E-ISSN 3048-152X Vol. 3, Issue 1 (2025)
Doi: https://doi.org/10.37899/mjdpp.v3i1.337

Moccasin Journal De Public Perspective

Legal Protection of Patient Privacy Rights in the Use of Electronic Medical Records in Indonesian Hospitals

Febriyani Masdar[1], Rukyyah Assam[1]

[1]*Faculty of Law, Universitas YARSI, Central Jakarta, Indonesia*

**Corresponding Author: Febriyani Masdar*
E-mail: fbtni@gmail.com

Article Info

Article History:
Received: 19 January 2026
Revised: 23 February 2026
Accepted: 12 March 2026

Keywords:
Patient Privacy Rights
Electronic Medical Records
Health Law
Personal Data Protection
Hospital Regulation

Abstract

The rapid adoption of electronic medical records in Indonesian hospitals has transformed healthcare delivery while simultaneously raising significant concerns regarding the protection of patient privacy rights. This study aims to analyze the adequacy of the legal framework governing patient privacy in the context of electronic medical records and to assess whether existing regulations provide effective and enforceable protection. The study employs normative legal research through statutory, conceptual, and analytical approaches to examine health law and personal data protection regulations relevant to digital medical records. The findings indicate that Indonesian law formally recognizes patient privacy as a fundamental legal and ethical principle. Nevertheless, regulatory provisions remain largely general and were originally designed for paper based medical records, resulting in limited applicability to digital systems. The lack of harmonization between health law and personal data protection law generates legal uncertainty, particularly regarding consent, data security standards, and the allocation of liability among healthcare institutions and technology providers. The study also finds that enforcement mechanisms tend to be reactive and institution centered, offering limited access to effective remedies for patients.

INTRODUCTION

The rapid digital transformation of health systems has fundamentally reshaped the way medical information is created, stored, and exchanged. One of the most significant developments in this transformation is the adoption of Electronic Medical Records (EMRs), which are widely promoted for their potential to improve efficiency, continuity of care, and clinical decision making. EMRs enable health professionals to access patient data more quickly, reduce duplication of medical tests, and enhance coordination across health services. However, alongside these benefits, the digitization of medical records has raised serious legal and ethical concerns, particularly regarding the protection of patient privacy and personal data. Scholars have emphasized that health data constitute one of the most sensitive categories of personal information, requiring a high level of legal protection to prevent misuse, unauthorized access, and data breaches (Rumbold & Pierscionek, 2017; Kruse et al., 2018).

Globally, concerns about patient privacy in digital health systems have intensified as incidents of data leakage, cyberattacks, and improper data sharing have become more frequent. Studies indicate that weaknesses in legal frameworks, governance mechanisms, and institutional practices often undermine the confidentiality of electronic health information (Fernández-Alemán et al., 2013; Appari & Johnson, 2010). In response, many countries have enacted specific data protection regulations, such as the General Data Protection Regulation in the European Union and the Health Insurance Portability and Accountability Act in the United States, to safeguard patient rights. These regulatory developments underscore the recognition that technological advancement in healthcare must be accompanied by robust legal instruments to ensure trust and accountability in health systems (European Commission, 2018; McGraw, 2013).

Despite global progress, the implementation of EMRs in developing and middle income countries presents distinct challenges. In such contexts, digital health reforms often outpace the development of comprehensive legal and institutional safeguards. Indonesia represents a compelling case in this regard. The Indonesian government has actively promoted health information system digitalization as part of broader health sector reform, including the integration of EMRs in hospitals. While these initiatives aim to improve service quality and administrative efficiency, they simultaneously expose patients to new privacy risks, particularly in the absence of mature enforcement mechanisms and uniform standards across healthcare institutions. Existing studies suggest that legal awareness among healthcare providers and patients regarding data protection obligations remains uneven, creating gaps between normative regulation and actual practice (Sutanto et al., 2021; Pratama & Aziz, 2022).

The central research problem addressed in this study concerns the adequacy of legal protection afforded to patient privacy rights in the use of EMRs in Indonesian hospitals. Although Indonesia has enacted several laws and regulations relevant to health data protection, including legislation on health services, medical practice, and personal data protection, questions remain regarding their coherence, effectiveness, and enforceability in the specific context of electronic medical records. Prior research indicates that fragmented regulation and overlapping institutional authority can weaken legal certainty and complicate compliance for healthcare providers (Butt, 2014; Lindsey, 2018). Consequently, patients may face heightened risks of privacy violations without clear mechanisms for legal redress.

A common solution proposed in the literature is the strengthening of legal frameworks through comprehensive data protection legislation and sector specific regulations for health information systems. Scholars argue that clear definitions of personal health data, explicit consent requirements, and strict obligations for data controllers are essential to ensure meaningful privacy protection (Bennett & Raab, 2018; Greenleaf, 2019). Additionally, effective enforcement through independent supervisory authorities and proportional sanctions is widely regarded as a critical component of legal protection. However, the mere existence of formal rules does not automatically translate into effective protection, particularly in institutional environments characterized by limited capacity and uneven compliance.

Previous research studies have emphasized the necessity of integrating privacy-by-design concepts into electronic medical record (EMR) systems, as well as the overall governance framework of medical institutions. In this approach, legal and ethical concerns are directly incorporated into the technological system, and they can include access controls, audit trails, and data minimisation procedures (Cavoukian, 2011; Mittelstadt et al., 2016). As noted in empirical research, it is also important to have institutional policies and standard operating procedures that define what the healthcare personnel do and should do as far as handling of

electronic patient data are concerned. Medical staff training programs and awareness campaigns are often mentioned as an inseparable supplement to statutory regulation since the causes of data breach in clinical practices are the human error and negligence (Kruse et al., 2017).

