TRANSPUBLIKA
Precise. Resilience. Felicitous.

Policy, Law, Notary and Regulatory Issues
https://ojs.transpublika.com/index.php/POLRI
Online ISSN 2809-896X

https://doi.org/10.55047/polri.v5i2.2203

Original Article

Legal Protection of Electronic Medical Record Data within Digital Based Health Information Systems in Indonesia

Christovel J. Timah[1*], Stefanus Timah[2], Mariana Mariana[3], Wilsa Wilsa[4]

[1,2]Universitas Pembangunan Indonesia Manado, Indonesia
[3]Universitas Sriwijaya, Palembang, Indonesia
[4]Universitas Samudra Langsa Aceh, Indonesia
Email: [1)] timahchristovel@gmail.com, [2)] stefanustimah@gmail.com [3)] ma_hanafiah@yahoo.com, [4)] wilsa@unsam.ac.id

Received : 28 March - 2026
Accepted : 26 April - 2026
Published online : 28 April - 2026

Abstract

The rapid advancement of digital health technology has transformed medical record management, making the legal protection of Electronic Medical Record (EMR) data increasingly critical. This study analyzes EMR data protection within digital-based health information systems in Indonesia, focusing on regulatory inconsistencies and their implications for data security and patient confidentiality. The research addresses a gap in current legal studies: the lack of comprehensive analysis integrating legal norms, institutional practices, and technological safeguards in EMR governance. It examines how existing legal frameworks ensure EMR data protection amid increasing digitalization and what structural weaknesses hinder implementation. Using a normative juridical approach with literature-based research, the study examines primary data from documented cases and EMR management reports, alongside secondary data including legal texts, academic literature, and prior studies. Data were analyzed through content analysis to identify legal inconsistencies, enforcement challenges, and systemic vulnerabilities. Findings reveal that primary legal issues lie in fragmented regulatory enforcement, absence of uniform institutional standards, and insufficient integration between legal provisions and technological systems. These gaps result in weak legal certainty and increased risk of data breaches. Existing regulations have not fully adapted to digital health system complexity, particularly regarding accountability and data protection mechanisms. This research contributes to legal scholarship by proposing harmonization of regulations, strengthening of enforcement mechanisms, and alignment between legal, institutional, and technological frameworks to ensure legal certainty, enhance patient data protection, and support sustainable development of digital health systems in Indonesia.

Keywords: Digital Health, Electronic Medical Records, Legal Protection.

1. Introduction

The rapid adoption of digital-based health information systems in Indonesia has significantly transformed the delivery of healthcare services, particularly through the implementation of Electronic Medical Records (EMR). While EMRs enhance efficiency, data accessibility, and coordination among healthcare providers, their integration also raises critical legal concerns regarding the protection of sensitive patient data. In Indonesia, the legal safeguards governing EMR remain insufficiently defined and fragmented, creating uncertainty in addressing issues such as unauthorized access, data breaches, and misuse of medical information. Existing incidents of cyberattacks and data leaks within healthcare institutions indicate not merely technical vulnerabilities, but also systemic legal deficiencies that fail to provide clear standards of accountability and protection.

A central legal problem lies in the absence of a comprehensive and coherent regulatory framework specifically governing EMR data protection. Although several legal instruments such as the Law on Electronic Information and Transactions (UU ITE), health sector regulations, and data protection provisions (are applicable), they do not explicitly and systematically regulate the management, security, and liability aspects of EMR systems. This regulatory gap results in ambiguity regarding institutional responsibilities, enforcement mechanisms, and legal remedies available to patients in cases of data breaches. Furthermore, the overlap and inconsistency among these regulations contribute to weak compliance and ineffective implementation across healthcare institutions (Basani, 2023).

Critically, existing legal frameworks in Indonesia tend to emphasize general data protection principles without adequately addressing the unique characteristics of health data, which require a higher standard of confidentiality and security. The UU ITE, for instance, primarily focuses on electronic transactions and cyber activities but lacks specific provisions tailored to medical data governance. Similarly, health regulations provide ethical and administrative guidelines but often do not establish enforceable legal standards for digital data protection. The recent development of personal data protection regulations marks a positive step; however, its operationalization within the healthcare sector remains limited and lacks clear technical and institutional integration. Hence, the current legal regime does not sufficiently bridge the gap between normative regulation and practical enforcement (Putra et al., 2024).

This study therefore focuses on examining the legal protection of EMR data within Indonesia's digital health system by identifying specific regulatory gaps, inconsistencies, and enforcement challenges. It seeks to critically evaluate whether existing laws provide adequate protection against unauthorized access, data misuse, and cyber threats, and to what extent these regulations are effectively implemented in practice. Additionally, the research explores how legal shortcomings impact patient rights, institutional accountability, and public trust in digital healthcare services (Komalasari & Mustafa, 2024).

