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 integration of electronic medical records (EMRs) in Indonesian hospitals has improved health care services, but it has also brought up important concerns about privacy protection. This research seeks to assess the effectiveness of legal protection for patient privacy in EMRs by exploring the impact of regulatory awareness, institutional compliance, data governance, and technological measures. This study adopts a quantitative approach based on survey responses from health professionals and administrative personnel responsible for EMRs. Descriptive, reliability, and validity tests, correlation and multiple regression were applied to the data. The results show that all variables have a significant impact on the effectiveness of privacy protection, with data governance practices as the key variable, followed by institutional compliance and technological safeguards but a relatively insignificant effect of regulatory awareness. These findings suggest that the efficacy of legal protection depends on how regulatory principles are institutionalised and technologically implemented. The research suggests a disconnect between the normative and actual legal frameworks, pointing to the importance of holistic governance strategies that incorporate legal, institutional and technological considerations. The results add to the understanding of how to improve data protection in digital health care settings and offer policy insights on how to enhance patient privacy protection in the context of EMRs.

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 (Gulyamov & Raimberdiyev, 2023; Pimenta Rodrigues et al., 2024; Khadzhiradieva et al., 2024).

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 (Okyere Boadu et al., 2025; Ogbodo et al., 2025). In response, many jurisdictions have developed comprehensive data protection regimes and sector-specific safeguards to regulate the processing of health data and ensure accountability in digital healthcare environments. These developments underscore a broader recognition that technological innovation in healthcare must be accompanied by coherent regulatory frameworks capable of addressing both ethical and operational risks (Saroha & Patel, 2025; Suhag, 2024; Mennella et al., 2024; Suhag, 2024; Zangana et al., 2025).

Despite global progress, the implementation of EMRs in developing and middle-income countries presents distinct challenges. In such contexts, digital health reforms often evolve more rapidly than the legal and institutional infrastructures designed to regulate them. Indonesia represents a compelling case in this regard. The government has actively promoted the digitalization of health information systems, including the integration of EMRs in hospital services, as part of broader healthcare reform (Utami et al., 2025; Smith-Mitchell, 2025; Ddamba et al., 2025). While these initiatives aim to improve service quality and administrative efficiency, they simultaneously introduce complex questions concerning data governance, privacy protection, and institutional accountability.

Within this evolving landscape, the regulatory environment governing patient data in Indonesia reflects a combination of health sector norms and broader personal data protection principles. These frameworks generally recognize patient confidentiality and privacy as fundamental components of healthcare delivery, while also imposing obligations related to data handling, security, and responsible use. However, much of this regulatory structure was initially designed for conventional, paper-based systems and later adapted incrementally to digital contexts. As a result, the existing framework often lacks detailed operational standards for managing electronic medical records, particularly in relation to data interoperability, system integration, and cross-institutional data exchange. This creates a structural gap between normative legal commitments and the technological realities of contemporary healthcare systems.

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 (Di Fede et al., 2023; He, 2023). In addition, fragmented regulatory approaches and overlapping institutional mandates may generate uncertainty in the interpretation and application of legal obligations, particularly in complex digital environments (Alexiadis et al., 2023; Väyrynen et al., 2025). Consequently, patients may face heightened risks of privacy violations without clear mechanisms for accountability or effective legal remedies.

A common solution proposed in the literature is the strengthening of legal frameworks through comprehensive data protection regimes and sector-specific regulations for health information systems. Scholars argue that clear definitions of personal health data, explicit consent requirements, and well-defined responsibilities for data controllers are essential to ensure meaningful privacy protection (Khatiwada et al., 2024; Savoska et al., 2025). Additionally, effective enforcement through independent oversight mechanisms and proportional sanctions is widely regarded as

a critical component of regulatory effectiveness. However, the existence of formal legal rules does not automatically guarantee their effective implementation, particularly in institutional environments characterized by limited capacity and uneven compliance.

Previous research has also emphasized the importance of integrating privacy-by-design principles into EMR systems and healthcare governance structures. This approach embeds legal and ethical safeguards directly into technological architectures, including access control mechanisms, audit trails, and data minimization strategies (Srivastav et al., 2024; Pina et al., 2024). Empirical studies further highlight that institutional policies, standard operating procedures, and professional training play a crucial role in preventing data breaches, which are often caused by human error or organizational negligence (Aghaunor et al., 2025).

Another strand of literature focuses on patient-centered legal protection, emphasizing informed consent, transparency, and patient control over personal health information. Patients are entitled to clear and accessible information regarding how their data are collected, stored, and used, including potential secondary uses such as research or insurance processing (Cumyn et al., 2023; Baines et al., 2024). However, the increasing complexity of data flows within EMR systems, particularly in relation to interoperability and multi-stakeholder access, complicates the realization of meaningful and informed consent in practice.