Another strand of literature available to us as supplementary literature is that which focuses on patient-based legal protections, which highlights informed consent, transparency, and patient control over personal health information. Studies suggest that patients are entitled to clear and understandable information about the collection, storage, sharing, and use of their data, including their secondary use in a study or insurance claims (Hall and McGraw, 2014; Kalkman et al., 2019). The issue of the interoperability of data and the presence of multiple data consumers also complicate the process of ensuring a meaningful consent in the context of the EMR. The legal scholars, therefore, believe that the creation of clear standards of consent and available grievance mechanisms should be put in place so that patients can enforce their rights without struggles whenever violations happen.

Despite the existence of useful information in the literature that supports the relevance of legal and technical interventions to ensure patient privacy, a significant gap still exists with regard to the context-editing work on the functionality of these safeguards through legal mechanisms in the work of most countries, including Indonesia. Majority of the previous research either takes a comparative international approach or dwells much on technical side of health information security giving minimal questioning on the interaction between national laws, hospital operations and patient rights. In addition, a lack of systematic studies about intersection between the recent personal data protection reforms in Indonesia and the regulations of the health sectors on the EMRs is apparent. This gap is a hindrance to a well-rounded explanation of the extent to which the existing legal provisions provide sufficient and consistent safeguards to patient privacy in hospitals.

It is on this background that the current study aims to review the legal issue of protecting patient privacy during the use of electronic medical records in the hospitals in Indonesia. Particularly, the research aims at evaluating the current regulatory base, determining normative and practical gaps, and assessing the overall ability to uphold the rights to patient privacy in the digital health context. The originality of the present study is in the form of integrative legal research that places the EMR implementation into the context of changing data protection regime and health-law regime in Indonesia. Focusing on hospital-based EMR practices, the study will be beneficial to the field of law and policy debate on improving patient privacy protection in the age of digital healthcare and provide viable suggestions to legislators, healthcare facilities, and practitioners.

METHODS

Research Design and Legal Approach

This study employed a normative legal research design with a doctrinal approach to examine the legal protection of patient privacy rights in the use of electronic medical records in Indonesian hospitals. The research focused on analyzing legal norms principles and doctrines governing personal data protection and health information confidentiality. A conceptual approach was also applied to understand how patient privacy rights are constructed within health law and data protection frameworks as reflected in existing regulations and scholarly interpretations.

Statutory and Conceptual Framework

The statutory framework of this study was grounded in Indonesian laws and regulations relevant to patient privacy and electronic medical records including health law hospital law and personal data protection regulations. These statutory

instruments were analyzed in conjunction with conceptual frameworks derived from international human rights law and health law literature that emphasize privacy confidentiality and data security as fundamental patient rights. This combination allowed for a systematic evaluation of legal consistency and normative adequacy.

Sources of Legal Materials

Legal materials used in this study consisted of primary secondary and tertiary sources. Primary legal materials included statutes government regulations ministerial regulations and official policy documents related to electronic medical records and patient data protection. Secondary legal materials comprised peer reviewed journal articles books legal commentaries and reports from international organizations discussing health data governance and privacy protection. Tertiary materials such as legal dictionaries and encyclopedias were used to clarify key legal concepts and terminology.

Data Collection Techniques

Data collection was conducted through systematic document review of relevant legal texts and scholarly publications. Statutory documents were collected from official government repositories while academic literature was obtained from reputable international journal databases. The selection of materials followed relevance credibility and recency criteria to ensure that the analysis reflected current legal developments and scholarly debates on patient privacy and electronic health information systems.

Methods of Legal Analysis and Interpretation

The study applied qualitative legal analysis methods including statutory interpretation systematic interpretation and comparative interpretation. Statutory interpretation was used to examine the meaning and scope of legal provisions governing electronic medical records and patient privacy. Systematic interpretation was employed to assess coherence between health regulations and data protection laws. Comparative interpretation drew insights from international standards and foreign legal practices to contextualize Indonesia's regulatory approach.

Integration of Health Law and Data Protection Law

An integrative analytical method was adopted to examine the intersection between health law and personal data protection law. This approach enabled the study to identify overlapping obligations conflicts and normative gaps in regulating electronic medical records. By analyzing these legal domains together the research highlighted how fragmented regulation may affect the effective protection of patient privacy rights in hospital settings.

Although primarily normative this study incorporated supporting empirical references from previous research reports and case studies to contextualize legal findings. Empirical literature on electronic medical record implementation data breaches and patient trust was used to illustrate practical implications of legal norms and to strengthen the relevance of normative analysis to real world healthcare practices.

RESULTS AND DISCUSSION

Normative Recognition of Patient Privacy in Indonesian Health Law

The findings indicate that Indonesian health law explicitly recognizes patient privacy as a foundational legal principle situated within the broader constitutional and statutory framework of the right to health. This recognition reflects the understanding that access to healthcare services must be accompanied by safeguards protecting the confidentiality of personal and medical information.

Legislative instruments governing healthcare practice consistently underscore that the protection of medical data is not merely procedural but constitutes an essential component of lawful medical service delivery. In this regard, confidentiality is positioned as both an ethical commitment rooted in professional medical standards and a binding legal obligation imposed upon healthcare providers. Such dual characterization reinforces the normative weight of privacy within the healthcare system and affirms its centrality in regulating the relationship between patients and medical professionals.

Moreover, the normative construction of patient privacy in Indonesian health law demonstrates alignment with international human rights principles, which conceptualize privacy as intrinsically connected to human dignity, autonomy, and personal integrity. Within global human rights discourse, privacy is regarded not simply as protection from intrusion but as a precondition for the meaningful exercise of individual freedom and self-determination. By embedding confidentiality within the right to health, Indonesian legal instruments implicitly acknowledge that the therapeutic relationship depends upon trust, and that trust is sustained through assurance that sensitive health information will not be improperly disclosed. This normative coherence situates Indonesian regulation within a broader transnational legal framework that treats medical confidentiality as a cornerstone of rights-based healthcare governance.

