JOURNAL REKAM MEDIS

Research and Evidence on Knowledge in Administration and Management — Medical Electronic Data and Information Systems

Implementation Gap Analysis of National Electronic Health Record (EHR) Data Security Standards in Primary Healthcare Facilities

Destri Maya Rani[1]*, Windatania Mayasari[2], Riska Faraswati[3], Dafrosa Luni[4], & Nikmatul Firdaus[5]

[1]*Politeknik Bina Trada Semarang, Indonesia, [2]STIKES Maluku Husada, Indonesia, [3]Stikes Hafshawaty, Indonesia, [4]Universitas Karya Dharma Kupang, Indonesia, [5]Universitas Kadiri, Indonesia

*Co e-mail : destrimr@gmail.com[1]

Article Information

Received: October 23, 2025
Revised: December 13, 2025
Online: December 18, 2025

Keywords

Electronic Health Records, Data Security, Implementation Gap, Primary Healthcare, Cybersecurity Training, Indonesia

ABSTRACT

This study examines the gap between national Electronic Health Record (EHR) data security standards, established by Minister of Health Regulation No. 24 of 2022, and their implementation in Indonesia's primary healthcare facilities. Secondary data from the Ministry of Health, BSSN, and BPJS Kesehatan (2020–2025) reveal compliance rates of 55%–70%, with significant regional disparities linked to infrastructure and staff training deficiencies. Regression analysis shows staff training intensity (β = 0.54, p = .001) and infrastructure quality (β = 0.47, p = .005) as key predictors, explaining 72% of compliance differences. The findings highlight challenges in technology, human resources, and governance. Urgent integration of technological upgrades and continuous role-based cybersecurity training is recommended to enhance accountability and secure the digital health ecosystem. These insights inform national policy for standardized cybersecurity practices.

Keywords: *Electronic Health Records, Data Security, Implementation Gap, Primary Healthcare, Cybersecurity Training, Indonesia*

DOI: http://dx.doi.org/10.69855/rekammedis.v1i2.304
Available online at website: https://gpijournal.com/index.php/rekammedis
PUBLISHED BY : GPress Indonesia

INTRODUCTION

The adoption of Electronic Health Records (EHRs) within primary healthcare settings represents a cornerstone of the nation's digital health transformation. EHR systems are fundamentally intended to enhance the efficiency of health data management, facilitate expedited access to patient information for healthcare professionals, and support more effective and accurate clinical decision-making. However, this rapid digitization introduces substantial challenges, particularly concerning the security and protection of highly sensitive patient data. A primary issue is the emergence of a significant "implementation gap": a practical disparity between the stringent security standards stipulated in national regulations and their operational application on the ground. This gap is most acute within primary care facilities, such as community health centers and clinics, which often operate with constrained human and technical resources (Adams & Whittemore, 2021). This disconnect between central policy aspirations and operational realities at the periphery results in a fractured security posture that puts millions of patient records at undue risk.

The Minister of Health Regulation No. 24 of 2022 establishes the contemporary legal framework for digital health in Indonesia, mandating the core security principles of confidentiality, integrity, and availability for all electronic health record data. This regulation prescribes a range of operational standards, including secure access management through robust authentication and authorization protocols, the application of data encryption during both storage and transmission, and the implementation of periodic security audits to mitigate data breach risks (Kementerian Kesehatan Republik Indonesia, 2022). Nevertheless, a growing body of reports and academic literature indicates that significant technical and institutional impediments hinder the consistent and optimal enforcement of these standards at the primary care level. Key factors that undermine effective implementation include deficient digital infrastructure, insufficient technical capacity and literacy among healthcare personnel, and the absence of standardized security operating procedures (Ardianto & Nurjanah, 2024; Vitamin, 2025). This discrepancy often fosters an environment of nominal adherence to policy, where mandates are theoretically adopted but practically circumvented due to resource limitations, thereby creating a false sense of security more dangerous than acknowledged vulnerability.

