Research Horizon

ISSN: 2808-0696 (p), 2807-9531 (e)

Research Horizon
Volume: 05
Issue: 06
Year: 2025
Page: 2817-2830

Citation:
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.

Article History:
Received: October 6, 2025
Revised: November 10, 2025
Accepted: December 16, 2025
Online since: December 31, 2025

Legal Protection of Personal Data in the Exchange of Electronic Medical Record in Healthcare Services

Davin Takaryanto[1*], Arman Lany[1]

[1] Universitas Islam Nusantara, Bandung, Indonesia

[*] *Corresponding author: Davin Takaryanto (takaryantodavin.md@gmail.com)*

Abstract

Digital transformation in Indonesia's health sector has fundamentally changed the way patient information is collected, stored, and managed through Electronic Medical Records (EMR). This study aims to (1) map the active legal basis governing the confidentiality of EMRs in Indonesia; (2) identify normative and practical gaps in its implementation; (3) propose auditable technical and governance standards for healthcare facilities and system providers; and (4) outline procedural and judicial mechanisms for resolving health data breach disputes. Using a normative legal approach, this study analyzes the constitutional, legislative, and regulatory legal framework, such as Law Number 17 of 2023 concerning Health, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 concerning Electronic Information and Transactions, Government Regulation Number 71 of 2019, and Minister of Health Regulation Number 24 of 2022. The results of the study show overlapping authorities, weak institutional coordination, and the absence of procedural standards related to the verification of RME in court. The study's findings reveal that EMR confidentiality protection in Indonesia is weak not due to a lack of legal regulations, but due to inadequate technical readiness and governance for its implementation.

Keywords

Electronic Medical Records, Data Confidentiality, Health Law, Personal Data Protection.

1. Introduction

Digital transformation in the health sector has fundamentally changed the way medical information is collected, stored, and managed (Komalasari & Mustafa, 2023). The implementation of Electronic Medical Records (EMR) has become an integral component of modern healthcare systems because it improves efficiency, accuracy of records, and coordination between healthcare professionals. However, this change also increases the potential risk of data leaks and misuse of personal and sensitive patient information. Amidst technological advances and the integration of national health systems such as *SatuSehat*, concerns have arisen regarding the ability of healthcare institutions to guarantee the confidentiality and integrity of patient data. At the constitutional level, Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees that every person has the right to protection of their personal self, family, honor, dignity, and property. This principle is the main legal basis for the state in protecting the security of its citizens' health data (Mendelson, 2017).

Normatively, the protection of medical record confidentiality in Indonesia has been clearly regulated through several legal instruments that are still in force (Hutabarat et al., 2022). Law Number 29 of 2004 concerning Medical Practice requires health workers to create, maintain, and protect the confidentiality of medical records. This obligation is reinforced by Law Number 44 of 2009 concerning Hospitals, specifically Article 29 letter (h), which requires hospitals to maintain the confidentiality of patient conditions. Additionally, Law Number 17 of 2023 on Health, as the new umbrella regulation in the health sector, explicitly guarantees patients' rights to the protection of their health information and data. In the digital context, Law Number 27 of 2022 concerning Personal Data Protection (*Perlindungan Data Pribadi*/PDP Law) classifies health data as sensitive personal data that can only be processed with the explicit consent of the data owner. This provision is reinforced by Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (*Penerapan Sistem dan Transaksi Elektronik*/PP PSTE), which requires all electronic system operators, including hospitals and medical application providers, to guarantee the security, confidentiality, and integrity of electronic data. At the technical level, Minister of Health Regulation Number 24 of 2022 concerning Medical Records is the latest operational regulation governing EMR management, including data storage mechanisms, access rights, and the responsibilities of health workers in maintaining patient confidentiality (Mulyadi et al., 2020; Rizki et al., 2024).

Although the legal framework is relatively comprehensive, various studies reveal gaps in the implementation of confidentiality principles in the field. Larasati et al. (2024) found that the implementation of Minister of Health Regulation Number 24 of 2022 still faces challenges, particularly in relation to the readiness of digital infrastructure and human resource competencies. Kemalasari and Putra (2023) highlighted the weak coordination between institutions in handling EMR data leaks, while Amir (2019) pointed out the lack of legal clarity regarding the evidentiary status of EMR in malpractice litigation cases. In a global context, Szalados (2021) asserts that data leaks are increasing exponentially with medical digitization and emphasizes the importance of legal instruments such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act in the United States as models for law enforcement. In line with this, Alhomidan et al. (2025) examine the ethical dimensions of Electronic Health Records, emphasizing the need to increase patient control over their personal data through technologies such as *blockchain* and *self-sovereign* identity systems.

Health data breaches have also become an international phenomenon that provides important lessons for Indonesia. Simon and Looten (2020), in a study of 244 incidents in the French healthcare sector, found that 80% of violations were caused by weak governance systems that failed to maintain data confidentiality. Meanwhile, Ettaloui et al. (2023) showed that blockchain-based EMR systems can improve compliance with the General Data Protection Regulation (GDPR) and HIPAA through permanent digital audits and transparent access tracking. In the Indonesian context, Yanto et al (2025) highlight the increasing complexity of legal accountability in cloud-based EMR systems, where government entities and technology providers act as both data controllers and data processors.