However, notwithstanding this formal acknowledgment, the articulation of patient privacy within statutory provisions remains predominantly abstract and declaratory in nature. Legislative texts tend to formulate privacy protection in broad and general terms, emphasizing duties of confidentiality without elaborating on specific parameters, operational standards, or technical safeguards. The absence of detailed definitional clarity limits the capacity of these provisions to function as concrete regulatory tools. Rather than providing explicit guidance on how privacy must be preserved in contemporary healthcare infrastructures, the law often reiterates normative commitments at a principled level. Consequently, privacy is framed more as a value to be upheld than as a set of clearly delineated compliance requirements.

This abstraction becomes particularly significant in the context of electronic medical record systems and digital health technologies. As healthcare delivery increasingly relies on digital platforms, data storage systems, and inter-institutional information exchange, the risks associated with unauthorized access, data breaches, and secondary use of medical information become more complex and technologically mediated. Yet the existing legal framework does not consistently translate its general commitment to confidentiality into operational standards tailored to digital environments. Without explicit technical benchmarks such as data encryption requirements, access control protocols, audit mechanisms, or retention limitations the legal protection of privacy may struggle to address the practical realities of electronic data management (Omotunde & Ahmed, 2023; Renuka et al., 2025; Ngesa, 2024; Razi et al., 2025; Isibor, 2024).

The findings further reveal that the lack of detailed normative guidance generates interpretative flexibility at the institutional level. In the absence of comprehensive statutory directives, healthcare institutions frequently rely on internally developed policies, standard operating procedures, and administrative guidelines to define and implement privacy protections. While such institutional autonomy may allow for contextual adaptation, it simultaneously introduces variability in interpretation and application. Different hospitals, clinics, or regional health authorities may adopt divergent standards concerning data access, disclosure practices, and information security measures, depending on their administrative capacity and technological resources.

This variability poses potential challenges to legal certainty and the uniform protection of patient rights. When privacy safeguards depend heavily on institutional discretion rather than standardized legal requirements, the level of protection afforded to patients may differ significantly across regions and healthcare facilities (Chowdhury & Ravi, 2022). Such inconsistency risks undermining the principle of equality before the law and may weaken public confidence in the healthcare system. Therefore, although Indonesian health law normatively affirms patient privacy as a core legal principle, the absence of detailed and operationally precise regulations may limit the effectiveness of its implementation, particularly within rapidly evolving digital healthcare contexts.

Regulatory Adaptation to Electronic Medical Records

The analysis demonstrates that Indonesian health regulations have yet to fully accommodate the structural transformation generated by the implementation of electronic medical records (EMRs). Much of the existing legal architecture governing medical documentation was formulated within a paradigm centered on paper-based recordkeeping. Consequently, regulatory provisions tend to emphasize physical custody, restricted manual access, and the tangible safeguarding of documents within institutional premises. These assumptions reflect a traditional understanding of medical data as static and geographically confined. However, such a framework is increasingly misaligned with contemporary healthcare systems in which information is digitized, stored on servers, transmitted across networks, and potentially accessed through interoperable platforms. The persistence of a paper-based regulatory mindset therefore creates a conceptual gap between legal norms and technological realities.

Electronic medical records fundamentally alter the nature of medical information management by enabling rapid data replication, remote accessibility, and cross-institutional integration. Unlike physical files, digital records can be duplicated instantaneously, transmitted across jurisdictions, and integrated into broader health information systems. While these capabilities enhance efficiency and continuity of care, they simultaneously generate new categories of risk, including unauthorized remote access, large-scale data breaches, system vulnerabilities, and unauthorized secondary use of data (Asha et al., 2024). Despite these evolving risks, the regulatory framework does not provide comprehensive guidance on critical technical dimensions such as cybersecurity protocols, encryption standards, authentication mechanisms, audit trails, or structured data lifecycle management. The absence of such provisions indicates that the law has not yet internalized the systemic implications of digital transformation.

This regulatory lag diminishes the effectiveness of the legal system as an instrument of risk mitigation and preventive governance. In digital environments, privacy protection depends not only on ethical commitments but also on technologically embedded safeguards. Without explicit legal requirements mandating minimum security standards or compliance benchmarks, healthcare providers may adopt heterogeneous and potentially inadequate protective measures (Panahi, 2025; Ayo-Farai et al., 2023). As a result, legal norms that were originally designed to secure confidentiality in physical settings may lack enforceability when confronted with sophisticated cyber threats and complex digital infrastructures. The law's preventive function is therefore weakened, as it does not systematically anticipate or regulate the operational vulnerabilities inherent in electronic record systems.

The findings further indicate that governmental promotion of digital health innovation has progressed more rapidly than the evolution of corresponding legal safeguards. Policy discourse frequently emphasizes the benefits of digitalization, including administrative efficiency, improved data accuracy, integrated service

delivery, and enhanced continuity of care. While these objectives are normatively desirable and operationally advantageous, the parallel development of comprehensive regulatory standards has not kept pace. This temporal imbalance creates a situation in which technological expansion occurs in a relatively underregulated environment, thereby increasing exposure to privacy risks. In effect, digital transformation is institutionally encouraged, yet the normative infrastructure required to secure patient rights remains comparatively underdeveloped.

Such an imbalance suggests that the trajectory of digital health development has been shaped to a significant extent by technological optimism rather than by systematic legal preparedness. The emphasis on modernization and innovation may inadvertently overshadow the necessity of embedding robust data protection frameworks within health governance structures. When digital systems are introduced without sufficiently detailed regulatory oversight, privacy protection becomes reactive rather than proactive, addressing breaches after their occurrence rather than preventing them through anticipatory design. This dynamic raises concerns regarding the sustainability and legitimacy of digital health reforms, particularly in light of the heightened sensitivity of medical information (Mubarak, 2026).