The study hypothesizes that Indonesia's current legal framework is inadequate to ensure comprehensive protection of EMR data due to its fragmented structure, lack of sector-specific regulation, and weak enforcement mechanisms. By analyzing the interaction between legal norms, institutional practices, and technological developments, this research aims to highlight the urgent need for a more integrated and enforceable legal framework. Ultimately, strengthening EMR data protection is not only a regulatory necessity but also a fundamental requirement to uphold patient rights, ensure legal certainty, and support the sustainable development of Indonesia's digital health ecosystem (Wulyardhi & Udiana, 2025).

2. Literature Review

2.1. Definition of Legal Protection (Revised with Theoretical Framework)

Legal protection should not be understood merely as a collection of rules, but as a normative and doctrinal framework grounded in fundamental legal theories, particularly the protection of rights, legal certainty, and the rule of law. Drawing from classical legal doctrine, legal protection reflects the state's obligation to recognize, respect, and enforce individual rights, especially those related to privacy and personal autonomy. Within this framework, the protection of personal data including health data which can be situated at the intersection of human rights law, administrative law, and health law.

In the context of health information systems, legal protection extends beyond the formal existence of statutes. It involves the effective operationalization of legal norms through

institutional mechanisms, enforcement practices, and compliance culture. Theoretically, this aligns with both preventive legal protection (aimed at avoiding violations through regulation, consent mechanisms, and standards) and repressive legal protection (focused on sanctions and dispute resolution after violations occur). This distinction is essential in evaluating whether a legal system merely regulates or genuinely protects.

Critically, while many jurisdictions have adopted comprehensive data protection regimes such as the GDPR in the European Union—Indonesia's approach remains fragmented and sectoral. Existing regulations, including the Electronic Information and Transactions Law and health-sector-specific rules, demonstrate a normative commitment to data protection but lack doctrinal coherence and consistent enforcement. This reveals a gap between law in the books and law in action, a central issue in socio-legal theory.

Moreover, the Indonesian framework tends to emphasize administrative compliance rather than rights-based protection. This contrasts with more mature legal systems where data protection is explicitly framed as a fundamental right. As a result, legal protection in Indonesia often functions more as a regulatory guideline than as a robust safeguard of individual autonomy. Therefore, understanding legal protection in the EMR context requires not only defining its elements but critically assessing its effectiveness, coherence, and alignment with broader legal principles.

2.2. Categorization/Manifestation of Legal Protection (Reframed Analytically)

Legal protection in healthcare systems can be analytically categorized into three interrelated dimensions: normative (legal rules), institutional (governance structures), and operational (implementation mechanisms). This tripartite framework allows for a deeper evaluation of how legal protection functions in practice.

First, the normative dimension encompasses statutory regulations that define rights, obligations, and sanctions. In Indonesia, this includes provisions on electronic information, health data governance, and professional responsibility. However, these norms often lack harmonization, leading to ambiguity in interpretation and application. From a doctrinal perspective, this fragmentation weakens legal certainty, which is a core principle of effective legal protection.

Second, the institutional dimension refers to the role of state agencies, healthcare institutions, and oversight bodies in enforcing legal norms. In theory, institutions act as intermediaries between abstract legal rules and concrete implementation. In practice, however, institutional capacity in Indonesia is often limited by insufficient supervision mechanisms, weak accountability structures, and overlapping authorities. This creates inconsistencies in enforcement and reduces the deterrent effect of existing regulations.

Third, the operational dimension involves procedural safeguards such as data access controls, audit mechanisms, encryption, and breach notification systems. While these mechanisms are widely recognized in international best practices, their implementation in Indonesia remains uneven. This highlights a critical disconnect between regulatory expectations and technological or organizational readiness.

Importantly, these three dimensions should not be viewed in isolation. Legal protection is effective only when normative clarity, institutional strength, and operational consistency are aligned. In the Indonesian context, the lack of integration among these dimensions results in a form of "formal compliance without substantive protection." This analytical categorization thus enables a more critical assessment of how legal protection for EMR data is structured and where its weaknesses lie (Masdar & Assam, 2026).

2.3. Definition of Electronic Medical Records (EMR) (Integrated with Legal Analysis)

Electronic Medical Records (EMR) are not merely digital repositories of patient information but constitute a legally significant form of data governance within modern healthcare systems. From a legal perspective, EMRs represent a convergence of technology, medical practice, and regulatory control, where issues of data ownership, access rights, and liability become central (Choironi & Heryawan, 2023).

Conceptually, EMRs embody two interrelated dimensions. First, as a technological system, they enhance efficiency, accuracy, and interoperability in healthcare delivery. Second, as a legal object, they contain sensitive personal data that is subject to privacy protection, confidentiality obligations, and regulatory oversight. This dual character necessitates a legal framework that is both technologically informed and rights-oriented.

In jurisdictions with advanced data protection regimes, EMRs are governed by comprehensive legal principles such as purpose limitation, data minimization, and accountability (Lestari, 2021). By contrast, Indonesia's regulatory framework does not yet fully incorporate these principles in a systematic manner. While existing regulations acknowledge the importance of data security and confidentiality, they often lack detailed standards for implementation and clear allocation of responsibility in cases of data breaches.