Although these studies have examined the legal, ethical, and technological aspects of health data protection, there are important gaps that have not been widely researched (Califano, 2018; Akhmad et al., 2024). Most studies still focus on normative analysis of regulations or case studies of violations, while the aspect of harmonization between positive legal norms and medical professional ethics in the era of digitalization has not been explored in depth. Furthermore, there has been no comprehensive research mapping the relationship between technical data security standards and legal accountability mechanisms at the level of health institutions and system providers. This gap is an important area for this research to contribute to, particularly in formulating auditable governance norms that can be implemented across institutions in the context of national EMR.

Based on these findings, this study identifies two main urgencies. First, there is still a gap in technical standards and data breach notification procedures specific to the health sector. Second, there is an urgent need to align legal norms with medical professional ethics in facing the challenges of medical record digitization. Therefore, this study aims to: (1) map the applicable legal basis for regulating the confidentiality of Electronic Medical Records in Indonesia; (2) identify normative and practical gaps in its implementation; (3) formulate auditable technical and governance norms for healthcare institutions and system providers; and (4) outline mechanisms for resolving potential legal disputes in cases of health data leaks.

2. Methods

This study uses a normative legal approach, also known as doctrinal legal research, with an emphasis on the analysis of written legal norms, legal principles, and doctrines relevant to the protection of the confidentiality of Electronic Medical Records (EMR) in Indonesia (Negara, 2023). This approach was chosen because the issues under review are normative in nature and do not require the direct collection of empirical data. The main focus of this research is to identify consistency between laws and regulations, assess their effectiveness in protecting patient privacy rights, and formulate derivative norms that can be implemented operationally. To deepen the analysis, this study also includes court decisions (*jurisprudence*) as a complementary source to illustrate how the principle of confidentiality is applied and interpreted in legal disputes related to data leaks. Thus, this study not only analyzes norms textually but also examines their practical implications in a judicial context.

The object of this study includes laws and regulations that are still in force and have direct relevance to patient data protection. The primary legal materials consist of the 1945 Constitution of the Republic of Indonesia; Law Number 29 of 2004 concerning Medical Practice; Law Number 44 of 2009 concerning Hospitals; Law Number 17 of 2023 concerning Health; Law Number 27 of 2022 concerning Personal Data Protection; Law Number 1 of 2024 as the fourth amendment to the Law on Electronic Information and Transactions; Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions; and Minister of Health Regulation Number 24 of 2022 concerning Medical Records. Secondary legal materials include academic literature, previous research results,

national and international journals, and official government documents related to health data governance. Meanwhile, an analysis of court decisions (jurisprudence) was conducted to examine how judicial institutions interpret and enforce the principle of medical data confidentiality and to identify gaps in its implementation.

Legal materials were collected through library research by examining official legal documents from national databases such as the Ministry of Law and Human Rights' Legal Documentation and Information Network, the Supreme Court, and the Secretariat of the Cabinet of the Republic of Indonesia. The research process began with the identification of relevant regulations, followed by a systematic review of the main provisions governing rights and obligations in medical record management. An analysis was conducted on the vertical relationship between laws, government regulations, and ministerial regulations, as well as the horizontal relationship across sectors, particularly between the Personal Data Protection Law and the Health Law. This stage aimed to reveal inconsistencies, overlaps, and legal loopholes that could affect the effectiveness of health data protection in Indonesia.

Data were analyzed qualitatively using both legislative and comparative approaches. The legislative approach was used to assess the binding force, coherence, and relevance of legal norms related to medical record confidentiality, while the comparative approach was conducted by comparing the Indonesian data protection framework with international standards, specifically HIPAA in the United States and GDPR in the European Union as benchmarks for medical data security, accountability, and governance. The analysis results were synthesized into normative recommendations in the form of operational and auditable derivative norms to strengthen confidentiality protection in healthcare facilities and digital health systems. Through this framework, the study provides a comprehensive understanding of the legal position of medical record confidentiality within the Indonesian legal system.

3. Results and Discussion

3.1. Mapping Legal Framework for Electronic Medical Record Confidentiality

The constitutional framework regarding data confidentiality protection in Indonesia is based on Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the right of every person to protection of their personal life, honor, and dignity. This provision, when interpreted teleologically, implies recognition of the right *to informational self-determination*, which places privacy as part of human dignity. This interpretation is in line with the development of constitutional law in various countries that make the protection of health data an integral part of human rights. Sukesti et al. (2024) state that this constitutional guarantee is the normative basis for the protection of the confidentiality of electronic medical records, but its implementation is still not optimal because there is no constitutional jurisprudence that explicitly regulates digital privacy. Therefore, the state's responsibility is operational, not merely declarative, namely by establishing institutional and procedural mechanisms to protect personal health data in the entire process of digitizing health services.

At the legislative level, Law Number 29 of 2004 on Medical Practice and Law Number 44 of 2009 on Hospitals emphasize confidentiality as a professional and institutional obligation. However, the legal construct still reflects a conventional paradigm that assumes a direct relationship between doctors and patients, and has not yet fully adapted to the digital healthcare ecosystem. Hutabarat et al. (2022) assess this condition as a form of structural weakness because legal responsibility for patient data now lies more with the organizational systems that manage data electronically. As a result, breaches of confidentiality often occur not because of medical personnel errors, but due to system weaknesses, such as weak network

security, *cloud storage*, or unencrypted data transmission. This condition emphasizes the importance of integrating medical ethics and health data governance so that the principle of confidentiality is not only understood as an individual responsibility but also as an institutional obligation inherent in the health care system.

