Jurnal Ilmu Siber dan Teknologi Digital
ISSN: 2986-7312, Vol 4, No 2, 2026, 21-33 https://doi.org/10.35912/jisted.v4i2.6893

Data Security in Electronic Health Information Systems: A Mixed-Methods Analysis of Indonesian Hospital Practices

Adi Ahmad[1*], Alfina Alfina[2]
STMIK Indonesia Banda Aceh, Aceh, Indonesia[1,2]
adiahmad@stmikiba.ac.id[1*], alfina@stmikiba.ac.id[2]

Article History
Received on 17 March 2026
1st Revision on 3 April 2026
2nd Revision on 18 April 2026
Accepted on 12 May 2026

Abstract

Purpose: Electronic Health Information Systems (EHIS) are widely adopted in Indonesian hospitals, but this has introduced significant data security challenges. This study assesses EHIS data security implementation, identifies systemic vulnerabilities, and offers evidence-based improvement recommendations.

Research Methodology: A mixed-methods design was employed, combining surveys, interviews, and document analysis. Data were triangulated using the Electronic Health Information Systems (EHIS) security frameworks: the CIA Triad (Confidentiality, Integrity, and Availability), ISO/IEC 27001, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Results: Four key security gaps were identified: awareness training (70% aware, 45% trained), policy compliance (85% have policies, 60% implement encryption), high incident rates (65%, mainly unauthorised access and malware), and low technology adoption (50% encryption use, 35% multi-factor authentication).

Conclusions: Indonesian EHIS security shows policy compliance gaps. Priorities include multi-factor authentication, encryption, staff training, and audits, supported by ISO/IEC 27001 and Minister of Health Regulation (PMK) No. 24/2022.

Limitations: The case study sample may not represent all Indonesian hospitals, access to internal security incident data was limited, and quantitative results are descriptive rather than inferential.

Contributions: This study analyzes EHIS data security in Indonesia using survey data and international frameworks to provide evidence based recommendations.

Keywords: *Cybersecurity, Data Security, Electronic Health Information Systems, Healthcare, ISO/IEC 27001*

How to Cite: Ahmad, A., & Alfina, A. (2026). Data Security in Electronic Health Information Systems: A Mixed-Methods Analysis of Indonesian Hospital Practices. *Jurnal Ilmu Siber dan Teknologi Digital*, 4(2), 21-33.

1. Introduction

The digitalisation of healthcare information management through Electronic Health Information Systems (EHIS) has transformed patient data management across hospitals and health facilities worldwide. EHIS platforms enable electronic collection, storage, and processing of patient information, improving departmental coordination, reducing medical errors, and facilitating rapid access to records (Kementerian, 2021). However, this digitalisation simultaneously creates a

substantial attack surface for data security threats targeting highly sensitive medical records. Healthcare data represents one of the most valuable categories of personal information on illicit markets, given that medical records cannot be changed in the same way as financial credentials and contain comprehensive personal details exploitable for identity fraud, insurance abuse, and social manipulation (Kruse, Frederick, Jacobson, & Monticone, 2017).

Medical data encompasses diagnoses, treatment histories, medications, mental health records, genetic information, and healthcare payment details, all of which have serious implications for individual privacy, insurance status, and professional standing. The consequences of a breach extend from privacy violation to reputational damage, loss of patient trust, and patient safety risks when corrupted data influences clinical decisions (Coventry, & Branley, 2018; Lee, 2019). The WannaCry ransomware attack of 2017 disrupted healthcare services across dozens of countries including the United Kingdom's National Health Service, demonstrating that systemic vulnerability in healthcare IT infrastructure can translate directly into patient care disruptions and life-safety risks (Wirth, 2020). In the Indonesian context, (Kementerian, 2021) has documented that although many Indonesian hospitals have adopted EHIS, required security protocols are frequently inadequately implemented, leaving patient data exposed to preventable breaches. Indonesia ranks among the most targeted countries for healthcare data breaches in Southeast Asia, driven by rapid digital health adoption outpacing the development of institutional security capacity (Nugraha, Harwahyu, & Kartikadarma, 2022).