Furthermore, the rapid adoption of EMR systems in Indonesia has not been matched byan equally robust legal infrastructure (Farhansyah & Nhifvellast, 2021). This creates a regulatory lag, where technological development outpaces legal adaptation. As a result, healthcare providers may comply with technical requirements without fully addressing legal risks, particularly in relation to patient consent, data sharing, and cross-institutional interoperability (Larasati et al., 2024).

Therefore, understanding EMR requires moving beyond a purely technical definition toward a critical legal analysis that situates EMRs within broader debates on data protection, digital governance, and patient rights. This approach provides a stronger foundation for evaluating how legal protection operates in practice and identifying necessary reforms in the Indonesian healthcare system (Takaryanto & Lany, 2025).

3. Methods

3.1. Research Object

The primary object of this study is the legal protection of Electronic Medical Record (EMR) data within digital-based health information systems in Indonesia. This issue is examined as a legal phenomenon situated within the framework of normative juridical analysis, focusing on the adequacy, coherence, and application of existing legal norms governing the protection of personal health data.

Rather than merely describing empirical occurrences, this research analyzes legal norms, principles, and regulations related to EMR data protection, including statutory provisions, regulatory frameworks, and doctrinal interpretations. Nevertheless, references to documented cases and reported incidents such as unauthorized access, data breaches, and misuse of sensitive medical information are utilized to illustrate the practical implications of normative gaps and inconsistencies in legal protection.

The study aims to identify normative deficiencies, inconsistencies in regulatory frameworks, and challenges in legal enforcement that affect patient privacy and the integrity of healthcare systems. Within the Indonesian context, this issue is particularly significant due to the rapid digitization of healthcare services, which has not been fully accompanied by

comprehensive and harmonized legal instruments. By situating the research object within a normative juridical framework, this study emphasizes the evaluation of legal norms (*das sollen*) in relation to their implementation in practice (*das sein*), thereby providing a structured legal analysis of EMR data protection in Indonesia (Tilaar & Sewu, 2023).

3.2. Research Type and Data Sources

This study adopts a normative juridical research method, which is primarily based on the analysis of legal norms and supported by a systematic review of literature. The research focuses on examining laws, regulations, legal doctrines, and scholarly opinions related to the protection of EMR data within digital health systems.

The data used in this research consist of:

1) Primary Legal Materials, including:
   a. Statutory regulations related to health law, data protection, and electronic information systems in Indonesia
   b. Official legal documents and regulatory frameworks governing EMR implementation
2) Secondary Legal Materials, including:
   a. Scholarly books
   b. Peer-reviewed journal articles
   c. Prior legal research
   d. Expert opinions and academic commentaries
3) Tertiary Legal Materials, including:
   a. Legal dictionaries
   b. Encyclopedias
   c. Supporting reference materials that clarify legal concepts

The use of these structured legal materials reflects the methodological characteristics of normative legal research, which prioritizes doctrinal analysis over empirical data collection. Literature discussing documented cases and practical challenges is incorporated to support legal interpretation, rather than serving as primary empirical evidence.

Through this approach, the research systematically evaluates the adequacy, consistency, and applicability of legal norms, while also identifying gaps and overlaps within the regulatory framework governing EMR data protection in Indonesia (Hutabarat et al., 2022).

3.3. Theoretical Foundation

This study is grounded in legal theory as its primary analytical framework, supported by complementary perspectives from health informatics. The central theoretical basis is the Theory of Legal Protection proposed by Rahardjo (2009), which emphasizes that law must function to safeguard individual rights while ensuring justice, certainty, and utility. Within the normative juridical approach, this theory is used to assess whether existing legal norms adequately provide preventive and repressive protection for EMR data. Preventive protection refers to regulatory measures designed to avoid violations, while repressive protection relates to enforcement mechanisms and sanctions in cases of legal breaches.

Additionally, the study incorporates Health Informatics Theory (Cimino & Shortliffe, 2006) to understand the technical and functional characteristics of EMR systems. However, this perspective serves as a supporting analytical tool rather than the primary research framework. The integration of these theories enables a comprehensive legal analysis that connects normative legal evaluation with the technological realities of digital health systems, ensuring both conceptual clarity and practical relevance (Antai et al., 2024).

3.4. Research Process and Data Collection

The research process follows a systematic literature-based approach, emphasizing rigorous data collection and analysis from written sources. Data and information are gathered through comprehensive examination of books, academic journals, prior studies, reports, policy documents, and articles relevant to the protection of EMR data and digital health governance. This approach involves identifying, reviewing, and synthesizing literature that addresses legal protection frameworks, documented case studies, institutional practices, and technological considerations associated with EMRs. Each source is critically assessed for credibility, relevance, and applicability to the Indonesian context, ensuring that insights drawn are evidence-based and analytically sound. The data collection process also involves cross-referencing multiple sources to identify convergences, discrepancies, and emerging patterns in legal and technological practices.

Furthermore, the research organizes findings thematically around the study's key concepts: Legal Protection, EMR, and Digital Health, enabling structured analysis and interpretation. This meticulous approach ensures that data is not only comprehensive but also aligned with research objectives, allowing the study to draw well-supported conclusions regarding gaps, challenges, and potential improvements in EMR legal protection within Indonesia. By systematically reviewing and compiling literature, the study creates a coherent foundation for subsequent analysis and discussion, linking empirical evidence with theoretical frameworks (Hutabarat et al., 2022).