Law Number 17 of 2023 concerning Health marks an important update in the national health legal regime by affirming the right to medical data confidentiality through Article 276. Novianti and Bakhtiar (2024) emphasize that this provision places the protection of electronic medical records in the context of national health system transformation in line with the constitutional mandate on privacy. This law redefines patient confidentiality as a technology-related right, which requires privacy protection to go hand in hand with data interoperability and health system integration. However, its successful implementation depends on the effectiveness of implementing regulations in establishing clear operational standards related to consent management, data retention, and access rights. Without such technical clarity, the promised protection has the potential to be declarative without enforcement.

Furthermore, Law Number 27 of 2022 concerning Personal Data Protection (*Perlindungan Data Pribadi/*PDP Law) strengthens legal protection by categorizing health information as sensitive personal data. Its management can only be carried out based on the explicit consent of the data owner, lawful processing, and accountability from the data controller. Basani (2023) views this regulation as a form of constitutionalization of data protection, which affirms that electronic medical records are not merely administrative data, but a manifestation of individual privacy autonomy. However, the sector-neutral nature of the PDP Law creates uncertainty in the division of supervisory authority in the health sector and the potential for overlap with the provisions of the 2023 Health Law. The absence of a mandatory data breach notification mechanism and weak access control regulations have resulted in a weak preventive effect against data breaches. Therefore, harmonization between the PDP Law, the Health Law, and its implementing regulations, such as Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, is important to build a coherent legal framework, where legal obligations are in line with technological audit capabilities and institutional responsibilities.

Government Regulation Number 71 of 2019 (*Penerapan Sistem dan Transaksi Elektronik/*PP PSTE) serves as the primary foundation for data protection in electronic systems, including digital medical records. This regulation requires every electronic system operator to maintain data integrity, confidentiality, and availability through technical measures such as encryption and authentication. Mukti and Setiawan emphasize the dual value of PP 71/2019, both technologically and legally, although its technology-neutral nature has led to varying interpretations regarding adequate protection standards. Building on this general framework, sectoral regulations through Minister of Health Regulation Number 24/2022 provide the most comprehensive operational guidelines for EMR governance. These regulations govern storage, access control, and the obligation to ensure patient confidentiality. Larasati et al. (2024) and Enaizan et al. (2020) note that the implementation of role-based access and authentication reflects the principle of privacy by design. However, weak audit standards and reporting mechanisms prevent confidentiality breaches from being optimal.

Furthermore, from an enforcement perspective, Law Number 1/2024 strengthens digital evidence and criminal liability for unauthorized data disclosure. Anwar et al. (2025) assessed that this change closes the gap between civil and criminal law, but still lacks an emphasis on preventative measures such as DPIAs or security certifications. In a global context, GDPR and HIPAA serve as benchmarks for regulatory maturity through requirements for encryption, breach notification,

and independent oversight. Santoso et al. (2024) assessed that Minister of Health Regulation 24/2022 has begun to adopt these principles, although it is not yet supported by equivalent institutional mechanisms. Following the ideas of Ettaloui et al. (2023), blockchain implementation is considered capable of increasing data transparency and integrity, in line with the policy shift towards compliance by design.

Although national regulations have developed rapidly, there is still an imbalance between technological advances and the ability of regulations to adapt. Putu et al. note that the acceleration of healthcare service digitalization has not been matched by updates to technical standards, resulting in inconsistent application of the principles of privacy by design and data minimization, especially in small healthcare facilities and rural areas (Kemalasari & Putra, 2023). As a result, although Indonesia's legal framework appears comprehensive on paper, its implementation is still uneven across all levels of the healthcare system. Therefore, a meta-regulatory approach is needed that can link legal obligations to auditable measures of compliance, such as encryption standards, access logging, and periodic security audits. This approach is expected to translate normative coherence into effective and equitable legal protection for all healthcare institutions.

3.2. Identification of Normative and Practical Gaps

The regulatory framework governing EMR in Indonesia still shows strong fragmentation between sectoral and cross-sectoral legal instruments. On the one hand, Law Number 17 of 2023 concerning Health recognizes medical data confidentiality as an integral part of the right to health. On the other hand, Law Number 27 of 2022 concerning Personal Data Protection (*Perlindungan Data Pribadi/*PDP Law) defines health data as sensitive personal data subject to explicit consent and strict processing standards. The existence of these two legal frameworks has led to overlapping mandates regarding data ownership, consent mechanisms, and supervisory authority. Basani (2023) noted that without a clear harmonization mechanism, health care facilities often rely on internal policies rather than legal guidelines in determining the scope of consent or data disclosure. This normative ambiguity weakens the principle of legal certainty (*rechtssicherheit)* as guaranteed by the constitution and opens up the potential for administrative and civil liability for health institutions.