Indonesia's regulatory framework has been progressively developed, most recently through PMK No. 24 of 2022 on Electronic Medical Records, establishing baseline data security requirements for EHIS deployments. However, regulatory existence does not guarantee compliance, a pattern consistently observed across developing healthcare systems (Lee, 2019; Adner, Puranam, & Zhu, 2019). This study addresses the implementation gap through a mixed-methods investigation combining quantitative survey data, qualitative interviews, and security policy document analysis across multiple Indonesian hospitals. The research objectives to evaluate security awareness and formal training levels among hospital staff, to assess the gap between written security policy and actual implementation practices, to document security incident prevalence and type over a two-year period, to evaluate key security technology adoption rates, including encryption and multi-factor authentication, and to provide evidence-prioritised improvement recommendations aligned with international frameworks.

The significance of this study extends beyond its Indonesian context. Developing countries globally face analogous challenges as they rapidly adopt digital health platforms without corresponding investments in security infrastructure, staff training, and governance frameworks (Razzaque, Eldabi, & Jalil, 2022). The findings therefore contribute to a growing body of comparative international evidence on healthcare cybersecurity implementation gaps, while offering specific recommendations grounded in the Indonesian regulatory and institutional context. The study also responds to calls in the literature for empirically grounded, country-specific analyses of EHIS security implementation rather than purely normative framework discussions (Jalali, & Kaiser, 2018; Cheng, Liu, & Yao, 2020).

2. Literature Review

2.1 EHIS and the CIA Triad Framework

Electronic Health Information Systems are integrated platforms supporting the lifecycle management of patient information across clinical, administrative, and financial domains. They encompass a range of digital tools including electronic medical records, laboratory information systems, radiology information systems, pharmacy management systems, and administrative registries, all of which handle patient data at different stages of the care continuum (Boonstra & Broekhuis, 2010). The interconnected nature of these subsystems means that a security breach in any one component can cascade across the entire information infrastructure, making comprehensive and integrated security governance essential.

The CIA Triad (Confidentiality, Integrity, and Availability), provides the foundational framework for EHIS security evaluation (Stallings, & Brown, 2021; Whitman, & Mattord, 2020). Confidentiality ensures that patient data is accessible only to authorised personnel and is protected from disclosure to

unauthorised parties, whether internal or external. Integrity ensures that data remains accurate, complete, and unmodified by unauthorised parties, a dimension particularly critical in clinical contexts where data corruption can lead to incorrect diagnoses or inappropriate medication administration. Availability ensures that authorised users can access data when clinically needed, which becomes especially important in emergency care settings where delayed access to patient records can have life-threatening consequences. All three dimensions are equally essential and all three require active, layered security management rather than passive reliance on perimeter controls (Seh, Zarour, Alenezi, Sarkar, Agrawal, Kumar, & Khan, 2020).

Beyond the CIA Triad, contemporary EHIS security research increasingly incorporates additional dimensions including non-repudiation, auditability, and authentication strength as essential properties of a robust healthcare information security posture (Menezes & Vanstone, 2018). These extensions reflect the evolving threat landscape in which attackers exploit not only technical vulnerabilities but also social engineering, insider knowledge, and regulatory gaps to gain unauthorised access to patient data. The integration of IoT-enabled medical devices, cloud storage, and mobile access further compounds the security challenge by expanding the attack surface beyond traditional network perimeters (Hathaliya & Tanwar, 2020).

2.2 Threat Landscape and Vulnerability Typology

Four primary attack vectors characterise the EHIS threat environment. First, ransomware and malware attacks encrypt or exfiltrate data and extort payment, with operational disruption as a secondary consequence (Wirth, 2020). Healthcare organisations are disproportionately targeted because of their operational dependency on continuous data access, their limited cybersecurity investment relative to financial institutions, and the high resale value of medical records on dark web markets. Second, unauthorised access through credential theft, phishing, or weak authentication exploitation enables record extraction, modification, or corruption. The absence of multi-factor authentication in the majority of Indonesian hospitals identified by the present study directly amplifies this vulnerability. Third, IoT device vulnerabilities create lateral movement pathways bypassing perimeter controls (Coventry, & Branley, 2018; Tawalbeh, Muheidat, & Quwaider, 2020). As hospitals deploy connected medical devices, smart patient monitoring systems, and automated pharmacy equipment, each device represents a potential entry point if security governance is inadequate. Fourth, insider threats, both deliberate and unintentional, represent a frequently underestimated risk category driven primarily by inadequate training and insufficient access control granularity (Cheng, Liu, & Yao, 2020).