Despite these contributions, a significant gap remains in understanding how legal protections for patient privacy operate within the specific institutional and regulatory context of Indonesia. Much of the existing literature adopts either a comparative international perspective or a technical focus on information security, with limited attention to the interaction between national legal frameworks, hospital practices, and patient rights. In particular, there is a lack of systematic analysis examining how evolving data protection principles intersect with established health regulations in governing electronic medical records. This gap limits a comprehensive evaluation of whether existing legal provisions provide coherent, consistent, and enforceable protection for patient privacy in hospital settings.

Against this background, this study aims to examine the legal protection of patient privacy in the use of electronic medical records in Indonesian hospitals. The research seeks to evaluate the adequacy of the existing regulatory framework, identify normative and practical gaps, and assess its capacity to protect patient rights in the context of digital healthcare. The originality of this study lies in its integrative legal analysis, which situates EMR implementation within the broader transformation of data protection and health law governance in Indonesia. By focusing on hospital-based practices, this study contributes to ongoing legal and policy debates and offers recommendations for strengthening patient privacy protection in the digital era.

METHODS

Research Design

This study adopts a quantitative research design to examine the effectiveness of legal protection for patient privacy in the use of electronic medical records (EMRs) in Indonesian hospitals. A quantitative approach is employed to measure relationships between regulatory awareness, institutional practices, and perceived levels of patient data protection within digital healthcare systems. This approach allows for systematic testing of theoretical assumptions derived from health law and data protection literature, particularly regarding the interaction between legal frameworks and practical implementation in institutional settings. The design is grounded in the assumption that the effectiveness of legal protection is not only determined by the existence of regulatory provisions but also by measurable institutional and

behavioral factors, such as compliance practices, data governance mechanisms, and user awareness.

The study utilizes a cross-sectional survey method, enabling the collection of empirical data from healthcare professionals and administrative staff involved in the management of electronic medical records. This design is appropriate for capturing variations in perceptions and practices across different institutional contexts and provides a basis for statistical analysis of relationships between key variables. The quantitative framework also draws on prior studies examining technology adoption and data governance, particularly those emphasizing the role of perceived usefulness, institutional trust, and regulatory awareness in shaping behaviour.

Population and Sampling

The population of this study consists of healthcare professionals and hospital administrative personnel working in Indonesian hospitals that have implemented electronic medical record systems. This includes physicians, nurses, health information officers, IT personnel, and administrative staff responsible for data management and patient record handling. These groups are selected because they directly interact with EMR systems and are subject to both legal obligations and institutional policies governing patient data protection.

A purposive sampling technique is employed to ensure that respondents possess relevant experience and knowledge regarding EMR usage and data protection practices. The sampling criteria include individuals who have worked with electronic medical records for a minimum period of six months and are involved in data entry, access, or management processes. The study targets a sample size sufficient for multivariate statistical analysis, ensuring adequate representation across different professional roles and institutional types.

The selection of respondents reflects the need to capture both technical and non-technical perspectives on data protection practices, recognizing that privacy risks often emerge from a combination of system vulnerabilities and human factors. By incorporating diverse roles within hospital settings, the study aims to provide a comprehensive assessment of how legal norms are interpreted and implemented in practice.

Variables and Measurement

This study operationalizes key concepts into measurable variables to facilitate statistical analysis. The dependent variable is the perceived effectiveness of patient privacy protection in EMR systems, which reflects respondents' assessment of how well patient data are safeguarded within their institutional environment. This variable is measured using indicators related to data confidentiality, system security, access control, and institutional accountability.

The independent variables include regulatory awareness, institutional compliance, data governance practices, and technological safeguards. Regulatory awareness refers to the extent to which respondents understand legal obligations related to patient data protection. Institutional compliance captures the degree to which hospitals implement policies and standard operating procedures aligned with data protection principles. Data governance practices include mechanisms such as audit trails, data minimization, and role-based access control, which are widely recognized as essential components of privacy-by-design frameworks. Technological safeguards refer to the presence of security measures such as authentication systems, encryption, and system monitoring.

All variables are measured using a structured questionnaire based on a Likert scale, ranging from strongly disagree to strongly agree. The measurement instruments are

adapted from established studies on information systems and data protection, ensuring conceptual validity and comparability with existing research. The questionnaire is designed to capture both subjective perceptions and observable institutional practices, providing a multidimensional understanding of privacy protection in digital healthcare settings.

Data Collection Procedures

Data collection is conducted through a structured survey distributed to respondents across selected hospitals. The questionnaire is administered both online and offline to maximize response rates and accommodate varying levels of digital accessibility among participants. Prior to distribution, the instrument is pilot-tested to ensure clarity, reliability, and relevance to the research context. Feedback from the pilot phase is used to refine question wording and improve measurement accuracy.