Equally important is the absence of an integrated procedural framework for breach notification and incident coordination in the event of a data leak. The PDP Law does require notification of affected individuals, but does not specifically regulate the mechanism for escalation and coordination between agencies, particularly with the Ministry of Health. Amir (2019) emphasized that this void reduces the state's ability to respond quickly to health data breach incidents, as there is no agency explicitly authorized to verify, classify, or announce incidents in the medical sector. This lack of procedural clarity creates systemic asymmetry: institutions can be held criminally liable for negligence, but do not have a well-defined compliance mechanism. As a result, reporting practices remain inconsistent; some hospitals opt for internal resolution rather than public notification, which contradicts the spirit of accountability in both the PDP Law and the Health Law.

From an institutional perspective, there is still ambiguity regarding the boundaries of responsibility between healthcare providers, the Ministry of Health, and information technology providers. The acceleration of medical system digitization has involved third parties as data management partners acting as data processors based on cooperation agreements. Day and Subekti (2024) assess that this type of partnership blurs legal accountability because the applicable regulations do not explicitly determine whether legal responsibility lies with the health facility as the principal or with the technology provider as the executor. This ambiguity contradicts the doctrine of vicarious liability, whereby the transfer of data

management does not remove the primary responsibility of healthcare institutions to ensure lawful data processing. This gap in legal accountability has the potential to threaten data integrity and patient trust, which form the ethical basis of medical confidentiality.

Beyond normative aspects, practical constraints in the healthcare ecosystem further complicate the enforcement of confidentiality principles. Larasati et al. (2024) identify infrastructure gaps, low digital literacy among healthcare workers, and the lack of comprehensive data security protocols as major obstacles to the effective implementation of EMR. These factors lead to a compliance deficit, where legal obligations exist on paper but are difficult to implement due to technological and resource limitations. Similarly, Novianti and Bakhtiar (2024) show that although EMR has been made a pillar of national health system transformation, technical audit mechanisms, data certification, and cyber security capacity building have not been systematically developed by the government. As a result, there is a widening gap between the complexity of legal norms and institutional readiness in their implementation.

These findings indicate that Indonesia's main problem is not the absence of legal recognition, but rather the coherence and enforceability of its regulatory framework. The overlap between the Health Law and the PDP Law, the absence of procedural standards for reporting violations, and the unclear boundaries of responsibility between institutions have led to fragmentation in the legal accountability system. To restore normative clarity, an integrated data governance framework is needed, which establishes clear supervisory authority, fixed procedures for handling violations, and interoperability standards in data control and processing. Without such harmonization, Indonesia's commitment to protecting medical data confidentiality risks remaining declarative and not yet realized in measurable institutional practice.

Indonesia has a broad legal framework to protect electronic medical records, but its effective implementation remains weak. Compliance with confidentiality standards varies widely, especially in rural health facilities with limited resources. Larasati et al. (2024) showed that many hospitals still use outdated infrastructure and unstable internet connections, threatening EMR security. Kemalasari and Putra (2023) added that the lack of training and digital literacy among healthcare workers weakens procedural compliance (Rizki et al., 2024), suggesting that legal compliance is understood more as an administrative obligation than an operational capability.

Institutionally, Indonesia lacks a central supervisory authority for health data, resulting in fragmented oversight. The Ministry of Health, the Ministry of Communication and Information Technology, and the BPJS Kesehatan (Social Security Agency for Health) carry out partial oversight without integrated coordination. Novianti and Bakhtiar (2024) assessed that this situation hinders accountability and slows down the handling of violations. Compared with the European Union and South Korea, which have a single authority, Indonesia needs a Health Data Protection Authority (HDPA) to shift oversight from reactive to preventative.

Technical enforcement mechanisms also remain inconsistent despite explicit legal obligations under Minister of Health Regulation Number 24 of 2022 and Government Regulation Number 71 of 2019. Basani (2023) emphasized that although regulations require the implementation of encryption, authentication, and access control, implementation remains sporadic and highly dependent on local managerial capacity. Only a small number of hospitals have implemented standard cryptographic systems such as AES-256 or maintain immutable access logs. Furthermore, the concept of Data Protection Impact Assessment (DPIA) as a risk prevention instrument has not been institutionalized routinely in Indonesian health facilities. The absence of uniform enforcement guidelines reduces the deterrent effect

of existing regulations, making legal obligations declarative without measurable compliance indicators.

These limitations are exacerbated by the absence of a continuous monitoring system and professional accountability mechanisms. Amir (2019) emphasized that medical confidentiality cannot be adequately guaranteed through written legal norms, but requires continuous institutional discipline, ethical reinforcement, and the integration of monitoring into the hospital accreditation system. However, current regulatory practices still separate data protection compliance from professional ethics audits, resulting in a fragmented accountability structure. The absence of a coordinated evaluation mechanism allows systemic weaknesses such as shared passwords or unencrypted data transmission to continue undetected. As a result, patient data protection relies more on the good faith of institutions than on enforceable procedural standards.