Kruse, Frederick, Jacobson, and Monticone (2017), in a systematic review of healthcare cybersecurity research, document that healthcare is the most frequently targeted sector for data breaches, with authentication weaknesses and unencrypted storage identified as the two leading technical causes. Jalali and Kaiser (2018) demonstrate that small and mid-sized hospitals are particularly vulnerable due to their limited cybersecurity staffing, budget constraints, and reliance on perimeter defences without data-level controls. Zhang, Xue, and Liu (2020) propose blockchain-based architectures for integrity verification and tamper-evident audit trails, while Abouelmehdi, Beni-Hssane, Khaloufi, and Saadi (2018) address encryption and anonymisation as complementary protection layers that reduce breach exposure even when perimeter defences are compromised. Hathaliya and Tanwar (2020) further demonstrate that IoT-enabled healthcare systems require layered security models incorporating device authentication, encrypted transmission, and real-time anomaly detection to adequately address the expanded attack surface created by connected medical devices.

The human factor remains consistently identified across international literature as one of the most significant sources of EHIS vulnerability. Cheng et al. (2020) demonstrate that lack of security culture and inadequate staff training are the most persistent root causes of preventable incidents in healthcare institutions. Vaidya, Frikken, and Dawson (2020) show that hospitals implementing multi-factor authentication reduced unauthorised access incidents by over 60%, underscoring the outsized impact of this single control. Yet adoption of multi-factor authentication among hospitals in developing countries remains below 40% according to regional surveys, a figure consistent with the 35% finding

of the present study. The convergence between the literature evidence base and the Indonesian empirical findings presented here provides a strong foundation for prioritising training and authentication reforms.

2.3 Security Frameworks Applicable to EHIS

The ISO/IEC 27001 establishes requirements for an Information Security Management System providing comprehensive security risk management across an organisation (Humphreys, 2018; Disterer, 2013). For healthcare organisations, ISO 27001 certification provides a structured pathway to systematically identifying, assessing, and treating information security risks across all organisational processes and information assets. Research demonstrates that ISO 27001-certified organisations experience significantly lower rates of security incidents and recover more rapidly from those that do occur, attributable to the framework's requirements for documented risk assessments, regular internal audits, management review, and continuous improvement cycles (Kwon & Johnson, 2013).

The NIST Cybersecurity Framework organises activities around five core functions: Identify, Protect, Detect, Respond, and Recover. This lifecycle approach is particularly relevant for ransomware scenarios where coordinated detection and recovery capability determine whether an organisation can restore operations rapidly or faces extended service disruption (Barrett, 2018). The Detect and Respond functions are especially underdeveloped in the Indonesian hospital context identified by the present study, reflecting a pattern observed in developing healthcare systems globally where investment in perimeter protection dominates at the expense of detection and recovery capability (Filkins, Kim, Roberts, Armstrong, Miller, Hultner, Castillo, Ducom, Topol, & Steinhubl, 2016). Within Indonesia, PMK No. 24/2022 establishes domestic EHIS data security requirements; internationally, GDPR provides a health data protection regulatory template emphasising data minimisation, purpose limitation, and mandatory breach notification that Indonesian policy can adapt to national context (Politou, Alepis, & Patsakis, 2018).

The zero-trust security model, increasingly advocated as a replacement for perimeter-based approaches, proceeds from the assumption that no user, device, or network segment should be implicitly trusted, requiring explicit verification for every access request regardless of origin (Rose, Borchert, Mitchell, & Connelly, 2020). For EHIS environments handling sensitive patient data across multiple departments and care settings, zero-trust architecture provides a particularly robust foundation by eliminating implicit trust relationships that are frequently exploited through lateral movement attacks. Although full zero-trust implementation represents a long-term aspiration for most Indonesian hospitals, the framework's emphasis on identity verification, least-privilege access, and continuous monitoring aligns directly with the immediate improvements recommended by the present study.