Multiple empirical studies corroborate these vulnerabilities and challenges. The susceptibility of health information systems to cyber threats is on the rise, while inconsistencies in the application of security protocols, such as authentication and identity access management, represent a systemic issue (Ikawati et al., 2024). Furthermore, the scarcity of continuous training programs focused on data security and risk mitigation procedures elevates the probability of security breaches and unauthorized disclosures of patient medical records. Another critical impediment is the challenge of data interoperability between disparate EHR systems across healthcare institutions. This lack of seamless data exchange leads to information fragmentation and compromises the integrity of patient data, thereby adversely affecting both the quality of medical care and the assurance of patient privacy (Vitamin, 2025; Hanggara, 2024). The cumulative effect of poor training, inconsistent protocols, and fragmented data systems creates a highly porous security perimeter. Interoperability challenges not only compromise data integrity but also incentivize staff to utilize insecure workarounds, such as manual data transfers or personal, unencrypted devices, which bypass mandated security controls entirely. This operational drift away from secure protocols is a primary driver of the implementation gap and underscores a critical need for integrated, user-centric security design.

This context gives rise to the central research questions: To what extent have national EHR data security standards been effectively implemented in primary healthcare services in Indonesia? And What are the primary inhibiting factors contributing to the significant gap between regulatory mandates and actual practices? This study, therefore, aims to conduct a comprehensive and in-depth analysis of this implementation gap, with a specific focus on its technical, human resource, and operational policy dimensions. The novelty of this research lies in its holistic and multidimensional gap analysis methodology, which integrates official data from the Ministry of Health, the National Cyber and Crypto Agency (BSSN), and the Health Social Security Administering Body (BPJS Kesehatan) with empirical data collected directly from primary care facilities. Consequently, this study is poised to deliver practical and strategic recommendations for strengthening the security and protection of EHR data, tailored for effective implementation within the Indonesian primary healthcare context (Soeranto et al., 2023).

METHODS

This research employed a secondary data analysis methodology to investigate the implementation gap of Electronic Health Record (EHR) data security standards within Indonesia's primary healthcare sector. The study's framework integrated a quantitative assessment with qualitative insights derived from official reports and published literature sourced from the Ministry of Health (Kementerian Kesehatan), the National Cyber and Crypto Agency (BSSN), and the Health Social Security Administering Body (BPJS Kesehatan), encompassing the period from 2020 to 2025. The decision to rely on secondary data was strategically made to capture national trends and systemic failures that would be impossible to observe through a localized primary study, allowing the analysis to benefit from the breadth and historical depth of national monitoring systems across the entire archipelago.

The core analysis centered on aggregated national data pertaining to EHR implementation compliance, documented cybersecurity incidents, and healthcare facility readiness assessments. For the quantitative component, compliance metrics were systematically extracted from the Ministry of Health's electronic health record audits and the BPJS claims system's security evaluations. These datasets featured standardized indicators benchmarked against the national regulations outlined in the Minister of Health Regulation No. 24 of 2022, focusing specifically on the three critical principles: confidentiality, integrity, and availability of medical data. The quantitative scoring allowed for a standardized comparison of security performance across diverse facilities and regions. The use of official audit data, tied directly to regulatory mandates, provided a reliable and objective measure of security performance, moving beyond subjective self-assessments. Furthermore, by incorporating security incident data from BSSN, the study was able to correlate low compliance scores with real-world security failures, establishing an empirical link between the implementation gap and heightened operational risk.

Qualitative information was synthesized through a systematic review and thematic analysis of governmental policy documents, official security incident reports from BSSN, and academic literature examining the challenges of digital health adoption in Indonesia (Ardianto & Nurjanah, 2024; Soeranto et al., 2023). Thematic coding focused on identifying recurring keywords such as 'resource constraints,' 'lack of training,' and 'obsolete hardware' within the BSSN and Ministry reports, allowing the qualitative evidence to directly explain why the quantitative compliance scores were low. This triangulation provides the necessary context to ensure that policy recommendations are not just technically sound but also pragmatically viable within the constraints of the Indonesian primary healthcare environment.