In general, these conditions reveal a fundamental imbalance between normative ambitions and institutional capacity. Indonesia's legal framework seeks to emulate global standards such as the GDPR and HIPAA, but its enforcement infrastructure lacks equivalent robustness. Without centralized oversight, a standardized audit system, and a professional culture that places data protection as part of institutional ethics, Indonesia's EMR confidentiality regime risks becoming mere compliance on paper without real effectiveness. Addressing these weaknesses requires regulatory reform as well as the establishment of institutional mechanisms that embed confidentiality protection as a fundamental value in national health governance (Van der Haak et al., 2003).

Court rulings in Indonesia offer critical insights into the interpretation and application of medical confidentiality principles. However, analyses of various decisions reveal that courts often prioritize procedural elements and institutional duties, overlooking substantive technical standards for data protection. This judicial pattern highlights a significant gap between intricate legal norms and the depth of court reasoning in health data breach cases. A prominent illustration is the Jakarta Administrative Court Decision Number 140/G/TF/2022/PTUN.JKT, concerning the mandatory *PeduliLindungi* app during the COVID-19 pandemic. Plaintiffs challenged the Ministry of Health and Ministry of Communication and Information Technology for large-scale health data processing without explicit consent. Although dismissed on formal grounds, the judges failed to delve into data protection specifics like encryption, audit logs, or data protection impact assessments (DPIA), leaving state accountability in mass medical data management unexamined (Neame, 2014).

Similarly, a Central Information Commission (*Komisi Informasi Pusat*/KIP) decision on Post-Immunization Adverse Events (*Kejadian Ikutan Pasca Imunisasi*/KIPI) data involved civil society seeking disclosure of vaccination side effects. The Ministry of Health denied access, citing patient privacy. While the Commission recognized partial confidentiality and mandated a consequence test before full exemption, the lack of national guidelines on anonymization or de-identification prompted blanket refusals, undermining proportionality and public access for research or policy. Inconsistencies further appear in Tangerang District Court Decision Number 1324/Pdt.G/2021/PN.Tng, where a patient sued for medical record summaries. The court ruled that physical records belong to institutions but information rights reside with patients. Yet, it referenced the revoked Minister of Health Regulation Number 269 of 2008, ignoring its replacement by Minister of Health Regulation Number 24 of 2022, exposing judicial gaps in health law updates that could inconsistent patient access to EMR.

Another facet emerges in a Bantul Religious Court divorce case, where medical records served as evidence of a party's health. Permissible under judicial exceptions for data disclosure, this lacks standardized protocols for requesting, redacting, and

securing documents, risking secondary leaks from uncontrolled access or online case publications. Thus, these jurisprudential trends underscore limited enforcement depth in Indonesia's medical data protection. Substantive issues like technical security, proportionality, and risk assessment remain absent from judicial considerations. To bolster courts as accountability guardians, key steps include: (i) enhancing judges' expertise in digital privacy and medical ethics; (ii) creating protocols for EMR evidence handling; and (iii) compiling decisions into a national health jurisprudence repository. These reforms could evolve judicial roles from mere legal interpreters to enforcers of robust health data governance.

3.3. Proposed Technical and Audit-Ready Governance Standards

Previous analysis shows that legal recognition of the confidentiality of EMR in Indonesia is normative-comprehensive, but still fragmented at the institutional level. The next step is to translate these abstract obligations into auditable and enforceable norms by integrating technical, institutional, and procedural safeguards. Based on the principles in Law Number 27 of 2022 concerning Personal Data Protection, Law Number 17 of 2023 concerning Health, and Minister of Health Regulation Number 24 of 2022 concerning Medical Records, this section proposes a structured framework covering three main areas: (1) minimum technical standards, (2) institutional and inter-agency governance mechanisms, and (3) sectoral guidelines for PDP implementation.

The core of auditable governance is the establishment of minimum technical standards that are mandatory for all health care facilities and EMR providers. Empirical and doctrinal studies show that technical security should be positioned not merely as a best practice, but as a legal obligation directly related to accountability. The application of a combination of AES-256 encryption and RSA-based digital signatures has been proven to increase the confidentiality and integrity of medical data, while ensuring verifiable authenticity during data transmission (Sundari & Retnowat, 2023). The integration of biometric authentication (e.g., fingerprints) with advanced encryption also forms a double barrier against unauthorized access. These technologies represent the minimum threshold for compliance with the principles of personal data protection rooted in Article 28G paragraph (1) of the 1945 Constitution.

Operationally, the use of AES-256 encryption, TLS 1.2 or higher communication standards, and Multi-Factor Authentication (MFA) must be mandatory for all EMR systems certified by the Ministry of Health. The implementation Of Role-Based Access Control (RBAC) ensures that healthcare workers can only access data that is absolutely necessary for their professional duties, thereby implementing the principle of least privilege in data protection law. These technical specifications are not optional accessories, but rather ethical imperatives in a digital health ecosystem that must prevent abuse at the source. These standards should be codified in ministerial technical regulations that explicitly link technical benchmarks to administrative sanctions in the event of non-compliance (Anwar et al., 2025).

Equally important is the implementation *of* immutable audit logs to record every access, change, or data export action within the EMR system. The principle of immutability, which is commonly adopted in blockchain-based healthcare systems in the European Union and the United States, provides a tamper-proof record that is essential for accountability and forensic investigation (Shingari & Mago, 2024). Encryption and continuous key rotation need to go hand in hand with real-time monitoring to detect anomalies before they escalate into breaches. Completing the data lifecycle, retention and destruction policies must be established to regulate the automatic deletion or secure archiving of patient data after it exceeds the period specified by law. This policy fulfills the objectives of privacy protection and efficiency, thereby preventing the accumulation of sensitive data that increases vulnerability to leaks.