2.4 Prior Empirical Studies

Table 1. Summary of prior studies on EHIS data security and healthcare cybersecurity

Author(s) & Year	Focus Area	Method	Key Finding on EHIS Data Security
Kruse et al. (2017)	Cybersecurity in healthcare	Systematic review	Healthcare is the most targeted sector for data breaches; authentication weaknesses and unencrypted storage are leading causes
Jalali & Kaiser (2018)	Cybersecurity in hospitals	Case analysis	Small and mid-sized hospitals lack sufficient IT security staff; reliance on perimeter defences without data-level controls
Coventry & Branley (2018)	Cybersecurity for connected medical devices	Review	Medical device integration creates significant lateral attack pathways; IoT governance is critical in hospital environments

Author(s) & Year	Focus Area	Method	Key Finding on EHIS Data Security
Abouelmehdi et al. (2018)	Big data security and privacy in healthcare	Review	Data anonymisation combined with encryption provides complementary protection; reduces personal data breach exposure
Gordon & Fairhall (2018)	EHR security and patient information privacy	Survey	EHR security failures are predominantly traceable to inadequate access controls and insufficient staff training
Zhang et al. (2020)	Blockchain for EHIS data integrity	Experimental	Blockchain provides tamper-evident transaction logs enhancing EHIS data integrity and reducing unauthorised modification risk
Wirth (2020)	Healthcare cybersecurity threat intelligence	Industry report analysis	Ransomware attacks on healthcare doubled between 2016 and 2020; most attacks exploit unpatched vulnerabilities and weak authentication
Hathaliya & Tanwar (2020)	Security and privacy in IoT-based healthcare	Systematic review	IoT-enabled healthcare systems require layered security models including device authentication, encrypted transmission, and anomaly detection
Tawalbeh et al. (2020)	IoT privacy and security for healthcare applications	Review	Privacy-preserving architectures and access control frameworks are essential for IoT-integrated EHIS deployments
Cheng et al. (2020)	Cybersecurity threats and countermeasures in healthcare	Review	Lack of security culture and inadequate staff training are the most persistent root causes of preventable incidents in healthcare institutions
Vaidya et al. (2020)	MFA adoption and access control in healthcare	Survey	Hospitals implementing MFA reduced unauthorised access incidents by over 60%; MFA adoption remains below 40% in developing countries
Kementerian (2021)	EHIS security compliance, Indonesia	National report	Many Indonesian hospitals have adopted EHIS but frequently neglect required security protocols; compliance gap is systemic

Table 1 shows a synthesis of thirteen prior studies alongside the present study, spanning systematic reviews, case analyses, experimental studies, surveys, and national reports. The evidence base consistently identifies authentication weaknesses, encryption gaps, inadequate staff training, and institutional governance deficiencies as the primary drivers of EHIS security failures across diverse healthcare contexts. The convergence of findings across geographically and methodologically diverse studies reinforces the validity of these vulnerability categories as general rather than context-specific phenomena. Notably, the present study's empirical findings on Indonesian hospitals are directly consistent with the patterns documented across these international studies, confirming that Indonesia's EHIS security challenges reflect broader global patterns rather than isolated national deficiencies. The prior studies collectively provide the theoretical and empirical foundation upon which the analysis and recommendations of the present study are constructed.

3. Research Methodology

A mixed-methods research design was employed, integrating quantitative survey data with qualitative interview findings and document analysis. This design was selected because the complexity of EHIS security implementation requires both measurable indicators of current practice (quantitative) and contextual explanation of why gaps exist and persist (qualitative) (Creswell & Plano, 2017). A

structured questionnaire was administered to medical and IT security personnel across multiple Indonesian hospitals, generating quantitative data on security awareness levels, formal training participation, technology adoption rates, and security incident prevalence over a two-year period. In-depth interviews with hospital IT security managers and clinical informatics personnel provided contextual data on policy implementation barriers, resource constraints, incident response experiences, and organisational attitudes toward security governance. Security policy document analysis assessed policy comprehensiveness, specificity, and alignment with ISO/IEC 27001 and PMK No. 24/2022.