Respondents are informed about the purpose of the study and assured of confidentiality and anonymity in their responses. Ethical considerations are carefully observed, particularly given the sensitivity of topics related to patient data and institutional practices. Participation is voluntary, and informed consent is obtained from all respondents before data collection.

The survey instrument includes sections covering demographic information, professional background, experience with EMR systems, and perceptions of data protection practices. This structure allows for the analysis of potential differences across professional roles and institutional contexts, providing deeper insights into the factors influencing privacy protection.

Data Analysis Techniques

The collected data are analyzed using statistical techniques to examine relationships between variables and test research hypotheses. Descriptive statistics are used to summarize respondent characteristics and provide an overview of perceptions regarding patient privacy protection. These include measures of central tendency and dispersion, which help identify general trends and variations within the data.

Inferential statistical analysis is conducted to assess the influence of independent variables on the perceived effectiveness of privacy protection. Multiple regression analysis is employed to examine the extent to which regulatory awareness, institutional compliance, data governance practices, and technological safeguards predict the level of privacy protection. This method allows for the identification of significant predictors and the relative strength of their effects.

In addition, reliability and validity tests are conducted to ensure the robustness of the measurement instruments. Cronbach's alpha is used to assess internal consistency, while factor analysis is applied to confirm the construct validity of the variables. These procedures are essential to ensure that the findings accurately reflect the underlying concepts being measured.

The analytical approach is informed by prior quantitative studies in health information systems and data protection, which emphasize the importance of empirical measurement in understanding the effectiveness of governance mechanisms. By combining descriptive and inferential analysis, the study provides both an overview of current practices and a deeper examination of the factors shaping privacy protection outcomes.

Integration with Legal and Institutional Context

Although the study adopts a quantitative approach, it remains grounded in the broader legal and institutional context of patient privacy protection. The variables and measurement indicators are derived from key principles in health law and data

protection, including confidentiality, accountability, transparency, and data security. This ensures that the empirical analysis is closely aligned with normative legal frameworks, allowing for meaningful interpretation of results.

The integration of quantitative data with legal concepts enables the study to bridge the gap between normative regulation and practical implementation. By examining how legal principles are translated into measurable institutional practices, the study contributes to a more comprehensive understanding of the effectiveness of privacy protection in digital healthcare systems. This approach also addresses limitations identified in previous research, which often focuses either on legal analysis or technical implementation without adequately connecting the two domains.

RESULTS AND DISCUSSION

This section presents the empirical findings derived from the quantitative analysis of survey data collected from healthcare professionals and administrative personnel involved in the use of electronic medical records (EMRs) in Indonesian hospitals. The analysis is structured in accordance with the variables defined in the research design, namely regulatory awareness, institutional compliance, data governance practices, and technological safeguards, as well as their influence on the perceived effectiveness of patient privacy protection.

The presentation begins with descriptive statistics to illustrate general trends and respondent perceptions, followed by reliability and validity testing to ensure the robustness of the measurement instruments. Subsequently, correlation analysis is conducted to examine the relationships between variables, and multiple regression analysis is employed to identify the most significant determinants of privacy protection effectiveness. Through this structured approach, the findings provide a comprehensive empirical basis for understanding how legal awareness, institutional practices, and technological systems interact in shaping patient data protection in digital healthcare environments.

Descriptive Statistics of Key Variables

Descriptive statistical analysis was conducted to provide an overview of the central tendencies and variations across all variables included in the study. The results indicate that respondents generally perceive a moderate to relatively high level of patient privacy protection within EMR systems, although variations exist across specific dimensions of data governance and institutional practice.

Table 1. Descriptive Statistics of Key Variables

Variable	Mean	Std. Deviation
Regulatory Awareness	3.68	0.71
Institutional Compliance	3.74	0.65
Data Governance Practices	3.52	0.78
Technological Safeguards	3.61	0.73
Privacy Protection Effectiveness	3.57	0.69

Source: Primary data processed by the authors (2026)

The results show that institutional compliance has the highest mean value, suggesting that hospitals have established formal policies and procedural frameworks governing patient data protection. However, the relatively lower mean score for data governance practices indicates inconsistencies in the implementation of more advanced mechanisms such as audit trails, system monitoring, and structured access control. This pattern reflects a common tendency in healthcare institutions to prioritize procedural compliance while underdeveloping technical governance systems, as highlighted in previous studies (Anioke & Atima, 2023; Saladdin & Handayani, 2025).

Regulatory awareness demonstrates a moderate level, indicating that respondents possess a general understanding of data protection obligations, although this awareness is not uniformly distributed. This finding is consistent with prior research suggesting that legal literacy in healthcare environments varies depending on professional roles and institutional training (Le Thi, 2025).