Institutional coordination is a key factor in maintaining the resilience of health data confidentiality. The division of authority between the Ministry of Health, the Ministry of Communication and Information Technology, and the Health Data Protection Authority (*Perlindungan Data Pribadi*/PDP) often results in slow and inconsistent incident responses. Therefore, the establishment of the Joint Governance Board on Health Data Protection (JGB-HDP) is necessary as a national platform that aligns regulation formulation, compliance monitoring, and violation handling (Rizki et al., 2024). Through this tripartite framework, the roles of each institution can be clearly defined: the Ministry of Health regulates operational standards for healthcare facilities, the Ministry of Communication and Information Technology ensures cybersecurity and infrastructure certification, while the PDP Authority oversees data processing compliance and sanctions. Thus, the JGB-HDP serves as a hub that unites medical ethics, data governance, and administrative accountability.

To strengthen this mechanism, periodic compliance certification should be made a legal requirement for all healthcare facilities and EMR providers. Biennial independent audits in line with HIPAA and GDPR will ensure the implementation of encryption, access control, and data retention standards, while upholding the principle of privacy by accountability. However, because the PDP Law is still general in nature, the health sector requires specific interpretative guidelines. Therefore, the Ministry of Health and the PDP Authority should develop sectoral guidelines that include a 72-hour breach notification protocol and a Data Protection Impact Assessment (DPIA) requirement for any development or change to the EMR system, as suggested by Manurung and Harefa (2024). These guidelines will ensure that risk mitigation is carried out preventively, not reactively.

Finally, a Health Data Protection Unit (HDPU) needs to be established within the PDP Authority to specifically handle data governance in the health sector. This unit will be authorized to coordinate investigations, provide expert opinions on compliance, and liaise with the Ministry of Health during system audits or incident responses. Its mandate includes publishing annual transparency reports summarizing violation statistics, sanction decisions, and systemic vulnerabilities. This institution will elevate data protection from a merely reactive regulatory obligation to a proactive administrative discipline, closing the cycle between policy formulation, technical compliance, and public accountability. This proposed framework operationalizes confidentiality as an auditable, measurable, and enforceable standard. By combining technical prerequisites (encryption, MFA, and immutable access logging), institutional coordination (joint governance and certification), and sectoral procedural obligations (DPIA, breach reporting, and special oversight), Indonesia can move towards a data protection regime that is in line with international benchmarks. The success of EMR confidentiality protection ultimately depends not only on the accuracy of the law's formulation, but also on the willingness to integrate technology, ethics, and law into a continuous cycle of accountability.

Previous analysis shows that legal recognition of the confidentiality of EMR in Indonesia is comprehensive in a normative sense, but still fragmented at the institutional level. Therefore, steps are needed to translate abstract legal obligations into auditable and enforceable norms through the integration of technical, institutional, and procedural safeguards. Based on the principles in Law Number 27 of 2022 concerning Personal Data Protection, Law Number 17 of 2023 concerning Health, and Minister of Health Regulation Number 24 of 2022 concerning Medical Records, this section proposes a structured framework covering three main aspects, namely: (1) minimum technical standards, (2) institutional and inter-agency governance mechanisms, and (3) sectoral guidelines for the implementation of PDP.

The establishment of mandatory minimum technical standards for all health facilities and EMR providers is essential, as studies show that security is no longer merely best practice but a legal obligation tied to accountability. The use of AES-256 encryption and RSA digital signatures strengthens confidentiality and integrity, while biometric authentication combined with multilayer encryption provides enhanced protection, aligning with Article 28G paragraph (1) of the 1945 Constitution. To ensure consistent implementation, AES-256, TLS 1.2+, MFA, and role-based access control (RBAC) must be mandatory in all Ministry of Health-certified EMR systems. These specifications represent ethical and legal obligations and should be embedded in ministerial regulations with strict administrative sanctions for non-compliance.

In addition, it is important to implement immutable audit logs to record every activity of access, change, or export of data in the EMR system. This principle of immutability, as applied in blockchain-based healthcare systems in the European Union and the United States, provides a tamper-proof record that is essential for accountability and forensic investigation (Khozaimi et al., 2021). The implementation of encryption and regular key rotation must be accompanied by real-time monitoring to detect anomalies before they lead to data leaks. To complete the data lifecycle, retention and destruction policies need to be regulated so that the system automatically deletes or archives patient data after exceeding the storage period stipulated by law. This policy not only guarantees privacy but also increases efficiency and prevents the accumulation of sensitive data that could potentially lead to leaks.

3.4. Institutional and Interagency Governance Mechanisms

The effectiveness of data confidentiality protection in the health sector depends not only on technical safeguards but also on strong institutional coordination. Currently, overlapping authority among the Ministry of Health, the Ministry of Communication and Information Technology, and the Data Protection Authority (DPA) creates weak enforcement coherence. To address this, a Joint Governance Board on Health Data Protection (JGB-HDP) needs to be established through a Presidential Decree or Joint Ministerial Decree as a national forum for harmonizing regulatory drafting, monitoring compliance, and managing data breaches. Within this tripartite structure, the Ministry of Health would set operational standards for healthcare facilities, Kominfo would oversee cybersecurity and infrastructure certification, and the PDP Authority would supervise data processing compliance and sanctions. Establishing the JGB-HDP will create a unified ecosystem that links medical ethics, data governance, and administrative accountability.