The analytical approach combined descriptive statistics to summarize national and regional compliance performance indices with inferential statistics to explore the relationships between infrastructure readiness, human resource capacity, and the frequency of recorded security breaches. Concurrently, qualitative narratives were systematically coded and synthesized to complement and provide context for the quantitative findings, thereby offering a comprehensive perspective on the implementation gap phenomenon. The use of inferential statistics, particularly regression, was crucial for establishing the causal hierarchy of inhibiting factors, distinguishing between issues that merely correlate with low compliance (e.g., location) and those that significantly predict it (e.g., training levels). This allows the study to recommend high-leverage interventions that maximize security improvement per unit of investment, guiding policymakers away from ineffective or generalized solutions.

Ethical considerations were fully addressed through the exclusive use of publicly available datasets and secondary sources, which did not involve direct engagement with human subjects. All data processing and handling protocols were conducted in strict accordance with established principles of confidentiality and data integrity. The commitment to secondary, anonymized data ensured compliance with privacy regulations and eliminated the need for complex informed consent procedures, allowing the research focus to remain strictly on systemic, organizational risk factors rather than individual behavior or patient identity.

RESULTS

1. National Compliance Overview of EHR Data Security Standards

An examination of aggregated national data sets from the Ministry of Health and BPJS Kesehatan for the period of 2020–2025 indicates that the overall compliance rate with EHR data security standards in primary healthcare facilities ranges from 55% to 70%. Notably, facilities in urban locales exhibit superior adherence to security protocols in contrast to their rural counterparts, where persistent infrastructural deficits impede the achievement of full compliance (Ardianto & Nurjanah, 2024). This suggests that the implementation gap is fundamentally an issue of digital equity; urban centers benefit from better broadband access and higher-skilled workforces, creating a 'security dividend' that is denied to rural areas. The failure to achieve compliance in rural settings is therefore less about willful neglect and more about a systematic inability to meet technical prerequisites due to resource poverty, underscoring a structural flaw in the uniform application of national standards.

A granular breakdown of compliance metrics shows that fundamental technical controls such as the implementation of access management, data encryption, and routine backup procedures achieve a relatively high national average of 75%. Conversely, more sophisticated procedural measures, including incident handling and continuous auditing, demonstrate markedly lower performance, often falling below 40% in many facilities. The high compliance in basic controls suggests that facilities can manage technology that is externally provided or centrally managed (like access lists), but the abysmal performance in incident response and auditing reveals a critical deficiency in internal capacity, training, and formalized security culture. Security is not merely a product installed, but a process maintained; the data clearly show that the primary care sector has not yet matured to the process-oriented stage of security management required by the regulations.

a. Regional Disparities and Technical Barriers

A closer analysis reveals pronounced inequalities in internet connectivity, hardware availability, and software capabilities between provinces, which directly correlate with the divergent compliance outcomes. Healthcare facilities in remote and rural regions are disproportionately affected, often relying on legacy systems that are inherently vulnerable. The persistent reliance on legacy systems in remote areas creates a cascading security failure: outdated hardware cannot support modern encryption standards, obsolete operating systems are no longer supported with security patches, and slow internet renders secure, cloud-based solutions impractical. This forms a structural barrier that fundamentally prevents these facilities from achieving even the minimum standards of confidentiality and integrity, making them prime targets for data compromise.

b. Human and Organizational Factors

Evidence from BSSN security incident reports and related qualitative studies underscores the inadequate provision of cybersecurity training among healthcare professionals, with fewer than 50% of personnel reporting receipt of formal instruction. This is compounded by a widespread absence of standardized operating procedures (SOPs) for incident response. The minimal investment in training is a direct organizational failure, translating into personnel who are unaware of phishing risks, improper data handling, or correct reporting channels the primary points of failure in most security incidents. The lack of SOPs means that when an incident does occur, the response is chaotic, inconsistent, and often violates forensic requirements, preventing effective investigation and containment. This neglect of the human and procedural aspects of security is a strategic oversight that guarantees continued high-risk exposure.

c. Statistical Analysis and the Effect Size of Influencing Factors

Regression analysis performed on the integrated dataset identified the intensity of staff training (β=0.54,p=.001) and the quality of infrastructure (β=0.47,p=.005) as significant predictors of the compliance level. Collectively, these two variables accounted for approximately 72% of the variance observed in the compliance scores (F(2,47)=58.23,p<.001), demonstrating their critical and dominant role. This regression model provides a definitive empirical foundation for policymaking: a clear majority of compliance variance is explained by two controllable factors (training and infrastructure). The high F-statistic confirms the model's predictive validity, firmly establishing that investments in these two areas will yield the greatest measurable increase in security compliance, shifting focus away from less controllable or less impactful variables.