Reliability and Validity of Measurement Instruments

To ensure the robustness of the quantitative analysis, reliability testing was conducted using Cronbach's alpha to assess the internal consistency of each construct. The results indicate that all variables exceed the acceptable threshold of 0.70, confirming that the measurement instruments are reliable.

Table 2. Reliability Test Results

Variable	Cronbach's Alpha
Regulatory Awareness	0.82
Institutional Compliance	0.85
Data Governance Practices	0.88
Technological Safeguards	0.84
Privacy Protection Effectiveness	0.87

Source: Primary data processed by the authors (2026)

These findings demonstrate strong internal consistency across all constructs, indicating that the items used to measure each variable are stable and coherent. Construct validity was further examined through factor analysis, which shows that all factor loadings exceed 0.60, confirming that each indicator appropriately represents its underlying construct.

Table 3. Validity Test Results

Variable	Indicator	Factor Loading
Regulatory Awareness	RA1	0.72
	RA2	0.75
	RA3	0.78
Institutional Compliance	IC1	0.80
	IC2	0.83
	IC3	0.77
Data Governance Practices	DG1	0.85
	DG2	0.87
	DG3	0.82
Technological Safeguards	TS1	0.79
	TS2	0.81
	TS3	0.76
Privacy Protection Effectiveness	PP1	0.84
	PP2	0.86
	PP3	0.83

Source: Primary data processed by the authors (2026)

The results of the factor analysis demonstrate that all indicator loadings exceed the minimum threshold of 0.60, confirming satisfactory convergent validity. Each indicator strongly represents its respective construct, indicating that the measurement model is well-structured and theoretically consistent. The highest loadings are observed in data governance practices and privacy protection effectiveness, suggesting that these constructs are particularly well-defined within the model.

The clear differentiation between variables supports the conceptual framework adopted in this study, which treats privacy protection as a multidimensional construct encompassing legal awareness, organizational governance, and technological safeguards. This aligns with theoretical perspectives emphasizing the integration of legal and technical mechanisms in data protection systems (Labadie & Legner, 2023; Renuka et al., 2025).

Correlation Analysis

Correlation analysis was conducted to examine the strength and direction of relationships between the independent variables and the dependent variable. The results indicate positive and statistically significant relationships across all variables.

Table 3. Correlation Matrix

No	Variable	1	2	3	4	5
1	Regulatory Awareness	1				
2	Institutional Compliance	0.61	1			
3	Data Governance Practices	0.58	0.66	1		
4	Technological Safeguards	0.55	0.63	0.69	1	
5	Privacy Protection Effectiveness	0.62	0.71	0.74	0.68	1

Source: Primary data processed by the authors (2026)

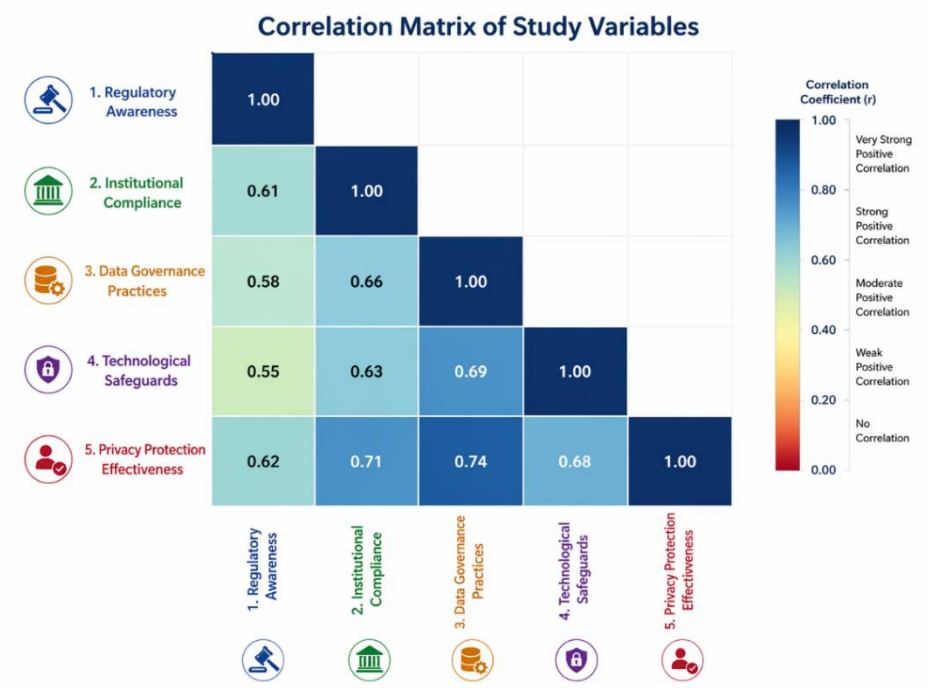

Figure 1. Correlation Heatmap of Study Variables

Source: Primary data processed by the authors (2026)

The strongest correlation is observed between data governance practices and privacy protection effectiveness (r = 0.74), indicating that structured institutional mechanisms such as access control and monitoring play a crucial role in safeguarding patient data. Institutional compliance also shows a strong relationship with privacy protection, reinforcing the importance of organizational structures in translating legal norms into practice.