In addition to coordination, compliance certification must be enforced for all healthcare facilities and EMR providers through periodic independent audits that verify encryption, access control, and retention policies. This approach aligns with HIPAA and GDPR, where certification functions as both oversight and public assurance, implementing the principle of privacy by accountability. To complement this, sectoral guidelines for PDP implementation must be jointly formulated by the Ministry of Health and the PDP Authority, including strict breach notification protocols requiring reports within 72 hours. Furthermore, every healthcare institution must conduct a Data Protection Impact Assessment (DPIA) before adopting or altering EMR systems, supported by standardized DPIA templates and mitigation strategies prepared by the Data Protection Authority.

Furthermore, a Health Data Protection Unit needs to be established under the Data Protection Authority, specifically responsible for overseeing data governance in the health sector (Kemalasari & Putra, 2023). This unit will be authorized to coordinate investigations, provide legal and technical opinions on compliance, and partner with the Ministry of Health in system audits or incident handling. The HDPU's mandate also includes the publication of annual transparency reports

containing statistical data on violations, sanction decisions, and systemic vulnerability mapping. Thus, health data protection will be elevated from a mere reactive legal obligation to a proactive administrative discipline that links policy, implementation, and public accountability.

This proposed framework makes confidentiality protection an auditable, measurable, and enforceable standard. Through a combination of minimum technical standards (encryption, MFA, and immutable access logging), institutional coordination (joint governance and certification), and sectoral procedural obligations (DPIA, violation reporting, and special supervision), Indonesia can move towards a health data protection regime that is in line with international standards. Ultimately, the success of EMR confidentiality protection depends not only on the completeness of legal norms but also on the willingness to integrate technology, ethics, and law into a sustainable cycle of accountability.

4. Conclusion

This study concludes that the confidentiality of EMR in Indonesia has a strong constitutional and statutory foundation, yet its implementation remains inconsistent due to fragmented institutional authority, regulatory overlaps, and uneven technical capacity. Building from these findings, the main empirical insight is that confidentiality protections fail not because of normative gaps, but because operational readiness, ranging from infrastructure to human resources, has not kept pace with legal mandates. Consequently, the practical implication is the urgent need for auditable governance mechanisms, including minimum encryption standards, multi-factor authentication, tamper-proof access logs, and mandatory breach reporting supported by a joint supervisory board and sector-specific Personal Data Protection guidelines. At the theoretical level, these findings emphasize that EMR confidentiality must be understood not merely as a legal obligation but as an integrated socio-technical system in which law, ethics, and digital architecture mutually reinforce one another.

However, this study is limited by its reliance on secondary sources and the absence of empirical field data from health facilities, which constrains the depth of analysis regarding real-world compliance challenges. Therefore, future research should incorporate multi-site case studies, institutional mapping, and technical audits to better capture the variability of EMR practices across regions. In addition, comparative studies with jurisdictions that have mature data-protection ecosystems could offer insights for refining Indonesia's regulatory model.

References

Akhmad, T. R., Pranadita, N., & Machmud, S. (2024). Legal protection of patients from leakage of electronic medical records data is reviewed from Law Number 27 of 2022 Concerning Personal Data Protection and Law Number 17 of 2023 Concerning Health. *International Journal of Asia Pasific Collaboration*, *2*(3), 45–56.

Alhomidan, Z. S., Albaqami, N. M., Alshehri, A. A., Aldubaib, A. A., Alsuwailem, A. B., & Al Ghadam, K. F. (2025). Confidentiality in the era of electronic health records: Ethical challenges and solutions. *International Journal of Community Medicine and Public Health*, *12*(4), 670–682.

Amir, N. (2019). Legal protection of patient data confidentiality electronic medical records. *SOEPRA Jurnal Hukum Kesehatan*, *5*(2), 198–208.

Anwar, T. M., Tambun, J. G., & Jaeni, A. (2025). Juridical analysis of the misuse of electronic medical records in the perspective of the electronic information and transaction law. *Pranata Hukum*, *20*(1), 26–36.

Basani, C. S. (2023). Legal protection of patient's electronic medical record: Indonesian legal perspective. *Dialogia Iuridica*, *15*(1), 94–112.

Califano, L. (2018). The electronic health record (EHR): Legal framework and issues about personal data protection. *Pharmaceuticals Policy and Law*, *19*(3–4), 141–159.

Day, S. A. S., & Subekti, R. (2024). Pertanggungjawaban penyedia sistem rekam medis elektronik dari partner system terhadap kebocoran data. *Demokrasi: Jurnal Riset Ilmu Hukum, Sosial dan Politik*, *1*(3), 92–101.

Enaizan, O., Zaidan, A. A., Alwi, N. M., Zaidan, B. B., Alsalem, M. A., Albahri, O. S., & Albahri, A. S. (2020). Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health and Technology*, *10*(3), 795–822.