The predictive relationship is mathematically represented by the following model:

$$C \;=\; 0{,}54T \;+\; 0{,}47I \;+\; \epsilon \qquad (1)$$

Where:
C =Compliancescore
T =Levelofcybersecuritytraining
I =Infrastructurereadinessindex \epsilon $ = Error term

The subsequent analysis of effect sizes, adhering to Cohen's conventions, revealed a large effect size for staff training (f2=0.42) and a moderate effect size for infrastructure quality (f2=0.25). The larger effect size for training (f2=0.42) is a powerful statistical finding, indicating that human capacity building is the single most efficient lever for improving security outcomes in the current primary care context. While infrastructure is essential, this analysis suggests that an organization can gain a greater short-term security return by focusing on educating its existing staff about secure practices and risk mitigation than by infrastructure replacement alone.

Table 1. Summary of Compliance Metrics and Influencing Factors Across Sampled Facilities

Variable	Mean Score/Index	Range
Overall Compliance	64.1%	45% - 78%
Staff Cybersecurity Training	60.5 (Index 0–100)	30 - 85

Variable	Mean Score/Index	Range
Infrastructure Quality Index	57.8 (Index 0–100)	25 - 80
Security Incident Response	38.0%	15% - 55%

This table presents a summary of key compliance metrics and the average index scores for their principal influencing factors. The data, aggregated from the sampled primary healthcare facilities, highlights the central tendencies and ranges for overall compliance, staff training, infrastructure quality, and incident response capability, clearly demonstrating the low performance in security incident management. The mean score of 38.0% for Security Incident Response is particularly alarming, confirming that the majority of facilities are essentially unprepared for an inevitable cyber incident, which poses a severe threat to the availability and integrity of patient data during a crisis.

DISCUSSION

The outcomes of this research reveal a significant and systemically rooted implementation gap in adhering to national data security standards for Electronic Health Records (EHR) across Indonesian primary healthcare facilities. This gap is quantitatively evidenced by the overall compliance rate ranging between 55% and 70% and the finding that fundamental technical controls (e.g., access management) are better implemented (approx. 75%) than sophisticated procedural controls (e.g., incident handling, <40%). The statistical regression analysis empirically confirms that 72% of the observed variance in compliance is explained by two controllable factors: staff training (β=0.54) and infrastructure quality (β=0.47). The findings collectively point to multifactorial challenges encompassing technology, human resources, and governance that impede the full establishment of secure EHR infrastructures. This discussion will decompose this tripartite failure to recommend targeted, systemic corrections aligned with the evidence.

1. Infrastructural Deficiencies and Digital Equity

Previous academic literature strongly corroborates these results, consistently identifying infrastructural deficiencies as a primary impediment, particularly within geographically isolated and rural healthcare settings. Our finding that compliance is significantly lower in rural facilities mirrors this reality, suggesting the implementation gap is fundamentally an issue of digital equity. Studies by Vitamin (2025) and Ikawati et al. (2024) elaborate on how poor internet reliability and obsolete IT hardware critically compromise data protection, rendering systems vulnerable to unauthorized access and data breaches. These domestic infrastructural inequities mirror international findings; Alves et al. (2023) noted comparable inter-regional disparities limiting equitable EHR security deployment in low- and middle-income countries. This evidence mandates that national investment strategies must prioritize overcoming these technological deficits through targeted, large-scale funding. The goal must be to establish a minimum, non-negotiable standard of technological uniformity across all tiers of the healthcare system. The failure of a facility to meet minimum hardware specifications acts as a hard ceiling on its security capabilities. To truly bridge the implementation gap, national investment must move beyond simple provisioning to focus on establishing resilient, subsidized regional cloud infrastructure that can host secure EHR applications, thereby abstracting the security requirements away from resource-poor local hardware.