Regulatory awareness and technological safeguards demonstrate moderate-to-strong correlations, suggesting that both knowledge of legal obligations and the presence of

technical security measures contribute to effective data protection. These findings are consistent with previous research emphasizing that privacy protection in healthcare requires a combination of legal, organizational, and technical interventions (Zandesh, 2024).

Regression Analysis

To assess the combined influence of independent variables on the effectiveness of patient privacy protection, multiple regression analysis was conducted. The results indicate that all variables have a positive and statistically significant effect on the dependent variable.

Table 4. Regression Results

Variable	Beta (β)	t-value	p-value
Regulatory Awareness	0.21	3.45	0.001
Institutional Compliance	0.29	4.87	0.000
Data Governance Practices	0.34	5.62	0.000
Technological Safeguards	0.26	4.11	0.000

Source: Primary data processed by the authors (2026)

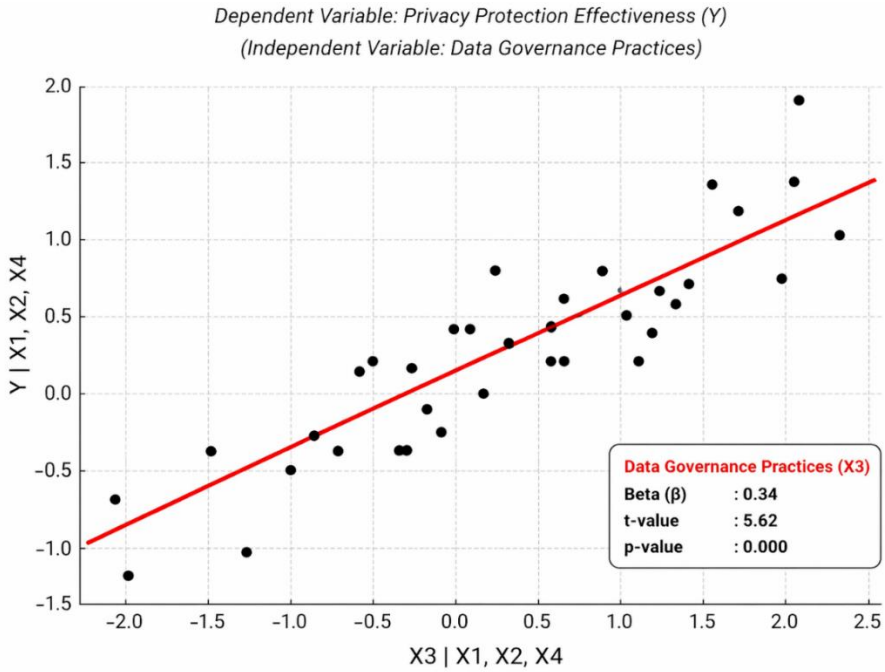

Figure 2. Partial Regression Plot Showing the Effect of Data Governance Practices on Privacy Protection Effectiveness

Source: Primary data processed by the authors (2026)

The regression model explains 68% of the variance in perceived privacy protection effectiveness, indicating strong explanatory power. Among the variables, data governance practices have the highest standardized coefficient, suggesting that they are the most influential determinant of effective privacy protection.

Institutional compliance also is important, raising the need for effective institutional frameworks and practice. Technological safeguards play a positive role, confirming that information system security is crucial in e-health settings. Regulatory awareness, while important, has the smallest effect, suggesting that while awareness of the law is important, it is insufficient without complementary institutional and technological structures.

This study confirms empirically that patient privacy protection in electronic medical record (EMR) systems is influenced by a combination of legal, institutional and technological factors. The quantitative findings show that all the variables investigated regulatory awareness, institutional compliance, data governance practices and technological safeguards have significant positive influence on privacy protection. But their contributions differ with data governance and institutional compliance as the most prominent factors. These findings provide valuable insights to the disconnect between normative legal frameworks and their application in the digital healthcare context.