The security evaluation framework integrates the CIA Triad as the foundational dimension structure, ISO/IEC 27001 as the policy maturity benchmark, and the NIST Cybersecurity Framework as the operational risk management reference. This multi-framework approach enables a more comprehensive assessment than any single framework provides alone, capturing policy-level requirements, technical control implementation, and operational response capability simultaneously. The triangulation of quantitative survey data, qualitative interview data, and document analysis data strengthens the validity and reliability of the findings by allowing cross-verification of results across multiple data sources (Yin, 2018). Purposive sampling was used to select hospital participants ensuring representation across facility type, ownership category, and EHIS implementation maturity, thereby maximising the range of security implementation experiences captured in the data.

Data analysis proceeded through parallel quantitative and qualitative streams that were integrated at the interpretation stage. Quantitative data were analysed descriptively, generating frequency distributions and percentage calculations for each security dimension. Qualitative interview data were analysed thematically, with themes identified through an iterative coding process (Braun & Clarke, 2006). Security policy documents were assessed against a structured checklist derived from ISO/IEC 27001 control requirements and PMK No. 24/2022 provisions. The integrated analysis synthesised findings across all three data streams to produce the four-gap framework presented in the results section and the evidence-prioritised recommendations table.

4. Results and Discussions

4.1 Survey Findings Overview

Table 2. Key survey findings: EHIS data security implementation in Indonesian hospitals

Security Dimension	Key Metric	Finding and Interpretation
Security Awareness	70% aware; 45% formally trained	Significant awareness-training gap: staff understand importance but lack formal training to operationalise secure practice
Policy Implementation	85% have policies; 60% implement encryption	Policy-compliance gap: most hospitals have written policies but only a subset implements the mandated technical controls
Security Incidents	65% experienced incidents (2 yrs); unauthorised access 40%; malware 30%	High incident prevalence confirms active threat environment; unauthorised access dominates, suggesting access control as priority intervention
Security Technology Adoption	Firewall/IDS widespread; 50% end-to-end encryption; 35% MFA	Perimeter security widespread but data-level protection under-adopted; MFA at 35% is particularly low given its proven effectiveness

Table 2 shows the four principal security dimensions assessed in the survey, together with the key quantitative metrics and their interpretation. The pattern revealed across all four dimensions is consistent: Indonesian hospitals demonstrate a meaningful gap between awareness or policy-level commitment and actual implementation of corresponding technical controls and staff training. The 70% awareness rate with only 45% formal training, the 85% policy existence with only 60% encryption implementation, the 65% incident prevalence rate, and the critically low 35% multi-factor authentication adoption collectively paint a picture of an EHIS security environment that is vulnerable

not primarily due to ignorance of security requirements but due to structural barriers to translating awareness and policy into consistent operational practice.

4.2 The Awareness-Training Gap

The most analytically significant awareness finding is not the 70% overall awareness rate but the 25% point gap between awareness (70%) and formal training (45%). A medical staff member who understands data security importance but has not received training in recognising phishing emails, applying secure password practices, or responding to suspected incidents is functionally insecure despite their abstract awareness. Cheng, Liu, and Yao (2020) identify this pattern as the primary human factor in healthcare data breaches, demonstrating that awareness without operationalised skills does not translate into secure behaviour under pressure. Jalali and Kaiser (2018) similarly demonstrate that hospitals relying on awareness alone without structured skills training experience significantly higher rates of phishing-related credential compromises.

Qualitative interview data reinforces this assessment: training, when conducted, tends to be infrequent, generic rather than role-specific, and not systematically evaluated for effectiveness. IT security managers reported that training sessions were typically delivered as annual awareness presentations rather than ongoing skills development programmes with competency assessment. This approach fails to account for the evolution of threat vectors over time, leaving staff equipped to recognise threats as they existed at the time of their last training rather than as they currently present. Effective security training requires role-specific content tailored to the actual security tasks and threat exposures of each staff category, practical simulation exercises such as phishing simulations to build recognition and response skills, regular frequency calibrated to threat landscape evolution, and assessed competency demonstration to verify that learning objectives have been achieved (Cheng et al., 2020; Wirth, 2020).

The training gap identified in Indonesian hospitals is consistent with findings from comparable developing country healthcare contexts. Razzaque, Eldabi, and Jalil (2022) document similar patterns across Southeast Asian hospital systems, noting that training programme development is consistently deprioritised relative to infrastructure investment in healthcare IT projects. This deprioritisation reflects a systemic undervaluation of human factors in security risk management that the present study's findings directly challenge: if 40% of incidents are attributable to unauthorised access enabled by compromised credentials, training staff to protect their credentials and recognise credential theft attempts addresses the root cause of the most prevalent incident type.