Accordingly, the results underscore the urgency of regulatory reform that transcends symbolic endorsement of digital health initiatives. Reform efforts should aim to articulate substantive, technically informed legal standards specifically tailored to electronic medical record systems. Such standards would ideally define minimum cybersecurity requirements, clarify accountability mechanisms, regulate data access hierarchies, and establish clear parameters for data retention and deletion. By integrating these elements into the statutory framework, the law can evolve from a declaratory affirmation of confidentiality into a comprehensive regulatory instrument capable of governing digital healthcare infrastructures effectively and consistently.

Interaction Between Health Law and Personal Data Protection Law

The results indicate that the personal data protection framework in Indonesia establishes a more systematic and conceptually coherent normative structure for safeguarding patient information than sector-specific health regulations. Unlike traditional health law provisions that primarily articulate confidentiality as a professional duty, personal data protection law formulates privacy protection through clearly defined legal principles governing data processing activities. Foundational principles such as lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability provide structured benchmarks against which the legality of electronic medical record (EMR) practices can be evaluated. These principles shift the regulatory focus from mere non-disclosure toward comprehensive governance of the entire data lifecycle, encompassing collection, processing, storage, dissemination, and deletion.

Moreover, the rights-based orientation embedded in personal data protection law strengthens the normative position of patients as data subjects rather than passive recipients of medical services. By recognizing enforceable rights such as the right to access personal data, the right to rectification, and the right to be informed about data processing activities the legal framework enhances individual autonomy and procedural fairness. In the context of EMR systems, this rights-based approach introduces mechanisms through which patients may exercise oversight over their own medical information (Alhasan, 2025). As a result, privacy protection is reframed not only as an institutional obligation but also as a legally protected entitlement grounded in individual dignity and informational self-determination.

However, despite the relative normative sophistication of data protection law, its interaction with health law remains institutionally and doctrinally fragmented. The

two legal regimes operate largely in parallel, each with its own conceptual foundations, enforcement structures, and regulatory objectives. Health law primarily emphasizes professional ethics, service delivery standards, and public health governance, whereas data protection law adopts a broader cross-sectoral perspective focused on personal data processing across industries (Galvin et al., 2025). The absence of explicit coordination mechanisms or hierarchical clarification between these regimes creates uncertainty regarding their respective scopes of application, particularly in cases involving medical data breaches or unauthorized disclosures within digital health systems.

This fragmentation becomes especially problematic when legal disputes arise concerning responsibility and applicable standards. It may be unclear whether a medical data breach should be adjudicated predominantly under sector-specific health regulations, which emphasize confidentiality as a professional duty, or under general data protection statutes, which impose structured compliance obligations and potential administrative sanctions. Without clear normative guidance on the relationship between lex specialis (sector-specific regulation) and lex generalis (general data protection law), courts and regulators may interpret the applicable framework inconsistently. Such ambiguity risks weakening legal certainty and complicating enforcement strategies.

The findings further suggest that overlapping obligations derived from both regimes may generate compliance challenges for healthcare institutions. Hospitals and other medical facilities are required to adhere simultaneously to health sector regulations governing medical records and to cross-sectoral data protection requirements governing personal data processing. While these frameworks are conceptually complementary, their practical requirements may differ in terminology, reporting obligations, documentation standards, and accountability mechanisms. In the absence of harmonized guidelines, healthcare administrators may encounter difficulties in reconciling these obligations within internal governance structures.

This regulatory ambiguity carries the risk of inconsistent enforcement and selective compliance. Institutions with greater administrative capacity may attempt to integrate both frameworks comprehensively, whereas others may prioritize one regime over the other due to limited resources or interpretative uncertainty. Such uneven implementation could undermine uniform protection of patient rights and erode public trust in digital health systems. Therefore, while personal data protection law provides a stronger and more structured normative foundation for safeguarding patient information, the lack of coherent integration with health law highlights the need for systematic harmonization to ensure clarity, consistency, and effective enforcement within electronic medical record governance.

Allocation of Legal Responsibility Among Stakeholders

The analysis indicates that hospitals occupy a central institutional position as the primary custodians of electronic medical records (EMRs), thereby bearing principal responsibility for data governance, storage, and security. Within the prevailing regulatory structure, hospitals are treated as the entities that exercise overarching control over patient records, including decisions related to data collection, retention, and access authorization. Healthcare professionals, such as physicians and nurses, are primarily assigned duties grounded in professional confidentiality and ethical conduct, reflecting long-stading medical norms regarding the protection of sensitive information (Dove, 2023; Alodhialah, 2025). Meanwhile, technology providers and system vendors are generally conceptualized as auxiliary or supporting actors that supply infrastructure, software, or technical maintenance services. This allocation of roles reflects a traditional hierarchical model of responsibility in which the healthcare

institution functions as the central authority, and other actors operate under its supervision.

Nevertheless, despite such formal arrangement, there is empirical evidence that statutory provisions do not provide a holistic and expressive delineation of the limits of liability between the concerned stakeholders. The regulatory framework generally describes generic obligations, e.g. the maintenance of confidentiality or the promise of data security, without stating the way in which the responsibility should be divided when there are several participants in processing and management of electronic medical records (EMRs). The chain of responsibility is even more complex in digitally networked settings where data storage can be located on cloud-based systems, the maintenance of the system can be outsourced, and the third-party application can be merged with hospital systems. Still the law does not always provide a clear understanding of how the liability must be allocated in the cases of shared control or delegated technical functions.