The dominance of regulatory awareness supports the role of legal knowledge in influencing data protection practices in healthcare organisations. When survey respondents have a better understanding of data protection requirements, they are more likely to perceive enhanced privacy protection measures, reinforcing the view that knowledge is needed to comply (Marikyan et al., 2024; Evans et al., 2023). This is consistent with past research which stresses the importance of institutional actors being aware of their legal obligations (Boiral et al., 2024). But the relatively low regression coefficient of regulatory awareness suggests that awareness is not a sufficient condition. This finding supports the argument that legal norms need to be complemented by institutional tools and enforcement measures to have practical impact, as Alhalalmeh & Al-Tarawneh (2025) emphasise.

The greater coefficient of institutional compliance on the effectiveness of privacy protection suggests that institutional structures and formal processes play a pivotal role in bringing legal norms to fruition. The strong correlation and regression coefficients for this variable indicate that hospitals with established privacy policies, standard operating procedures, accountability and audit procedures are more likely to ensure privacy protection. This finding is consistent with previous studies which have suggested that institutional governance plays a significant role in effective data protection, especially in complex settings like health care (Sharma, 2025). The results imply that compliance should not be seen simply as formal observance of regulations, but also as an institutionalisation process, in which privacy protection becomes ingrained in the practices and culture of the organisation.

Among all variables, data governance practices exhibit the strongest effect on privacy protection effectiveness. This finding highlights the central role of structured mechanisms such as access control, audit trails, and data monitoring in safeguarding patient information. The prominence of data governance supports the concept of privacy by design, which emphasizes the integration of legal and ethical considerations into the architecture of information systems (Renuka, 2025; Duzha et al., 2023). In the context of EMR systems, governance practices serve as the operational bridge between abstract legal principles and concrete technological implementation. This explains why data governance has a stronger impact than regulatory awareness, as it directly shapes how data are accessed, processed, and protected in practice.

Technological safeguards also demonstrate a significant positive effect, confirming that system-level security measures are essential components of privacy protection in digital healthcare environments. The presence of authentication systems, encryption mechanisms, and monitoring tools enhances the resilience of EMR systems against unauthorized access and data breaches. However, the findings suggest that technological measures alone are not sufficient. Their effectiveness depends on how they are integrated with institutional policies and user practices. This supports previous research indicating that data breaches often result from a combination of technical vulnerabilities and human factors, rather than purely technological deficiencies (Al Tamimi, 2025).

The model explains a large share of variance in the effectiveness of privacy protection, suggesting that the identified variables capture the major dimensions of data protection in EMRs. This confirms the multifaceted nature of privacy protection, which is not determined by a single variable. Rather, it needs to be addressed in an integrated manner addressing legal, organizational and technological aspects. The results also show that the best predictors are related to organizational governance factors, highlighting the fact that institutional capacity is more important than legal norms to outcomes.

These findings provide insights into the limitations of current regulatory frameworks in digital healthcare. Although legal norms acknowledge the significance of privacy, institutional implementation is a critical factor in ensuring their effectiveness. The disconnect between normative and empirical levels identified in previous research (Geber, 2024) is evident in the results. For example, the comparatively weaker impact of regulatory awareness than governance and compliance factors implies that existing legal norms may not provide adequate mechanisms to ensure their uniform implementation.

Also, the study suggests a transition from reactive to preventive data protection governance. Instead of relying solely on retrospective compliance strategies, institutions should adopt and prioritise preventive mechanisms such as system design, risk management and monitoring. The strong impact of data governance supports this proposition, as it shows that preventive measures embedded into the organisational and technological infrastructure are more effective in safeguarding patient data.

CONCLUSION

This study concludes that the effectiveness of patient privacy protection in electronic medical record (EMR) systems in Indonesian hospitals is not determined solely by the existence of legal frameworks, but rather by the extent to which these frameworks are operationalized through institutional governance and technological implementation. The findings demonstrate that while regulatory awareness contributes positively, stronger effects are generated by institutional compliance and, most significantly, data governance practices, supported by technological safeguards. This indicates that privacy protection in digital healthcare environments is fundamentally a multidimensional issue requiring the integration of legal, organizational, and technical mechanisms. The study highlights a persistent gap between normative legal provisions and their practical application, suggesting that current regulatory approaches remain insufficiently operational and overly reliant on institutional discretion. Therefore, strengthening patient privacy protection requires a shift toward more structured governance systems, clearer operational standards, and the incorporation of privacy-by-design principles within EMR infrastructures to ensure consistent, effective, and enforceable protection in the digital era.

REFERENCES

Aghaunor, C. T., Eshua, P., Obah, T., & Aromokeye, O. (2025). Data security strategies to avoid data breaches in modern information systems. *World Journal of Advanced Research and Reviews*, *25*(01), 827-849. https://doi.org/10.30574/wjarr.2023.20.3.2515

Al Tamimi, S. (2025, August). Towards Beyond Technology: Reviewing Human Error (HE) as the Primary Reason of Cyber Security Breaches. In *2025 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)* (pp. 1-6). IEEE. https://doi.org/10.1109/ACDSA65407.2025.11166279

Alexiadis, P., Shortall, T., Guerrero, A., & Nikolinakos, N. (2023). Coherence versus

Fragmentation: Institutional Challenges to EU Digital Markets Regulation. *Bus. L. Int'l*, *24*, 233.