3.5. Data Analysis Techniques

The study employs content analysis as its primary data analysis technique, allowing for systematic identification, categorization, and interpretation of patterns, themes, and relationships within collected literature. This method involves detailed reading and coding of textual sources to extract information related to legal protection mechanisms, EMR system practices, and digital health implementations. Patterns are identified in terms of regulatory adequacy, institutional compliance, technological vulnerabilities, and interactions between legal frameworks and healthcare operations. The analysis also examines recurring challenges, best practices, and recommendations reported in prior studies, providing a comparative perspective to assess the Indonesian context. By employing content analysis, the study synthesizes complex information into structured insights, enabling the researcher to highlight gaps, trends, and implications for both theory and practice. This technique supports critical evaluation of literature, ensuring that interpretations are evidence-based, coherent, and relevant to research objectives. Ultimately, content analysis facilitates the transformation of diverse written sources into meaningful conclusions, providing a robust foundation for the study's subsequent results, discussion, and policy recommendations regarding legal protection of EMR data in Indonesia's digital health systems (Lavreniuk & Odusanvo, 2024).

4. Results and Discussion

4.1. Research Results

The study reveals that the implementation of digital-based health information systems in Indonesia, particularly the management of Electronic Medical Records (EMR), faces significant challenges related to legal protection and operational compliance. Literature and documented cases indicate that although statutory laws, including the Electronic Information and Transactions Law and Ministry of Health regulations, exist to safeguard patient data, practical enforcement is inconsistent. Smaller healthcare facilities often lack administrative

capacity, technical expertise, and awareness of legal obligations, which increases the risk of unauthorized access and misuse of sensitive patient information. Meanwhile, larger hospitals demonstrate better compliance due to structured IT units, policy frameworks, and procedural safeguards, illustrating a disparity in EMR protection between institutions. The uneven application of legal protections underscores the misalignment between rapid technological adoption and regulatory preparedness, emphasizing the need for integrated measures that combine statutory law, institutional policy, and procedural enforcement to ensure patient data confidentiality, integrity, and accessibility (Hendrata & Karim, 2025).

Analysis shows that legal protection manifests through statutory regulations, institutional policies, and operational procedures. Statutory laws define patient rights and penalties for breaches, while institutional policies translate these into internal guidelines, including employee training, access control, and audit processes. Procedural safeguards operationalize these policies, involving monitoring system activities, reporting breaches, and maintaining documentation. Hospitals with comprehensive policies and procedural safeguards report fewer incidents of data breaches and higher compliance levels, whereas institutions relying solely on statutory provisions experience greater vulnerabilities. These findings highlight the importance of a layered approach in which law, institutional governance, and operational measures work in synergy to reinforce EMR security and safeguard patient information (Ikawati & Haris, 2024).

The research identifies common technological and organizational vulnerabilities within EMR systems. Technical weaknesses include inadequate encryption, insufficient authentication protocols, lack of interoperability, and limited backup mechanisms. Organizational challenges encompass unclear staff responsibilities, insufficient training, and inconsistent application of policies. Literature and case analyses show that these vulnerabilities lead to unauthorized access, accidental disclosure, and cybersecurity breaches, even in environments where legal frameworks are in place. Addressing these vulnerabilities requires a dual approach that combines technological security measures with strong institutional policies and consistent legal enforcement, ensuring that EMR systems operate safely and effectively (Kartika, 2025).

Findings indicate that the adoption of digital health technologies is increasing rapidly, driven by government initiatives, urbanization, and patient demand for efficient healthcare services. Technologies such as EMRs, telemedicine platforms, mobile health applications, and cloud-based hospital management systems are being implemented with varying degrees of sophistication. However, adoption is uneven: urban hospitals generally demonstrate higher technological maturity and compliance with legal standards, while smaller or rural facilities lag behind. This disparity suggests that digital health benefits are not equally distributed and that institutions lacking legal and operational readiness are more susceptible to breaches, emphasizing the critical link between digital health adoption and comprehensive EMR protection (Makarim & Wijayanto, 2024).

The study identifies multiple documented incidents of patient data breaches, including unauthorized internal access, accidental disclosure, and cyberattacks. These cases highlight both technological and institutional gaps in EMR management. Literature reports that inadequate legal awareness, poor procedural enforcement, and insufficient technical safeguards contribute to such breaches. The consequences of these incidents include reputational damage, loss of patient trust, and potential legal liability. These findings underscore the need for a proactive and preventive approach that aligns legal protections with operational and technological measures, ensuring secure and reliable management of EMR data.

Institutional responses to EMR security challenges vary significantly. Larger hospitals often establish dedicated compliance and IT units, conduct routine audits, and implement multi-layered access control systems. Smaller clinics, however, may have minimal security measures and limited understanding of legal obligations. Literature shows that institutions combining legal compliance with internal operational policies demonstrate higher levels of EMR security and lower breach incidence. These findings suggest that context-specific strategies, tailored to institutional capacity and resources, are essential to ensure effective legal and technological protection of EMR data.