Such ambiguity is especially relevant when it comes to data breaches due to technological errors, cybersecurity weaknesses, or mistakes in third-party applications. In situations whereby there has been a breach due to a software defect, insufficient encryption procedures, or unauthorised third-party access, it is hard to tell whether a breach lies with the hospital, data controller, or the technology provider, who designed and maintained the system. Such a situation makes the accountability system more complicated due to the spread of responsibility, as the affected patients might face the procedural and evidentiary barriers to determining the party that is legally guilty. Furthermore, deterrence is reduced in uncertain or divided liability because no single party might be willing to take full responsibility of taking strong preventive mechanisms.

The lack of statutory assignment of responsibility also produces considerable ramifications of the relationships of the contract between the hospitals and the vendors of the technology. Practically, the related task of data protection and breach management is often negotiated privately by means of a contractual relationship, such as service-level agreement or indemnification provision. The absence of clearly set legislative requirements on minimum non-delegable requirements, means that hospitals can either seek to transfer large segments of risk to the system providers, or vendors can seek to limit the risk through restrictive contractual language. Allocation of contractual risks like these is usually not guided by the desire to protect the rights of patients as a public interest factor but by commercial factors.

The privatisation of risk management also poses normative issues of patient right in the EMR systems. In the case where the liability is mainly decided by the means of private agreements, the goals of the law, including the need to provide a successful remedy to the patients and the need to have equal data protection standards, can be subject to cost-efficiency or risk-distribution approaches. Without a set of regulations, contractual relationships are likely to be poor in indicating the relative control and power of each party in the medical data. In turn, it might lead to barriers in the redress that patients may face in case the responsibility is shared among various entities with complicated contractual relations.

In line with this, the results confirm the need to further legalize and better define the responsibility of EMR ecosystem participants. Regulation reform must express varied but aligned liability provisions depending on the level of control, decision-making power, and technical impact of every actor on data processing processes. The law can make it accountable by ensuring that all the involved parties are accountable based on their functional contribution by ensuring creating clear accountability structures that might be seen as differentiating between data controllers, data processors and joint controllers. This explanation would help create a higher level of

legal clarity, deterrence, and protect the rights of patients in further complicated digitized healthcare settings.

Legal Construction of Patient Consent in Digital Contexts

The results indicate that patient consent continues to function as a foundational legal basis for the collection and use of medical information within the Indonesian healthcare framework. Consent is traditionally conceptualized as a manifestation of patient autonomy, reflecting the individual's voluntary agreement to medical examination, treatment, and the associated processing of personal health data. Within the therapeutic relationship, consent embodies trust, mutual respect, and recognition of the patient's right to make informed decisions concerning their own body and personal information. This normative understanding is deeply rooted in established principles of medical ethics and health law, which regard informed consent as both a moral obligation and a legal prerequisite for lawful medical intervention (Partama & Putra, 2025).

In conventional clinical settings, consent is typically obtained in relation to specific diagnostic or therapeutic procedures, with an implicit understanding that relevant medical information will be recorded and used for treatment purposes. This model presumes a relatively limited and context-bound use of data, primarily confined to the immediate healthcare interaction. However, the introduction of electronic medical records (EMRs) fundamentally alters the scope and temporal dimension of data processing. Digital systems enable not only continuous storage and retrieval of patient information but also secondary processing activities, such as administrative analysis, quality control, system integration, and inter-institutional data exchange (AlSalamah, 2025). These expanded functionalities challenge the adequacy of traditional consent models, which were designed for discrete and relatively contained uses of information.

Existing regulatory provisions do not sufficiently articulate how consent should operate within these digitally mediated conditions. While laws affirm the necessity of patient approval for medical procedures and data disclosure, they rarely address the complexities introduced by automated processing, long-term storage, algorithmic analysis, or cross-platform interoperability. The absence of detailed standards concerning the scope, duration, and revocability of consent in electronic environments creates ambiguity regarding the extent to which initial consent extends to subsequent or secondary uses of medical data. As a result, the legal framework may inadequately capture the dynamic and ongoing nature of data flows within digital health systems.

The findings further suggest that, in practice, consent is frequently reduced to a one-time procedural requirement, typically documented through standardized forms signed at the point of hospital admission or prior to treatment. This formalistic approach risks transforming consent into a symbolic administrative step rather than a substantive mechanism for protecting patient autonomy. Patients may sign documents without comprehensive understanding of how their data will be stored, integrated into broader health information systems, or potentially shared with third parties for operational or regulatory purposes. The complexity of digital infrastructures further limits the capacity of patients to meaningfully comprehend the long-term implications of data processing practices.

Consequently, patients often lack effective awareness and ongoing control over their personal health information once it enters electronic systems. Even where legal provisions formally recognize the right to access or correct data, the practical exercise of these rights may be limited by informational asymmetries and technical opacity. Without transparent communication regarding data retention periods, access hierarchies, or secondary processing activities, consent cannot fully function as an

instrument of autonomous decision-making. Instead, it may operate as a generalized authorization detached from the evolving realities of digital data management.

Accordingly, the results highlight a significant gap between the legal ideal of informed consent and its operationalization within digital healthcare environments. While the normative framework continues to emphasize autonomy and voluntariness, the procedural mechanisms for securing consent have not been recalibrated to address continuous and technologically complex data use. Bridging this gap requires reconceptualizing consent not as a singular event but as an ongoing, context-sensitive process supported by transparency, periodic reaffirmation, and accessible mechanisms for withdrawal or modification. Without such adaptation, the protective function of consent may remain aspirational rather than effectively realized in electronic medical record systems.