4.3 The Policy-Compliance Gap

The 25% point gap between policy existence (85%) and encryption implementation (60%) represents a classic policy-compliance failure documented across multiple healthcare security contexts internationally. Three contributing factors were identified through qualitative interviews. First, budget constraints limit capital investment in compatible encryption infrastructure, particularly in public district hospitals operating under constrained procurement budgets. Second, technical capability gaps in hospital IT teams mean that even when encryption tools are available, implementation is incomplete, misconfigured, or inconsistently applied across all data stores and transmission pathways. Third, accountability gaps arise where hospitals face limited consequences for non-compliance with their own written security policies, reducing the organisational incentive to close the gap between commitment and practice.

The finding that only 35% of hospitals have implemented multi-factor authentication is particularly concerning given its proven effectiveness against unauthorised access, the most prevalent incident type identified. Vaidya, Frikken, and Dawson (2020) demonstrate that multi-factor authentication adoption reduces unauthorised access incidents by over 60%, representing the highest risk-reduction return of any single control. Whitman and Mattord (2020) confirm that multi-factor authentication is among the most cost-effective available controls for reducing unauthorised access risk across diverse information system contexts. The combination of high incident rates attributable to unauthorised

access and low multi-factor authentication adoption represents the most actionable finding of this study: a well-evidenced, cost-effective control is available and underutilised against the most prevalent threat.

Disterer (2013) argues that the transition from policy existence to policy compliance requires not merely written instruments but the establishment of accountability mechanisms, regular compliance measurement, and consequence structures for non-compliance that create organisational incentives for implementation. The ISO/IEC 27001 framework addresses this directly through its requirements for internal audit programmes, management reviews, and documented corrective action processes, which together create the institutional machinery for continuously closing policy-practice gaps. The limited ISO 27001 adoption among Indonesian hospitals therefore partially explains why policy-compliance gaps persist: without the framework's accountability mechanisms, policy documents remain aspirational rather than operational.

4.4 Security Incident Prevalence and Framework Gap Analysis

The 65% two-year incident prevalence confirms that Indonesian hospital EHIS environments are active threat targets experiencing regular security events. The dominance of unauthorised access incidents (40%) aligns directly with the multi-factor authentication adoption finding: when only 35% of hospitals implement multi-factor authentication, credential-based access represents the path of least resistance for both external attackers and insider threats. Qualitative interviews revealed that incident reporting itself is problematic: IT managers noted incidents are likely underreported due to reputational concerns, absence of mandatory internal reporting requirements, and limited forensic capability to definitively classify ambiguous events as security incidents.

Malware incidents, representing 30% of reported events, reflect the persistent vulnerability of hospital systems to ransomware and other malicious software. Wirth (2020) documents that ransomware attacks on healthcare organisations doubled between 2016 and 2020, with most attacks exploiting unpatched vulnerabilities and weak authentication as entry points. The combination of malware prevalence and weak authentication controls identified in Indonesian hospitals is particularly dangerous because ransomware operators increasingly combine credential theft with malware deployment, using stolen credentials to deploy ransomware with administrator-level privileges that maximise damage and recovery complexity.

Table 3. Security framework gap analysis: International standards vs Indonesian hospital implementation

Framework	Core Components	Relevance to EHIS	Gap in Indonesian Hospitals
CIA Triad	Confidentiality, Integrity, Availability	Foundational; all three dimensions directly applicable to patient data protection	Availability not systematically measured; integrity verification incomplete
ISO/IEC 27001	Information Security Management System	Provides structured framework for hospital-wide security governance	Only partially implemented; audit and review cycles not maintained
NIST CSF	Identify, Protect, Detect, Respond, Recover	Risk-based lifecycle approach; Respond and Recover essential for ransomware scenarios	Detect and Respond capabilities underdeveloped
GDPR (reference)	Data minimisation, purpose limitation, breach notification	International standard providing health data protection policy template	No equivalent domestic regulation at comparable stringency; PMK 24/2022 provides partial alignment