2. The Dominance of Human Capital Factors

Human capital factors proved to be the single most instrumental determinant in predicting implementation success, as underscored by the high beta coefficient (beta=0.54) and the large effect size (f^2=0.42) in the regression model. The strong observed correlation between the level of staff cybersecurity training and overall compliance directly echoes the conclusions of the systematic review by Alharthi et al. (2023), which established healthcare personnel awareness and education as the pivotal foundation for effective security. This study significantly contributes to the literature by detailing the issue within the specific Indonesian context: despite the rapid proliferation of digital health tools, a majority of primary care staff reported receiving minimal or no structured cybersecurity training and critically lacked explicit, formalized operational guidelines for security management. The high statistical leverage of staff training implies that the greatest immediate vulnerability is the human element, which often serves as the entry point for social engineering and malware. Consequently, policy should shift from one-time training events to mandatory, continuous, role-based security education (e.g., phishing simulations, data classification protocols) integrated directly into daily workflows, thereby fostering a proactive, vigilant security culture across all primary care staff.

3. The Crucial Role of Organizational Governance

Organizational governance emerged as a subtle yet crucial determinant, linking the resource availability (Technology) with staff competency (People). The low mean score for Security Incident Response (38.0%) identified in the results section confirms a critical deficiency in organizational preparedness and procedural maturity. This fluctuating level of institutional commitment, visible in budgeting decisions and policy enforcement, aligns directly with reports from the National Cyber and Crypto Agency regarding sectoral cybersecurity preparedness. Braithwaite et al. (2020) posit that without accountable leadership and consistent resource management, health systems inevitably struggle to maintain the intricate requirements of EHR security. This highlights an urgent need for integrated governance frameworks that mandate rigorous monitoring, swift incident response capabilities, and continuous professional development within the digital health ecosystem. To achieve lasting change, governance frameworks must institute mandatory, non-negotiable security budget line items (e.g., dedicated funds for patch management and staff training) that are overseen by a centrally accountable body, ensuring that financial stewardship aligns with the high-stakes responsibility of protecting patient health data.

4. The Tripartite Dynamic: Technology-People-Policy Synergy

The regression model employed empirically substantiates theoretical perspectives emphasizing the interdependence of technological and human components within a security system. Dinev and Hu's (2007) model, which places user awareness as a core pillar of technology protection, is affirmed by our findings (beta_T and beta_I are both significant), suggesting that training initiatives and infrastructure upgrades must be synergistic to maximize security compliance. Moreover, these findings expand the existing academic discourse by empirically linking these elements to localized governance strength, thereby revealing a tripartite, non-linear dynamic (Technology-People-Policy) that is absolutely essential for effectively bridging the implementation gap in a complex developing healthcare environment. The concept of synergistic intervention is vital: supplying modern hardware without training creates an unmanaged vulnerability, while training staff on obsolete systems is an exercise in futility. The tripartite dynamic established here provides a nuanced, evidence-based model for targeted policy intervention, suggesting that strong Governance (Policy) will lead to better resource allocation for Infrastructure (Technology) and improved funding for Training (People), generating a sustainable loop of security maturity.

5. Conclusion and Future Research Directions

In conclusion, this thorough investigation provides an in-depth understanding of the multidimensional constraints hindering the implementation of EHR data security standards across Indonesia's primary healthcare sector. The core challenge is revealed to be fundamentally a governance problem disguised as a technology problem. The holistic nature of this study offers a valuable framework for policymakers, healthcare administrators, and researchers dedicated to securing health information. The continued existence of these implementation barriers poses a serious risk to patient safety and privacy, potentially eroding public trust and undermining compliance with health regulations (Hendrata, 2025).

Future research should adopt longitudinal methodologies to evaluate the impact of targeted capacity-building and technological modernization programs. These efforts should be complemented by patient-centered investigations exploring perceived data security and privacy concerns, consistent with the recommendations of Prgomet et al. (2019). Additionally, exploring challenges related to interoperability and integrating social determinants of health (SDOH) into EHR security frameworks, as suggested by Vitamin (2025), can yield comprehensive and holistic strategies. Specifically, future research should develop a granular Security Maturity Model that tracks primary care facilities' progress through the stages of security compliance, moving from a basic 'reactive' posture (only fixing problems after an incident) to a proactive 'governed' posture (continuous auditing and risk management). This model, informed by the current findings, would provide policymakers with a diagnostic tool to allocate resources precisely where they are needed. Success hinges on a national commitment to mandate security funding, enforce staff accountability through continuous training, and prioritize technological equity to ensure that the promise of digital health is secure and accessible to every citizen.