Comparative literature demonstrates that countries with comprehensive EMR legal frameworks, such as Singapore and South Korea, exhibit stronger data protection, consistent enforcement, and standardized operational procedures. In contrast, Indonesia's regulatory environment, though improving, suffers from fragmentation, ambiguity, and inconsistent enforcement. These comparative insights suggest that integrating international best practices, including clear regulatory guidance, regular monitoring, and standardized institutional protocols, could strengthen EMR protection in Indonesia and enhance public trust in digital health systems.

The analysis confirms that the three key elements including legal protection, EMR systems, and digital health adoption are deeply interrelated. Effective legal protection reinforces EMR security, which in turn supports broader digital health objectives, including patient trust, system reliability, and efficient healthcare delivery. Weak legal safeguards, however, compromise technology adoption, increase vulnerability to breaches, and erode confidence in digital health services. Literature emphasizes that optimal outcomes require coordinated strategies where laws, institutional policies, and technological safeguards function together, addressing vulnerabilities across multiple levels of the healthcare system.

Overall, the study finds that while digital health adoption in Indonesia is progressing, significant gaps remain in legal protection and operational practices. Institutional readiness varies widely, technological vulnerabilities persist, and enforcement of existing laws is inconsistent. Literature suggests that addressing these gaps requires an integrated approach combining statutory frameworks, institutional policies, procedural safeguards, and technological security measures. The findings underscore the urgent need for evidence-based reforms, institutional capacity-building, and technology-driven interventions to ensure that EMR systems are secure, compliant, and capable of supporting a trustworthy and sustainable digital health ecosystem in Indonesia.

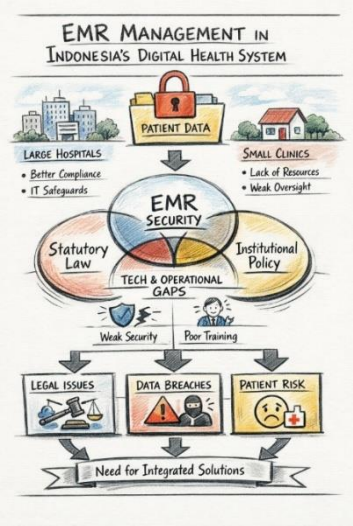

Figure 1. EMR management challenges in Indonesia

The diagram in figure 1 illustrates the challenges of managing Electronic Medical Records (EMR) within Indonesia's digital health system. At the top, "Patient Data" is highlighted as the central element that needs protection. The diagram contrasts large hospitals and small clinics: large hospitals typically have better compliance and IT safeguards, while small clinics face limited resources and weak oversight.

At the center, EMR Security is depicted as the intersection of three main components: Statutory Law, Institutional Policy, and Technological & Operational Measures. Weaknesses in technology and operations—such as poor security and insufficient staff training—create vulnerabilities in EMR management.

These gaps lead to three key risks: Legal Issues, Data Breaches, and Patient Risk, each visually represented at the bottom of the diagram. Arrows from these risks point toward a concluding note emphasizing the Need for Integrated Solutions, highlighting that effective EMR protection requires coordinated legal enforcement, institutional governance, and technological safeguards to ensure patient data confidentiality, integrity, and trust in digital health services.

4.2. Discussion

4.2.1. Implications for Legal Frameworks

The research indicates that Indonesia's legal frameworks for EMR protection, though formally established, demonstrate inconsistent enforcement across healthcare institutions. Literature shows that while laws, such as the Electronic Information and Transactions Law and Ministry of Health regulations, provide a legal basis for protecting patient data, practical implementation varies widely. Larger hospitals may comply rigorously due to dedicated compliance units, but smaller clinics often lack awareness or resources to meet statutory requirements. This disparity leaves certain patient populations exposed to risks of unauthorized access, data breaches, and misuse of sensitive medical information, compromising trust in digital health systems.

The study emphasizes that gaps in enforcement diminish the effectiveness of existing regulations. Case studies and literature suggest that regulatory oversight is limited, monitoring mechanisms are weak, and penalties for noncompliance are inconsistently applied. Without a uniform enforcement strategy, institutions interpret and implement laws differently, leading to fragmented protection for EMR data. This highlights the need for clearer operational guidelines, standardization of institutional procedures, and mechanisms to monitor compliance continuously.

Another implication concerns the alignment of technological adoption with legal preparedness. Rapid digitization has introduced advanced EMR systems without simultaneous adaptation of legal protections or guidance on operational implementation. Literature suggests that when legal frameworks fail to keep pace with technological developments, gaps emerge in data protection, potentially undermining patient privacy and institutional accountability. Strengthening legal frameworks requires dynamic adaptation to technological realities while maintaining ethical and human rights principles.

The findings also underline the necessity of integrating stakeholder engagement into legal reforms. Policymakers, healthcare administrators, IT professionals, and patients should be involved in shaping regulations to ensure applicability and feasibility. Literature demonstrates that participatory approaches result in clearer guidelines, improved compliance, and increased awareness of rights and responsibilities among healthcare personnel.