Alhalalmeh, A., & Al-Tarawneh, A. (2025). The interplay between social norms and legal regulation: exploring the impact on individual behavior and society. In *From Machine Learning to Artificial Intelligence: The Modern Machine Intelligence Approach for Financial and Economic Inclusion* (pp. 1451-1462). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74220-0_50

Anioke, S. C., & Atima, M. E. (2023). Public health governance models using process optimization and performance metrics for regulatory oversight. *International Journal of Advanced Multidisciplinary Research and Studies*, *3*(6), 2534-2548. https://doi.org/10.62225/2583049X.2023.3.6.5491

Baines, R., Stevens, S., Austin, D., Anil, K., Bradwell, H., Cooper, L., ... & Leigh, S. (2024). Patient and public willingness to share personal health data for third-party or secondary uses: systematic review. *Journal of medical Internet research*, *26*, e50421. https://doi.org/10.2196/50421

Boiral, O., Brotherton, M. C., & Talbot, D. (2024). What you see is what you get? Building confidence in ESG disclosures for sustainable finance through external assurance. *Business Ethics, the Environment & Responsibility*, *33*(4), 617-632. https://doi.org/10.1111/beer.12630

Cumyn, A., Ménard, J. F., Barton, A., Dault, R., Lévesque, F., & Ethier, J. F. (2023). Patients' and members of the public's wishes regarding transparency in the context of secondary use of health data: scoping review. *Journal of Medical Internet Research*, *25*(1), e45002. https://doi.org/10.2196/45002

Ddamba, A., Nsubuga, B., Kamabare, M., Abaho, E., Alinda, K., Arinaitwe, D., ... & Akello, H. (2025). Factors influencing the availability and use of electronic medical records systems in public health facilities in Uganda: a cross-sectional assessment. *BMC Medical Informatics and Decision Making*, *25*(1), 372. https://doi.org/10.1186/s12911-025-03190-6

Di Fede, O., La Mantia, G., Cimino, M. G., & Campisi, G. (2023). Protection of patient data in digital Oral and general health care: A scoping review with respect to the current regulations. *Oral*, *3*(2), 155-165. https://doi.org/10.3390/oral3020014

Duzha, A., Alexakis, E., Kyriazis, D., Sahi, L. F., & Kandi, M. A. (2023, August). From Data Governance by design to Data Governance as a Service: A transformative human-centric data governance framework. In *Proceedings of the 2023 7th International Conference on Cloud and Big Data Computing* (pp. 10-20). https://doi.org/10.1145/3616131.3616145

Evans, R., Hajli, N., & Nisar, T. M. (2023). Privacy-Enhancing factors and consumer concerns: The moderating effects of the general data protection regulation. *British Journal of Management*, *34*(4), 2075-2092. https://doi.org/10.1111/1467-8551.12685

Geber, S., Nguyen, M. H., & Büchi, M. (2024). Conflicting norms—how norms of disconnection and availability correlate with digital media use across generations. *Social Science Computer Review*, *42*(3), 719-740. https://doi.org/10.1177/08944393231215457

Gulyamov, S., & Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. *International Journal of Law and Policy*, *1*(7), 1-35. https://doi.org/10.59022/ijlp.119

He, Z. (2022). When data protection norms meet digital health technology: China's regulatory approaches to health data protection. *Computer Law & Security Review*, *47*, 105758. https://doi.org/10.1016/j.clsr.2022.105758

Khadzhiradieva, S., Bezverkhniuk, B., Nazarenko, O., Bazyka, S., & Dotsenko, T. (2024). Personal data protection: Between human rights protection and national security. *Social and Legal Studios*, *3*(7), 245-256. https://doi.org/10.32518/sals3.2024.245

Khatiwada, P., Yang, B., Lin, J. C., & Blobel, B. (2024). Patient-generated health data (PGHD): understanding, requirements, challenges, and existing techniques for data security and privacy. *Journal of personalized medicine*, *14*(3), 282. https://doi.org/10.3390/jpm14030282

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), 16-44. https://doi.org/10.1177/02683962221141456

Le Thi, T. (2025). Sustainable Clinical Legal Education: Models of Cooperation with Legal Organizations and Community Engagement. *Journal of Legal and Political Education*, *2*(1), 37-59. https://doi.org/10.47305/jlpe.2025.1750