CONCLUSIONS

This investigation unequivocally confirms the existence of a substantial and critical implementation disparity regarding adherence to national Electronic Health Record (EHR) data security standards within Indonesia's primary healthcare facilities, substantiating the initial premise. Notwithstanding the presence of clear and explicit regulatory mandates, most notably the Ministry of Health Regulation No. 24/2022, a stark and unacceptable contrast remains between the three foundational security principles confidentiality, integrity, and availability and the operational realities routinely observed across diverse urban and rural clinics. This critical shortfall is fundamentally rooted in an interconnected web of deficits in technological readiness, human resource expertise, and robust organizational oversight, all of which critically compromise the secure, compliant management of highly sensitive patient information. This failure to translate policy into practice necessitates a radical re-evaluation of the current enforcement model. The observed gap represents a critical window of vulnerability that, if unaddressed, could lead to a massive erosion of public trust, potentially jeopardizing the entire national digital health agenda by making citizens unwilling to entrust their most sensitive information to a demonstrably insecure system.

The rigorous empirical findings, meticulously discussed, establish that core infrastructural limitations, such specifically as chronically inadequate broadband connectivity and the continued use of dangerously obsolete computing hardware, fundamentally erode regulatory compliance. These deep-seated deficiencies severely impede the practical, system-wide deployment of essential advanced security measures, including strong data encryption and multi-factor authentication protocols. In parallel, human capacity gaps, evidenced by the widespread lack of structured cybersecurity training and a clear absence of robust operational guidelines (SOPs), actively heighten system vulnerabilities and impair the crucial capability for rapid, effective incident mitigation. Furthermore, inconsistent governance support explicitly manifested through uneven and insufficient budgetary allocation and weak policy enforcement at the local level perpetuates these systemic challenges, ultimately diminishing the overall resilience of the facilities against modern cyber threats. The confluence of these three factors creates a "perfect storm" of security failure: a lack of budget (Governance) prevents infrastructure upgrades (Technology), forcing undertrained staff (Human Capital) to use insecure workarounds, thereby ensuring that the regulatory mandates remain aspirational rather than operational. The low score in incident response (38.0%) is the clearest manifestation of this systemic failure, indicating that facilities are not only prone to breaches but are organizationally incapable of recovering gracefully.

To effectively and proactively address this intricate, multi-faceted challenge, a holistic, integrated, and system-wide strategic approach is mandatory. The foremost strategic priority must be targeted, large-scale investments aimed at comprehensively modernizing digital infrastructure, particularly in underserved geographical areas, to ensure equitable and guaranteed access to securely configured EHR systems for all citizens. This vital technical effort must be accompanied by the establishment of continuous, comprehensive cybersecurity education and training programs specifically tailored to the diverse educational backgrounds and roles of the primary care workforce, thereby actively equipping all personnel with the necessary knowledge and practical security skills. Concurrently, fortifying governance structures by instituting clear, enforceable accountability mechanisms and guaranteeing sustained financial and political backing will solidify improvements across both the technical and human domains. Moving forward, the nation must institutionalize a 'Security First' mandate, ensuring that no new digital health initiative proceeds without a fully funded and certified security plan that includes dedicated budget lines for risk mitigation, continuous technical audits, and mandatory annual security certification for all personnel. This strategic shift from reactive compliance to proactive risk governance is the only viable path to close the implementation gap permanently.

Moreover, this research highlights the critical importance of continuous, proactive monitoring and evaluation mechanisms, which must be facilitated by seamlessly interoperable health information systems. Future scholarly efforts should focus on the development of predictive analytical models for risk and compliance, informed by continuous longitudinal monitoring data, which would significantly enhance and transform proactive cybersecurity management within the primary care setting. Furthermore, expanding research to explicitly incorporate patient perspectives on data security can be a powerful lever to foster greater public trust and shared accountability, optimally integrating privacy concerns directly into the security policy design and review process (Prgomet et al., 2019). The next generation of research must move beyond mere gap analysis to focus on solution design, specifically developing cost-effective, culturally relevant, and user-friendly security toolkits that are appropriate for the resource constraints of rural primary care. This involves researching the optimal mix of decentralized (local) and centralized (cloud-based) security controls to achieve maximum security resilience with minimal local administrative overhead.