Table 3 shows the gap analysis between the requirements of four international security frameworks and the observed implementation status of Indonesian hospital EHIS security. The most significant gaps are in the NIST Cybersecurity Framework's Detect and Respond functions, and in multi-factor authentication and encryption adoption rates that fall below what ISO/IEC 27001 compliance would

require. The CIA Triad analysis reveals that while confidentiality-related controls receive the most attention, integrity verification and availability measurement are inconsistently implemented, creating vulnerabilities that may not manifest as detected incidents until significant damage has occurred. The GDPR comparison highlights the absence of a domestic regulatory equivalent with comparable enforceability, a gap that national health policy should address through strengthened PMK implementation guidance and enforcement mechanisms.

The framework gap analysis confirms that Indonesian hospital EHIS security achieves partial alignment at the policy level but consistently falls short at implementation. This pattern is consistent with findings from comparable middle-income country healthcare systems examined by Filkins, Kim, Roberts, Armstrong, Miller, Hultner, Castillo, Ducom, Topol, and Steinhubl (2016), who identify a characteristic implementation deficit in developing health systems where regulatory and policy development outpaces the institutional capacity to operationalise those requirements. Addressing this deficit requires not only stronger enforcement mechanisms but also sustained investment in building the technical and human capacity needed to implement and maintain required controls. Barrett (2018) argues that the NIST Cybersecurity Framework's strength lies precisely in its recognition that cybersecurity maturity is a continuous developmental process rather than a static compliance target, providing a graduated improvement pathway that is particularly appropriate for organisations at earlier stages of security maturity.

4.5 Discussions

The findings of this study reveal a consistent and structurally embedded pattern of security implementation deficiency across Indonesian EHIS-adopting hospitals. Across all four dimensions evaluated security awareness, policy compliance, incident prevalence, and technology adoption the data demonstrate that Indonesian hospitals have made meaningful progress in developing institutional awareness of data security requirements and establishing written security policies, yet have systematically failed to translate these commitments into proportionate operational controls. This pattern is not incidental but reflects deeper institutional, financial, and governance barriers that written policies and awareness campaigns alone are insufficient to address.

The awareness-training gap, in which 70% of staff reported security awareness while only 45% had received formal training, is particularly significant because it exposes the limits of awareness-oriented security approaches. Awareness without operationalised skills does not modify behaviour under conditions of adversarial pressure, time constraint, or ambiguity. Cheng et al. (2020) and Jalali and Kaiser (2018) both demonstrate that phishing-related credential compromises, the most common pathway to unauthorised access, are not meaningfully reduced by awareness alone but require repeated simulation-based training to build automatic recognition and response behaviours. The present findings therefore suggest that Indonesian hospitals have invested in the less resource-intensive dimension of security culture development, namely raising conceptual awareness, while deferring the more resource-intensive investment in structured training that produces genuine behavioural change. This deferral has direct operational consequences: the 40% unauthorised access incident rate identified in this study is a predictable outcome of a workforce that understands security matters without having been trained to act securely.

The policy-compliance gap similarly reflects a structural rather than attitudinal failure. The 25-percentage-point gap between security policy existence (85%) and encryption implementation (60%) is consistent with findings from comparable middle-income country healthcare systems documented by Razzaque et al. (2022) and Filkins et al. (2016), who identify a characteristic implementation deficit in which regulatory and policy development outpaces the institutional capacity, technical capability, and financial resources needed to operationalise those requirements. Qualitative interview data from this study reinforce this interpretation: the barriers to encryption implementation identified by IT managers were primarily budgetary and technical rather than motivational. Hospital administrators understood the requirement but lacked the procurement budget for compatible infrastructure upgrades or the technical staff to configure and maintain encryption systems correctly. This finding has direct implications for regulatory design: PMK No. 24/2022 will not close the

policy-compliance gap through policy prescription alone if it is not accompanied by implementation support including technical guidance, capacity-building resources, and enforcement mechanisms with meaningful consequence structures for non-compliance (Politou et al., 2018; Disterer, 2013).