Additionally, the study highlights the importance of harmonizing national laws with international best practices. Comparative literature indicates that countries with robust EMR

legal frameworks, such as Singapore and South Korea, enforce consistent rules, clear penalties, and standardized institutional measures. Indonesia can adopt these practices while tailoring them to local healthcare realities, technological infrastructure, and resource availability.

Finally, the research suggests that legal frameworks should be designed to support operationalization at the institutional level. Laws alone cannot ensure protection; they must provide actionable guidance, clear responsibilities, and structured monitoring. Integrating these elements strengthens accountability, enhances patient trust, and ensures that EMR systems operate within a legally and ethically secure environment.

Table 1. Gaps in Indonesia's EMR Legal Frameworks: Findings and Recommendations

Theme	Key Research Finding	Implication/Recommendation
Inconsistent Enforcement	Formal laws (e.g., Electronic Information and Transactions Law, Ministry of Health regulations) exist, but enforcement varies: large hospitals comply via dedicated units, while smaller clinics lack resources/awareness.	Develop uniform enforcement strategies, clearer operational guidelines, and continuous monitoring to reduce fragmentation and protect vulnerable patients.
Gaps in Regulatory Oversight	Weak monitoring, inconsistent penalties, and differing institutional interpretations undermine regulations.	Standardize procedures across institutions and apply penalties consistently to boost effectiveness.
Technological vs. Legal Misalignment	Rapid EMR digitization outpaces legal adaptations, creating data protection gaps.	Dynamically update frameworks to match tech advancements while upholding ethics and human rights.
Stakeholder Engagement	Limited involvement of policymakers, admins, IT pros, and patients in reforms.	Adopt participatory approaches for feasible, awareness-boosting regulations.
Alignment with International Practices	Indonesia lags behind robust systems in Singapore/South Korea (consistent rules, penalties, standards).	Harmonize with global best practices, tailored to local infrastructure and resources.
Operationalization Needs	Laws lack actionable guidance, responsibilities, and monitoring for institutions.	Embed practical elements in frameworks to enhance accountability, trust, and ethical EMR use.

4.2.2. Technological and Operational Challenges

The study identifies numerous technological vulnerabilities in EMR systems that affect the protection of patient data. Literature shows that weaknesses such as inadequate encryption, poor authentication, insufficient backup mechanisms, and lack of interoperability create potential entry points for unauthorized access or cyberattacks. These deficiencies compromise the integrity, confidentiality, and availability of medical information, even when laws and institutional policies exist.

Organizational challenges further exacerbate technological vulnerabilities. Hospitals and clinics often exhibit unclear staff responsibilities, limited training, and inconsistent application of policies. Literature suggests that personnel unfamiliar with legal obligations or technological systems are more likely to engage in unintentional breaches or mishandling of data. The combination of technological gaps and operational shortcomings produces systemic vulnerabilities.

The study finds that smaller healthcare institutions are particularly affected due to limited resources and technical expertise. While large hospitals may implement advanced IT solutions, multi-factor authentication, and continuous monitoring, smaller clinics often rely on basic digital tools with minimal security features. Literature demonstrates that this disparity increases the risk of breaches and highlights the importance of tailored interventions based on institutional capacity.

Integration of legal frameworks with technological measures is critical for mitigating risks. Literature indicates that when laws and regulations are complemented by robust technology solutions—such as encrypted databases, role-based access control, and audit trails—institutions achieve higher levels of EMR security. The research underscores that technology alone is insufficient; it must work in tandem with legal and organizational measures.

Proactive technological strategies, such as regular system audits, penetration testing, and risk assessments, are essential. Literature highlights that continuous evaluation allows institutions to identify vulnerabilities, anticipate emerging threats, and update systems accordingly. These practices, combined with legal guidance, enhance overall EMR protection and align operational procedures with regulatory expectations.

Overall, the research demonstrates that technological and operational measures are interdependent. Effective EMR protection requires harmonizing IT infrastructure, staff competency, institutional procedures, and legal compliance. Neglecting any of these components can compromise the system, emphasizing a holistic approach that integrates technology, operations, and law.

4.2.3. Role of Institutional Policies

Institutional policies serve as the operational backbone translating statutory laws into practical measures within healthcare facilities. Literature indicates that hospitals with well-documented internal policies—covering access control, staff responsibilities, and data handling—experience higher compliance with legal requirements and fewer security breaches. Policies formalize expectations and provide guidance for day-to-day EMR management.

The study finds that institutional policies contribute to a culture of accountability. When employees understand their obligations and the consequences of violations, adherence to data protection practices increases. Literature shows that policy enforcement combined with training programs reinforces staff awareness and reduces the likelihood of errors, strengthening EMR security.

Policies also play a critical role in aligning technology with legal frameworks. Operational guidelines ensure that technological measures, such as system monitoring, encryption, and authentication protocols, are implemented consistently and in accordance with legal standards. Literature highlights that alignment between policy, technology, and law minimizes gaps and enhances institutional resilience against data breaches.