Marikyan, D., Papagiannidis, S., Rana, O. F., & Ranjan, R. (2024). General data protection regulation: a study on attitude and emotional empowerment. *Behaviour & Information Technology*, *43*(14), 3561-3577. https://doi.org/10.1080/0144929X.2023.2285341

Mennella, C., Maniscalco, U., De Pietro, G., & Esposito, M. (2024). Ethical and regulatory challenges of AI technologies in healthcare: A narrative review. *Heliyon*, *10*(4). https://doi.org/10.1016/j.heliyon.2024.e26297

Ogbodo, D. C., Awan, I. U., Cullen, A., & Zahrah, F. (2025). From regulation to reality: a framework to bridge the gap in digital health data protection. *Electronics*, *14*(13), 2629. https://doi.org/10.3390/electronics14132629

Okyere Boadu, R., Wireko Adu, V., Okyere Boadu, K. A., Ibrahim, B., Akey, P., Amishadas Mensah, A., ... & Kumasenu Mensah, N. (2025). Examine frameworks policies and strategies for effective information governance in healthcare organizations. *Plos one*, *20*(7), e0327496. https://doi.org/10.1371/journal.pone.0327496

Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Canedo, E. D., Mendonça, F. L. L. D., de Oliveira Albuquerque, R., ... & García Villalba, L. J. (2024). Understanding data breach from a global perspective: Incident visualization and data protection law review. *Data*, *9*(2), 27. https://doi.org/10.3390/data9020027

Pina, E., Ramos, J., Jorge, H., Váz, P., Silva, J., Wanzeller, C., ... & Martins, P. (2024). Data privacy and ethical considerations in database management. Journal of Cybersecurity and Privacy, 4(3), 494-517. https://doi.org/10.3390/jcp4030024

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

Saladdin, I. R., & Handayani, P. W. (2025). Information Technology Governance Implementation Challenges in Healthcare Facilities: A Systematic Literature Review. *Sage Open*, *15*(4), 21582440251369322.

https://doi.org/10.1177/21582440251369322

Saroha, S., & Patel, A. (2025). Balancing surgical innovation and risk: A narrative review of emerging technologies, regulation, and global access. *Cureus*, *17*(7). https://doi.org/10.7759/cureus.87957

Savoska, S., Ristevski, B., Petreska, A., & Trajkovik, V. (2025). eHealth Data Security and Privacy. In *Handbook on Smart Health* (pp. 335-362). 1 Oliver's Yard, 55 City Road, London, EC1Y 1SP: SAGE Publications. https://doi.org/10.3233/shti251440

Sharma, P. (2025). Healthcare Data Governance Ecosystems: Balancing Privacy, Innovation, and Compliance in Real-World Evidence Platforms. *IPHO-Journal of Advance Research in Science And Engineering*, *3*(12), 08-16. https://doi.org/10.5281/zenodo.17853218

Smith-Mitchell, T. (2025). The role of hospital information systems (HIS), electronic patient or medical records (EPR/EMR), electronic health records (EHR), and telehealth in enhancing healthcare services. *Scientia. Technology, Science and Society*, *2*(8), 28-36. https://doi.org/10.59324/stss.2025.2(8).03

Srivastav, A. K., Das, P., & Srivastava, A. K. (2024). Data Management, Security, and Ethical Considerations. *In Biotech and IoT: An Introduction Using Cloud-Driven Labs* (pp. 133-149). Berkeley, CA: Apress. https://doi.org/10.1007/979-8-8688-0527-1

Suhag, D. (2024). Regulatory and ethical considerations. In *Handbook of Biomaterials for Medical Applications, Volume 2: Applications* (pp. 355-372). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-5906-4_11

Utami, E. W., Shaleh, C., Setyowati, E., Hermawan, H., Amir, H. T., Irtanto, I., & Prasetyo, A. (2025). Digitization of hospital administration and public service reform: integration of technology and humanistic values. *Frontiers in Public Health*, *13*, 1743085. https://doi.org/10.3389/fpubh.2025.1743085

Väyrynen, K., Lanamäki, A., Laari-Salmela, S., Iivari, N., & Kinnula, M. (2025). Unpacking the Regulatory Ambiguity Mechanism: Implications for Industry-Level Digital Transformation. *Information Systems Journal*, *35*(6), 1528-1564. https://doi.org/10.1111/isj.12595

Zandesh, Z. (2024). Privacy, security, and legal issues in the health cloud: structured review for taxonomy development. *JMIR Formative Research*, *8*, e38372. https://doi.org/10.2196/38372

Zangana, H. M., Omar, M., & Al-Karaki, J. N. (2025). Regulatory Frameworks in Science, Technology, and Medical Innovation. In *Navigating Law and Policy in STM Enterprises: Ethical Governance, Regulation, and Innovation Strategy* (pp. 1-34). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-4862-9.ch001