Enforcement Mechanisms and Access to Legal Remedies

The analysis demonstrates that enforcement mechanisms embedded within health law are predominantly administrative in character and primarily oriented toward institutional compliance. Regulatory oversight tends to focus on ensuring that healthcare facilities adhere to established procedural standards, professional codes of conduct, and documentation requirements. When violations occur, sanctions are often directed at correcting institutional behavior through warnings, internal disciplinary measures, or administrative penalties. While such mechanisms reinforce organizational accountability, they do not consistently prioritize direct remedies for patients whose privacy rights have been compromised. As a result, the enforcement structure appears to emphasize regulatory order and professional discipline rather than individualized redress.

This institutional orientation may weaken the deterrent effect of privacy obligations. When sanctions are limited to administrative consequences that primarily affect organizational licensing or internal governance, the tangible impact on decision-makers may be comparatively modest. Furthermore, patients who experience harm from data breaches may encounter limited avenues for obtaining compensation or formal acknowledgment of rights violations. The absence of robust civil liability mechanisms or clearly accessible compensatory pathways reduces the practical consequences of non-compliance. Consequently, privacy protection risks being perceived as a procedural requirement rather than a substantive legal entitlement backed by meaningful enforcement (Renuka et al., 2025; Norris, 2022).

In contrast, personal data protection law introduces comparatively stronger enforcement instruments, including administrative fines, corrective orders, and supervisory authority interventions. These tools are designed to impose more concrete financial and operational consequences on data controllers and processors that fail to comply with legal obligations. The availability of such sanctions reflects a governance model that treats personal data protection as a matter of public regulatory priority. However, despite the existence of these formal enforcement mechanisms, the findings indicate that procedural pathways through which individual patients may seek redress remain insufficiently clear. The process for filing complaints, initiating investigations, or pursuing judicial remedies may involve multiple administrative stages and technical documentation requirements that are not easily navigable by laypersons.

Limited public awareness further constrains effective access to remedies. Patients may not fully understand their rights under data protection law, nor the procedures available to challenge unlawful data processing or seek compensation for harm. In addition, the complexity of digital data systems can make it difficult for individuals to detect privacy violations in the first place. Without accessible complaint channels, transparent reporting obligations, and supportive institutional assistance,

enforcement mechanisms may remain underutilized. Thus, while personal data protection law formally strengthens the regulatory toolkit, its practical accessibility for affected individuals may still be restricted.

The findings also reveal that enforcement practices in both health law and data protection law tend to be predominantly reactive rather than preventive. Legal intervention typically occurs after a breach has been identified, reported, or publicized. Investigations and sanctions are therefore triggered by incidents of harm rather than by systematic monitoring of compliance before violations arise. Although reactive enforcement can address specific breaches, it does not necessarily foster a culture of continuous risk assessment and proactive data governance within healthcare institutions.

This reactive orientation limits the preventive capacity of the legal framework. Effective privacy protection in electronic medical record environments requires anticipatory supervision, routine audits, mandatory impact assessments, and continuous compliance monitoring. Without such proactive oversight mechanisms, regulatory authorities may struggle to identify vulnerabilities before they result in data breaches. Consequently, the enforcement system may mitigate consequences after harm has occurred but may be less effective in preventing harm in the first instance. Strengthening preventive supervision alongside accessible remedial pathways would therefore be essential to enhancing the overall effectiveness of privacy protection within digital healthcare governance.

Discrepancies Between Normative Standards and Practical Implementation

The results reveal a substantial disjunction between normative legal standards governing patient privacy and their practical implementation within healthcare institutions. Although statutory provisions consistently mandate confidentiality, data security, and responsible information management, they frequently articulate these obligations in broad and principle-based language. The regulatory framework affirms the necessity of safeguarding medical information but does not define minimum technical requirements, standardized security benchmarks, or detailed compliance protocols. In the absence of such specificity, the translation of abstract legal duties into operational safeguards is largely delegated to healthcare providers themselves.

This structural indeterminacy effectively transfers interpretative responsibility to hospitals and other healthcare institutions. Administrators must determine independently how to operationalize legal mandates within their technological infrastructure, often without authoritative regulatory guidance. Decisions regarding encryption standards, access controls, authentication procedures, system audits, and data retention policies are therefore shaped by institutional discretion rather than by uniform statutory directives. While such flexibility may allow adaptation to local contexts, it simultaneously generates variability in how privacy protections are conceptualized and enforced at the institutional level.

As a consequence, the effectiveness of implementation becomes heavily contingent upon institutional capacity, financial resources, and technical expertise. Well-funded hospitals with advanced digital infrastructures may invest in sophisticated cybersecurity systems, comprehensive monitoring tools, and specialized data protection personnel. In contrast, smaller or resource-constrained facilities may rely on more basic technological safeguards and limited oversight mechanisms. This uneven distribution of protective measures produces disparities in the level of privacy protection afforded to patients, depending on where they receive medical care. Such disparities challenge the principle of equal protection of rights and may undermine public confidence in the healthcare system as a whole.

The findings further indicate that internal institutional policies may, in practice, prioritize operational efficiency and administrative convenience over the robust protection of patient rights. Digital health systems are often implemented to streamline workflows, accelerate information exchange, and reduce bureaucratic burdens. In the absence of clearly defined external benchmarks, compliance efforts may focus on ensuring that procedural requirements are formally satisfied—such as maintaining documentation or adopting general confidentiality statements—without necessarily embedding substantive and technologically rigorous safeguards. This procedural orientation risks reducing privacy compliance to a checklist exercise rather than fostering a culture of proactive rights protection.

Moreover, without standardized national benchmarks or supervisory audits, institutions may gradually normalize minimal levels of data security that satisfy internal assessments but fall short of best practices in information governance. Over time, this normalization may lower expectations regarding what constitutes adequate protection, particularly if regulatory authorities do not systematically evaluate or compare institutional standards. The absence of external accountability mechanisms further reinforces the tendency toward variable and potentially insufficient implementation.