The research emphasizes that policies must be context-specific. Institutions vary in size, technological capacity, and resources; therefore, uniform guidelines may not be practical. Literature recommends tailored approaches that consider local realities while maintaining compliance with national legal requirements, ensuring both feasibility and effectiveness.

Regular monitoring and auditing of institutional policies are essential. Literature suggests that ongoing evaluation identifies weaknesses, informs updates, and supports continuous improvement. Policies without monitoring risk becoming nominal procedures that fail to protect patient data effectively.

Ultimately, institutional policies are indispensable for operationalizing legal protections. By establishing clear procedures, responsibilities, and enforcement mechanisms, institutions can bridge the gap between theoretical rights and practical implementation, creating a secure and compliant environment for EMR management.

4.2.4. Relationship Between Digital Health Adoption and Legal Risk

Rapid digital health adoption introduces both opportunities and risks. Literature indicates that technologies such as EMRs, telemedicine, and mobile health applications enhance efficiency, access, and patient engagement, but also magnify legal and operational vulnerabilities when safeguards are insufficient. The study finds that legal gaps can undermine the benefits of digital health, as institutions adopting these technologies without integrated legal and procedural measures are at greater risk of breaches, misuse, and noncompliance. Literature further demonstrates that such gaps erode patient trust, limit technology adoption, and expose facilities to legal liabilities, highlighting the interdependence of innovation and regulation.

Building on this, the research suggests that proactive risk assessment is critical during digital health implementation. Identifying potential threats to data confidentiality and integrity allows institutions to align technological, operational, and legal safeguards. Literature emphasizes that preemptive measures reduce exposure to incidents and improve compliance outcomes.

Beyond risk assessment, staff training emerges as another key factor. The study finds that personnel must be aware of both technological protocols and legal obligations, as informed staff reduce accidental breaches and contribute to a culture of compliance, reinforcing EMR protection as digital health systems expand. Equally important, monitoring and continuous evaluation must accompany these efforts. Since digital health technologies evolve rapidly and legal frameworks may lag behind, institutions must adapt policies and technical safeguards in response to emerging risks, maintaining alignment between law, technology, and practice.

In summary, successful digital health adoption depends on harmonizing technological innovation with robust legal and operational measures. Failure to integrate these dimensions increases vulnerability, whereas coordinated implementation strengthens EMR security and promotes sustainable digital healthcare delivery.

5. Conclusion

The findings of this study demonstrate that the protection of Electronic Medical Record (EMR) data within Indonesia's digital-based health information systems is significantly influenced by the interplay of legal frameworks, institutional policies, and technological infrastructure. While statutory regulations, such as the Electronic Information and Transactions Law and Ministry of Health directives, provide a formal basis for safeguarding patient information, their enforcement is inconsistent, particularly in smaller or resource-limited healthcare institutions. Technological vulnerabilities, including inadequate encryption, poor authentication protocols, and limited interoperability, further exacerbate risks, as do operational deficiencies like unclear staff responsibilities and insufficient training. The literature indicates that institutions combining robust legal compliance with structured

operational procedures and advanced technological measures demonstrate higher data security, reduced breaches, and greater patient trust. The study highlights the critical importance of aligning law, policy, and technology in a cohesive and coordinated manner to address the complex challenges posed by the rapid digitization of healthcare services in Indonesia.

Consequently, the research underscores the urgent need for integrated strategies to strengthen EMR protection and enhance the sustainability of digital health systems. Recommendations include reinforcing legal frameworks through clear enforcement mechanisms, standardizing institutional policies across healthcare facilities, and implementing technological safeguards that align with regulatory and operational standards. Additionally, capacity-building initiatives such as staff training, continuous monitoring, and adaptive feedback systems are essential to maintain compliance and mitigate emerging risks. Comparative insights from international practices suggest that harmonizing these three dimensions—law, technology, and operational policy—can provide a resilient foundation for secure EMR management while fostering public trust and optimizing healthcare delivery. Ultimately, this study contributes both theoretical and practical guidance, emphasizing that effective EMR protection is achievable only through a holistic, multi-layered approach that integrates legal, technological, and institutional measures within Indonesia's evolving digital health ecosystem.

6. References

Antai, G. O., Mulegi, T., Barongo, E. K., Ekpenisi, C., Kisubi, E. C., & Okonji, I. C. (2024). Exploring mechanisms for enforcing human rights within the context of international law: Issues and challenges. *NIU Journal of Legal Studies*, *10*(1), 59–70. https://doi.org/10.58709/niujls.v10i1.1943

Basani, C. S. (2023). Legal protection of patient's electronic medical record: Indonesian legal perspective. *Dialogia Iuridica*, *15*(1), 94–112. https://doi.org/10.28932/di.v15i1.7492

Choironi, E. A., & Heryawan, L. (2023). Persepsi Dokter Klinik Dalam Menggunakan Rekam Medis Elektronik Berbasis Cloud Computing: Survei Penggunaan rekmed.com. *Jurnal Ilmiah Informatika Global*, *13*(3). https://doi.org/10.36982/jiig.v13i3.2691