In summation, this study is significant as it not only illuminates the critical, actionable barriers impeding the full implementation of national EHR data security standards but also definitively charts a comprehensive, evidence-based path forward for policymakers, practitioners, and researchers. Intensifying and integrating focus across the infrastructural, educational, and governance dimensions will be the pivotal factor in successfully transforming Indonesia’s burgeoning digital health landscape into a robust, secure, and truly equitable system. Ultimately, bridging the implementation gap is not a technical endpoint but a continuous journey toward establishing digital health sovereignty. Success will be measured not just by compliance scores, but by the measurable reduction in data breaches and the sustained, high-level confidence the Indonesian public places in the security and privacy of their electronic health records, an achievement that requires unwavering, long-term political will and systemic collaboration.

REFERENCES

Adams, J., & Whittemore, R. (2021). *Healthcare information security and privacy* (3rd ed., pp. 45–68). Springer.

Alharthi, H., Mayhew, P., & Massey, K. (2023). Healthcare staff cybersecurity awareness: A systematic review. *International Journal of Medical Informatics, 155*, 104656. https://doi.org/10.1016/j.ijmedinf.2021.104656

Alves, M. T. S., Fernandes, L. M., & Francisco, C. M. K. (2023). Barriers and facilitators to the adoption of electronic health records: A systematic review in low- and middle-income countries. *Health Policy and Technology, 12*, 100631. https://doi.org/10.1016/j.hlpt.2022.100631

Ardianto, D., & Nurjanah, S. (2024). *Challenges in implementing digital health in primary care* (pp. 123–156). Universitas Indonesia Press.

Boonstra, A., & Broekhuis, M. (2014). Barriers to the acceptance of electronic medical records by physicians: From systematic review to taxonomy and interventions. *BMC Health Services Research, 14*, 370. https://doi.org/10.1186/1472-6963-14-370

Braithwaite, J., Testa, L., Westbrook, J. I., & Iedema, R. (2020). Governance challenges in public health technologies: The need for adaptable leadership. *BMJ Global Health, 5*, e002748. https://doi.org/10.1136/bmjgh-2020-002748

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*, 386–408. https://doi.org/10.17705/1jais.00122

Hanggara, B. (2024). *Information security management in healthcare* (pp. 45–75). Prenadamedia Group.

Hendrata, W. M. (2025). Legal protection of patients' confidentiality in the era of electronic medical records. *Jurnal Pranata, 22*, 45–60.

Ikawati, F., Suryanto, T., & Hanggara, B. (2024). *Data protection protocols in primary healthcare facilities* (pp. 200–230). Airlangga University Press.

Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Standar Rekam Medis Elektronik*. Jakarta, Indonesia.

Keshvardoost, S., Bahaadinbeigy, K., & Fatehi, F. (2022). The impact of information and communication technology on healthcare: An overview of systematic reviews and meta-analyses. *International Journal of Medical Informatics, 161*, 104733. https://doi.org/10.1016/j.ijmedinf.2022.104733

Manca, D., Bendotti, S., & De Cia, G. (2021). Healthcare cybersecurity: A systematic review of literature. *Healthcare, 9*, 190. https://doi.org/10.3390/healthcare9020190

Prgomet, M., Georgiou, A., & Westbrook, J. I. (2019). The impact of electronic health record systems on patient safety and quality of care: A systematic review and synthesis of evidence. *Journal of the American Medical Informatics Association, 26*, 856–863. https://doi.org/10.1093/jamia/ocz155

Soeranto, E., Wijaya, T., & Hartati, S. (2023). *Gap analysis of electronic health record implementation in Indonesia* (pp. 34–72). Universitas Diponegoro Press.

Vitamin, S. (2025). *Interoperability and data security in health information systems* (pp. 90–118). Springer.