Accordingly, the results underscore the inherent limitations of norm-based regulation that is not accompanied by detailed technical and institutional guidance. While principled legal standards provide an essential normative foundation, they must be complemented by clear operational criteria, supervisory oversight, and capacity-building measures to ensure consistent application. Without such integrative support, the protective ambitions of the legal framework risk remaining aspirational, with implementation outcomes determined more by institutional resources than by uniformly enforceable legal requirements.

Preventive Versus Reactive Legal Approaches

This analysis shows that the legal system that is still in place to protect patient data is more of a reactionary one. The infractions are mainly defined through legislation and determine the sanctions, as well as the remedial measures to be provided after a breach in confidentiality. Though necessary to deal with misconduct and institutional accountability, these mechanisms are ex post in nature in that they come into effect only after the damage has been done and not as a form of anticipatory governance. Preventative obligations, e.g. keeping sufficient safeguards, or data security, are usually set in programmatic language which often does not provide a binding operational specification. As a result, the legal system can be said to be more geared towards dealing with the aftermath of the violation of privacy rather than dealing with preventing it systematically.

This reactive orientation is further demonstrated by the lack of expressive in-service of forward-looking principles, namely privacy by design, privacy by default and proactive risk assessment in health-specific regulations. These are broadly acceptable principles of data-governance which require privacy requirements be taken into account explicitly in the design of digital systems across the board. This lack of inclusion in the healthcare regulatory framework forcefully harms the ability of the law to affect the conceptualisation, development, and implementation of electronic medical record (EMR) systems. Practically, digital platforms are regularly designed to maximise efficiency, interoperability, and administrative capabilities, and privacy protection is introduced later based on the perceived risks or compliance audits.

The fact that technological implementation has been sequenced before its wider regulation is part of a larger trend in digital governance in which the process of innovation is ahead of its normatively prescriptive regulation. The operationalisation

of digital systems prior to the establishment of privacy standards that are unambiguously defined may lead to the adoption of architectures that are hard to change or expensive to refurbish afterwards. Regulatory intervention thus ends up being corrective and not constitutive and seeks to reduce vulnerability once the structural decisions have been entrenched. Such dynamism limits the ability of the law in influencing the institutional behaviour within its initial stage and weakens its deterrent effectiveness.

The results show that this reactive model is particularly insufficient when applied in complex digital infrastructures. EMRS are complex systems that include databases that are inter-connectable, remote access systems, automated processing and integration with third party service providers. The magnitude and speed at which information could be retrieved, copied or transferred increases the possible impact of security breaches. In these settings the damage may occur in a very short time and impact huge numbers of patients simultaneously. Post-incident remediation can be used to help avert some of the effects and cannot be used to undo the loss of confidentiality once the sensitive information is revealed.

Effective prevention therefore requires legal integration at the earliest stages of system design and procurement. Regulatory frameworks should mandate structured risk assessments prior to system deployment, require demonstrable security testing, and impose clear accountability for incorporating privacy safeguards into technical specifications. By embedding preventive obligations into the design phase, the law can function as a guiding framework that shapes technological development rather than merely reacting to its outcomes. Such integration would also encourage institutional cultures that treat data protection as a core structural requirement rather than as an ancillary compliance concern.

CONCLUSION

This study examined the legal protection of patient privacy rights in the use of electronic medical records within Indonesian hospitals by analyzing the coherence, adequacy, and practical implications of the existing legal framework. The findings demonstrate that patient privacy is normatively recognized as a fundamental right in health law and personal data protection law. However, this recognition has not yet been translated into a comprehensive and operational legal framework that adequately addresses the technical and organizational risks associated with electronic medical records. Regulatory provisions remain fragmented, abstract, and largely reactive, creating gaps between normative standards and real world implementation. The study further reveals that responsibility for protecting patient data is unevenly allocated among hospitals, healthcare professionals, and technology providers, resulting in unclear accountability in cases of data breaches. Patient consent, while formally required, is often reduced to a procedural formality and does not fully reflect the continuous and complex data processing inherent in digital health systems. Enforcement mechanisms also remain limited, with insufficient access to effective remedies for patients whose privacy rights are violated.

These findings contribute to the existing body of knowledge by highlighting the structural limitations of sector based health regulation when confronted with digital transformation. The study underscores the need for harmonization between health law and personal data protection law, clearer liability allocation, and a shift toward preventive legal approaches such as privacy by design. Future research may explore comparative legal models or empirical assessments of institutional compliance to further strengthen patient privacy protection in digital healthcare environments.

REFERENCES

Alhasan, T. K. (2025). Managing legal risks in health information exchanges: A

comprehensive approach to privacy, consent, and liability. *Journal of Healthcare Risk Management*, *44*(4), 12-24. https://doi.org/10.1002/jhrm.70002

Alodhialah, A. M. (2025). Exploring the influence of organizational culture on evidence-based practice adoption among nurses in tertiary hospitals: a qualitative study. *BMC nursing*, *24*(1), 1029. https://doi.org/10.1186/s12912-025-03647-z

AlSalamah, S. (2025). VCAC: A Blockchain-Based Virtual Care Access Control Model for Transforming Legacy Healthcare Information Systems and EMRs into Secure, Interoperable Patient-Centered Virtual Hospital Systems. *Information*, *16*(11), 972. https://doi.org/10.3390/info16110972

Asha, N. B., Biswas, T. R., Yasmin, F., Shawn, A. A., & Rahman, S. (2024). Navigating security risks in large-scale data handling: a big data and MIS perspective. *Letters in High Energy Physics*, *12*, 5347-5361.