Cimino, J. J., & Shortliffe, E. H. (2006). *Biomedical Informatics: Computer Applications in Health Care and Biomedicine (Health Informatics)*. Springer-Verlag. https://link.springer.com/book/10.1007/978-3-030-58721-5

Farhansyah, F., & Nhifvellast, R. (2021). Sosialisasi Sistem Penyimpanan Rekam Medis di Klinik Panacea. *JOURNAL OF SUSTAINABLE COMMUNITY SERVICE*, *2*(1), 47–51. https://doi.org/10.55047/jscs.v2i1.436

Hendrata, W. M., & Karim, A. (2025). Legal Protection of Patients' Confidentiality in the Era of Mandatory Electronic Medical Records. *Widya Pranata Hukum: Jurnal Kajian Dan Penelitian Hukum*, *7*(2), 236–257. https://doi.org/10.37631/widyapranata.v7i2.1723

Hutabarat, D. T. H., Zebua, R., Sitorus, R. A., Subakti, F. A., Ramadhani, H., Mangunsong, J., Nduru, F., Alfah, G. S., Pasaribu, J. C. D., & Malau, R. M. (2022). The Urgency Of Legal Protection Against The Implementation Of Electronic Information Technology-Based Medical Records In Regulation Of The Minister Of Health Of The Republic Of Indonesia Number 269 Of 2008. *Journal of Humanities, Social Sciences and Business (JHSSB)*, *1*(4), 59–68. https://doi.org/10.55047/jhssb.v1i4.234

Ikawati, F. R., & Haris, M. S. (2024). Challenges in implementing digital medical records in Indonesian hospitals: Perspectives on technology, regulation, and data security. *Proceeding International Conference Of Innovation Science, Technology, Education, Children And Health*, *4*(2), 1–25. https://doi.org/10.62951/icistech.v4i2.70

Kartika, A. N. (2025). The Urgency of Legal Protection for Electronic Medical Records Amid Cybercrime Threats: A Literature Review on Patients' Rights and Doctors' Obligations. *Greenation International Journal of Law and Social Sciences*, *3*(2), 546–557. https://doi.org/10.38035/gijlss.v3i2.494

Komalasari, R., & Mustafa, C. (2024). Electronic Health Records in Indonesia: A Law and Policy Analysis. *Jurnal Mahkamah Keadilan*, *2*(1). https://doi.org/10.2139/ssrn.4986272

Larasati, T., Fardiansyah, A. I., Saketi, D., & Dewiarti, A. N. (2024). The ethical and legal aspects of health policy on electronic medical records in Indonesia. *Cepalo*, *8*(2), 103–112. https://doi.org/10.25041/cepalo.v8no2.3634

Lavreniuk, S., & Odusanvo, V. (2024). Obstacles in the employment of people with disabilities: The perspective of employees and employers in Ukraine. *Baltic Journal of Legal and Social Sciences*, *4*, 204–221. https://doi.org/10.30525/2592-8813-2024-4-20

Lestari, A. (2021). *Tinjauan Beban Kerja Petugas Rekam Medis Guna Meningkatkan Produktivitas Petugas Unit Rekam Medis Di Rumah Sakit TNI-AD TK*. STIKES BHAKTI HUSADA MULIA.

Makarim, M. H., & Wijayanto, E. (2024). Digital-Based Health Law System Transformation in Indonesia: Legal Protection for Patients and Healthcare Workers. *Dialogia Iuridica*, *16*(1), 27–48. https://doi.org/10.28932/di.v16i1.9422

Masdar, F., & Assam, R. (2026). Legal Protection of Patient Privacy Rights in the Use of Electronic Medical Records in Indonesian Hospitals. *Moccasin Journal De Public Perspective*, *3*(1), 45–61. https://doi.org/10.37899/mjdpp.v3i1.337

Putra, N. I. K. U., Kuswardhani, T., & Purwani, S. P. M. E. (2024). Analysis of patient rights protection through medical record confidentiality and information disclosure system in Indonesian Hospitals. *Journal La Sociale*, *5*(2), 539–549. https://doi.org/10.37899/journal-la-sociale.v5i2.1141

Satjipto, R. (2009). Penegakan Hukum suatu tinjauan sosiologis. *Yogyakarta: Genta Publising*.

Takaryanto, D., & Lany, A. (2025). Legal protection of personal data in the exchange of electronic medical record in healthcare services. *Research Horizon*, *5*(6), 2817–2830. https://doi.org/10.54518/rh.5.6.2025.897

Tilaar, T. S., & Sewu, P. L. S. (2023). Review of electronic medical records in Indonesia and its developments based on legal regulations in Indonesia and its harmonization with electronic health records (manual for developing countries). *Daengku: Journal of Humanities and Social Sciences Innovation*, *3*(3), 422–430. https://doi.org/10.35877/454ri.daengku1662

Wulyardhi, G. S., & Udiana, G. K. (2025). The legal status of electronic medical records and health data privacy in Indonesia: Current regulations, gaps, and future directions. *Jurnal Dharmaputra Hukum Kesehatan*, *1*(2), 47–52. https://dmedlaw.org/index.php/dmlj/article/view/10