rests largely with an external, third-party vendor. This regulatory void creates an environment where crucial evidence needed for accountability may genuinely not exist or be legally inaccessible, echoing the vulnerabilities exposed in international litigation.

---

[47] ISO 27789:2019, *Health Informatics — Audit Trails for Electronic Health Records* (International Organization for Standardization, 2019).

[48] Quandary Peak Research, *EHR Audit Trail Production and Legal Implications: Analysis of Meherg v. Rush* (Industry Report, 2023).

[49] European Union, *Regulation (EU) 2016/679 on the protection of natural persons... (General Data Protection Regulation)*, art. 5; Dimitropoulos, "The General Data Protection Regulation and Health Data: An Overview of the EU Framework," *Medical Law International* 16, no. 3 (2016): 199–227.

Third, the effective resolution of these technical and legal gaps necessitates a comprehensive and specialized regulatory intervention. This research therefore culminates in the **prescriptive proposal** for the establishment of the **Health Digital Evidence Framework (HDEF)**. The HDEF is envisioned as a mandatory national technical standard that must legally mandate:

1. **Standardized Audit Trail Protocols**: Setting clear, minimum requirements for logging, retention, and security measures (e.g., WORM functionality) for all EHR system logs.
2. **Explicit Metadata and Log Preservation Requirements**: Mandating that system vendors and healthcare providers implement cryptographic protection for crucial metadata to prevent undetected alteration.
3. **Clear Digital Custody Protocols**: Establishing legally enforceable procedures for the forensic collection, seizure, and transfer of EHR data from cloud environments under judicial order, thus securing the evidentiary chain.

Implementation of the HDEF is crucial to ensure that the legal system effectively keeps pace with technological transformation. By securing the technical integrity of clinical digital evidence, the HDEF will uphold the principles of accountability and predictability in the resolution of medical malpractice disputes in the rapidly evolving digital landscape of Indonesian healthcare.

REFERENCES

1. Ali, A. (2009). *Menguak tabir hukum (Legal Research Methodology)*. Kencana Prenada Media Group.
2. Bal, B. S. (2009). The 21st century medical record: An updated perspective. *Clinical Orthopaedics and Related Research*, *467*(10), 2539–2542.
3. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet*. Academic Press.
4. Dimitropoulos, A. (2016). The General Data Protection Regulation and health data: An overview of the EU framework. *Medical Law International*, *16*(3), 199–227.
5. European Union. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119.
6. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*(1), S64–S73.
7. Groh, A. E. (2019). Digital evidence and cloud computing: Addressing jurisdictional challenges. *Journal of Digital Forensics, Security and Law*, *14*(1), 1–18.
8. Indonesia. *Law No. 11 of 2008 concerning Electronic Information and Transactions* (UU ITE).
9. Indonesia. *Law No. 17 of 2023 concerning Health*.
10. Indonesia. *Government Regulation No. 71 of 2019 concerning Implementation of Electronic Systems and Transactions* (PP 71/2019).

11. ISO 27789:2019. *Health informatics — Audit trails for electronic health records*. International Organization for Standardization.

12. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.

13. ISO/IEC 27037:2012. *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. International Organization for Standardization.

14. Kohn, L. T., Corrigan, J. M., & Donaldson, M. S. (Eds.). (2000). *To err is human: Building a safer health system*. National Academies Press.

15. Lickona, T. (1992). *Educating for character: How our scholl can teach respect and responsibility*. Bantam Books.

16. Mello, M. M., Chandra, A., Gawande, A. A., & Studdert, D. M. (2010). National costs of the medical liability system. *Health Affairs*, *29*(9), 1568–1576.

17. National Institute of Standards and Technology (NIST). (2020). *NIST Special Publication 800-86: Guide to integrating forensic techniques into incident response*. U.S. Department of Commerce.

18. Powers, J. M., & Cookson, P. W. Jr. (1999). The politics of school choice research. *Educational Policy*, *13*(1), 104–122. https://doi.org/10.1177/0895904899131009

19. Quandary Peak Research. (2023). *EHR audit trail production and legal implications: Analysis of Meherg v. Rush*. (Industry Report).

20. Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM*, *40*(8), 92–100.

21. Soekanto, S., & Mamudji, S. (1983). *Penelitian hukum normatif: Suatu tinjauan singkat*. Rajawali.

22. Wiyana, N. A., & Barnawi. (2016). *PAUD format: Concepts, characteristics & implementation of early childhood education*. Ar-Ruzz Media.

23. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592.