Ayo-Farai, O., Ogundairo, O., Maduka, C. P., Okongwu, C. C., Babarinde, A. O., & Sodamade, O. T. (2023). Telemedicine in health care: a review of progress and challenges in Africa. *Matrix Science Pharma*, *7*(4), 124-132. https://doi.org/10.4103/mtsp.mtsp_24_23

Batbaatar, E., Dorjdagva, J., Luvsannyam, A., Savino, M. M., & Amenta, P. (2017). Determinants of patient satisfaction A systematic review. *Perspectives in Public Health*, 137(2), 89–101. https://doi.org/10.1177/1757913916634136

Chowdhury, J., & Ravi, R. P. (2022). Healthcare accessibility in developing countries: A global healthcare challenge. *J Clin Biomed Res*, *4*(152), 2-5. https://doi.org/10.47363/JCBR/2022(4)152

Davis, F. D. (1989). Perceived usefulness perceived ease of use and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. https://doi.org/10.2307/249008

Dove, E. S. (2023). Confidentiality, public interest, and the human right to science: when can confidential information be used for the benefit of the wider community?. *Journal of Law and the Biosciences*, *10*(1), lsad013. https://doi.org/10.1093/jlb/lsad013

Galvin, M., Heverin, M., Mac Domhnaill, É., Mcfarlane, R., Meldrum, D., Murray, D., ... & Hardiman, O. (2025). Challenges and solutions to complex data governance issues in cross-national, cross-sectoral, multidisciplinary real world health research: a descriptive overview. *Amyotrophic Lateral Sclerosis and Frontotemporal Degeneration*, *26*(sup1), 1-7. https://doi.org/10.1080/21678421.2024.2428927

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2019). *A primer on partial least squares structural equation modeling (PLS SEM)* (2nd ed.). Sage Publications.

Hallinger, P. (2019). Mapping knowledge production and dissemination in educational leadership and management 1960–2018. *Educational Management Administration and Leadership*, 47(3), 1–25. https://doi.org/10.1177/1741143218822778

Isibor, E. (2024). Regulation of healthcare data security: Legal obligations in a digital age. *Available at SSRN 4957244*.

Mubarak, F. (2026). Digital health literacy and the ethics of information access: a

systematic review of global trends, equity challenges and policy responses. *Journal of Information, Communication and Ethics in Society*, 1-30. https://doi.org/10.1108/JICES-08-2025-0212

Ngesa, J. (2024). Tackling security and privacy challenges in the realm of big data analytics. *World Journal of Advanced Research and Reviews*, *21*(2), 552-576. https://doi.org/10.30574/wjarr.2024.21.2.0429

Nguyen, T. H., Pham, Q. T., & Huynh, P. T. (2023). Factors influencing trust and security perceptions in mobile payment adoption. *Journal of Information Security and Applications*, 69, 103278. https://doi.org/10.1016/j.jisa.2022.103278

Norris, L. P. (2022). The Promise and Perils of Private Enforcement. *Virginia Law Review*, *108*(7), 1483-1545.

Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of CyberSecurity*, *2023*, 115-133. https://doi.org/10.58496/MJCSC/2023/016

Panahi, O. (2025). Secure IoT for healthcare. *European Journal of Innovative Studies and Sustainability*, *1*(1), 17-23. https://doi.org/10.59324/ejiss.2025.1(1).%D1%85%D1%85

Partama, T. A., & Putra, M. D. (2025, November). NORMATIVE ANALYSIS OF PROFESSIONAL ETHICS AND LEGAL ACCOUNTABILITY OF HEALTH WORKERS IN THE IMPLEMENTATION OF INFORMED CONSENT. In *INTERNATIONAL SEMINAR* (Vol. 7, pp. 102-112). https://doi.org/10.36563/49sfwm12

Purwanta, C. S., & Setiawan, S. T. (2024). Behavioral intention toward digital payment adoption in emerging economies. *Journal of Asian Business and Economic Studies*, 31(1), 45–60. https://doi.org/10.1108/JABES-08-2023-0124

Razi, Q., Piyush, R., Chakrabarti, A., Singh, A., Hassija, V., & Chalapathi, G. S. S. (2025). Enhancing data privacy: A comprehensive survey of privacy-enabling technologies. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3546618

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2025). Data privacy and protection: Legal and ethical challenges. *Emerging threats and countermeasures in cybersecurity*, 433-465. https://doi.org/10.1002/9781394230600.ch19

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2025). Data privacy and protection: Legal and ethical challenges. *Emerging threats and countermeasures in cybersecurity*, 433-465. https://doi.org/10.1002/9781394230600.ch19

Republik Indonesia. (2009). *Undang Undang Republik Indonesia Nomor 36 Tahun 2009 tentang Kesehatan*. Lembaran Negara Republik Indonesia Tahun 2009 Nomor 144.

Republik Indonesia. (2022). *Undang Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Santos, J., Cardoso, L., & Figueiredo, V. (2022). Trust security and user intention in mobile payment systems. *Information Technology and People*, 35(5), 1507–

1529. https://doi.org/10.1108/ITP-09-2020-0653

Soelasih, Y., & Sumani. (2022). Trust and perceived usefulness in mobile wallet usage among urban consumers. *Journal of Financial Services Marketing*, 27(2), 128–141. https://doi.org/10.1057/s41264-021-00123-4

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model four longitudinal field studies. *Management Science*, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

World Health Organization. (2021). *Ethics and governance of artificial intelligence for health*. World Health Organization.

Zachariah, M., Sari, D. P., & Pratama, R. A. (2022). Extended technology acceptance model for mobile payment adoption in developing countries. *International Journal of Innovation and Technology Management*, 19(4), 2250021. https://doi.org/10.1142/S0219877022500213

Zolnierek, K. B. H., & DiMatteo, M. R. (2009). Physician communication and patient adherence to treatment A meta analysis. *Medical Care*, 47(8), 826–834. https://doi.org/10.1097/MLR.0b013e31819a5acc