Ettaloui, N., Arezki, S., & Gadi, T. (2023). An overview of blockchain-based electronic health records and compliance with GDPR and HIPAA. *Data and Metadata*, *2*(1), 166-178.

Hutabarat, D. T. H., Zebua, R., Sitorus, R. A., Subakti, F. A., Ramadhani, H., Mangunsong, J., ... & Sahdan, P. (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*, *1*(4), 59–68.

Jakarta State Administrative Court. (2020). *State administrative court decision* (Decision No. 140/G/TF/2020/PTUN.JKT).

Kemalasari, N. P. Y., & Putra, I. P. H. S. (2023). Protection of medical record data as a form of legal protection of health data through the Personal Data Protection Act. *Journal of Digital Law and Policy*, *2*(3), 111–118.

Khozaimi, A., Putro, S. S., & Yaqin, A. (2021). Improve the performance and security of medical records using fingerprint and advance encryption standart. In *Proceedings of International Conference on Health Informatics, Medical, Biological Engineering, and Pharmaceutical* (pp. 285–290). Setúbal: Scitepress.

Komalasari, R., & Mustafa, C. (2023). Electronic evidence in the healthy justice system: Reimagined. *Jurnal Hukum dan Peradilan*, *12*(3), 547–580.

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.

Manurung, K. H., & Harefa, B. (2024). The validity of electronic evidence and its relation to personal data protection. *Jurnal Daulat Hukum*, *7*(4), 455–472.

Mendelson, D. (2017). Legal protections for personal health information in the age of Big Data—A proposal for regulatory framework. *Ethics, Medicine and Public Health*, *3*(1), 37–55.

Mulyadi, D., Danil, E., Chandrawila, W., & Warman, K. (2020). Medical negligence dispute settlement in Indonesia. *Indian Journal of Forensic Medicine & Toxicology*, *14*(4), 7890–7897.

Neame, R. L. (2014). Privacy protection in personal health information and shared care records. *Journal of Innovation in Health Informatics*, *21*(2), 84–91.

Negara, T. A. S. (2023). Normative legal research in Indonesia: Its origins and approaches. *Audito Comparative Law Journal (ACLJ)*, *4*(1), 1–9.

Novianti, & Bakhtiar, H. S. (2024). Implementation of electronic medical record system in Indonesia viewed from the perspective of legal certainty. *International Journal of Engineering Business and Social Science*, *2*(4), 1114–1122.

Rizki, P. R., Arawinda, S. H., & Widhanarti, H. (2024). Juridical analysis on infringement against patients' electronic medical records at telemedicine services based on Indonesian regulation. *International Journal of Multidisciplinary Research and Analysis*, *7*(12), 42–61.

Santoso, A. P. A., Soraes, D., Gegen, G., & Astuti, O. A. S. (2024). Ethics and law of using blockchain technology for electronic health records in Indonesia. In *Proceeding of International Conference on Science, Health, and Technology* (pp. 97–104).

Shingari, N., & Mago, B. (2024). The importance of data encryption in ensuring the confidentiality and security of financial records of medical health. *2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)* (Vol. 2, pp. 1–6). New York: IEEE.

Simon, M., & Looten, V. (2020). Description of data breaches notifications in France and lessons learned for the healthcare stakeholders. In *Integrated citizen centered digital health and social care* (pp. 192–196). Amsterdam: IOS Press.

Sukesti, I., Sutrisno, E., & Indraswari, S. P. (2024). Legal study of electronic medical records for the protection of patient rights. *Hermeneutika: Jurnal Ilmu Hukum*, *8*(2), 223–233.

Sundari, E., & Retnowati, A. (2023). The limits access of medical records in Indonesia and a broader propose to support patients in malpractice claims. *Journal of Law and Sustainable Development*, *11*(12), 26-36.

Szalados, J. E. (2021). Medical records and confidentiality: Evolving liability issues inherent in the electronic health record, HIPAA, and cybersecurity. In *The medical-legal aspects of acute care medicine: A resource for clinicians, administrators, and risk managers* (pp. 315–342). Springer International Publishing.

Tangerang District Court. (2021). *Civil case decision* (Decision No. 1324/Pdt.G/2021/PN Tng).

Van der Haak, M., Wolff, A. C., Brandner, R., Drings, P., Wannenmacher, M., & Wetter, T. (2003). Data security and protection in cross-institutional electronic patient records. *International Journal of Medical Informatics*, *70*(2–3), 117–130.

Yanto, O., Putri, K. A. R., & Prananingrum, D. H. (2025). Rekam medis elektronik berbasis cloud computing: Pertanggungjawaban hukum akibat kebocoran data pasien. *Widya Yuridika: Jurnal Hukum*, *8*(1), 20–32.

Acknowledgment
We gratefully acknowledge the contributions of individuals who supported the completion of this article.

Funding Information
This research did not receive any funding.

Conflict of Interest Statement
The authors declare that there is no conflict of interest.

Ethical Approval and Originality Statement
Ethical approval was obtained for this study. The manuscript represents original work and has not been previously published, nor is it under consideration by another journal.

Data Disclosure Statement
The data that support the findings of this study are available from the corresponding author upon reasonable request.