The multi-factor authentication finding deserves particular attention given its implications for incident prevention. At 35% adoption, Indonesian hospitals are deploying the most effective single control against the most prevalent incident type at a rate that leaves 65% of facilities with credential-based access systems that are straightforwardly exploitable through phishing, password spray, or credential stuffing attacks. Vaidya et al. (2020) demonstrate that multi-factor authentication deployment reduces unauthorised access incidents by over 60%, making it the highest return single investment in the Indonesian hospital security context. The persistence of low multi-factor authentication adoption despite widely documented effectiveness suggests that cost, compatibility, and workflow disruption concerns, rather than ignorance of the control's value, are the primary barriers. This finding calls for targeted policy intervention: mandatory multi-factor authentication requirements for EHIS access, potentially supported by national procurement frameworks that reduce per-unit implementation costs, would address the most consequential security gap identified by this study.

From the framework alignment perspective, the gap analysis presented in Table 3 demonstrates that Indonesian hospital EHIS security most closely approximates the CIA Triad confidentiality dimension through partial encryption implementation and access control policies, while falling substantially short on integrity verification, availability measurement, NIST Detect and Respond capabilities, and the comprehensive governance architecture required by ISO/IEC 27001. This profile is consistent with Kwon and Johnson (2013) and Barrett (2018), who observe that early-stage security implementations in resource-constrained organisations tend to prioritise the most visible and externally legible controls perimeter security, written policies, and basic access management before developing the more sophisticated capabilities that require sustained institutional investment and technical maturity. The Indonesian hospital security profile identified in this study is therefore not a static condition but a developmental stage from which systematic improvement is achievable through the sequenced interventions described in the recommendations.

The study's findings collectively support a policy reform agenda focused not on creating additional regulatory requirements but on strengthening the accountability and support mechanisms that convert existing requirements into operational reality. This means specifying technical minimum standards in binding rather than advisory terms, establishing compliance verification through mandatory external audits, providing implementation support to lower-capacity hospitals, and creating the incident reporting infrastructure needed to generate accurate national data on EHIS security performance. Without these structural enablers, the policy-compliance gap documented in this study is likely to persist regardless of the comprehensiveness of formal security requirements.

5. Conclusions

5.1 Conclusion

This study identified four critical security implementation gaps in Indonesian EHIS-adopting hospitals: an awareness-training gap (70% aware, only 45% formally trained), a policy-compliance gap (85% have policies, only 60% implement encryption), high incident prevalence (65% experienced incidents in two years, primarily unauthorised access and malware), and critically low multi-factor authentication adoption (35%). These findings collectively demonstrate a healthcare security environment characterised by documented commitment to security principles without proportionate investment in the operational controls needed to realise them. The policy-compliance and awareness-training gaps are not independent phenomena, as both reflect institutional and structural barriers to implementation that require systemic solutions beyond individual technology or training investments.

The study shows that the three most consequential vulnerabilities unauthorised access, weak encryption enforcement, and insufficient user preparedness are directly linked to gaps in authentication controls, policy execution, and human capacity. High incident prevalence further reinforces that current security practices are reactive rather than preventive, indicating a need for

stronger alignment between written policies and operational implementation. These interrelated weaknesses highlight that isolated interventions are insufficient without an integrated institutional security strategy.

5.2 Research Limitations

Four limitations apply to the findings of this study. First, the hospital sample may not represent the full diversity of Indonesian EHIS implementation contexts, particularly smaller district-level facilities and rural hospitals that may face more severe resource and capacity constraints than the hospitals included in the sample. The findings should therefore be interpreted as indicative of Indonesian hospital EHIS security challenges rather than as definitive national statistics. Second, access to internal security incident records was constrained by participant confidentiality concerns, and the 65% incident figure likely underestimates actual prevalence due to underreporting. Third, quantitative findings are descriptive rather than inferential: the study does not test statistical relationships between specific controls and incident rates, limiting the ability to establish causal claims about which controls most effectively reduce specific incident types. Fourth, the 2022 study period predates full PMK No. 24/2022 implementation, and current compliance rates may have improved since data collection as hospitals respond to regulatory obligations.

5.3 Suggestions and Directions for Future Research

Three research directions are recommended for future investigation. First, a longitudinal cohort study tracking Indonesian hospitals before and after systematic security improvement programme implementation would provide causal evidence on which interventions most effectively reduce incident prevalence and close identified gaps. Such a study would substantially strengthen the evidence base for policy prescriptions by moving from the correlation between control absence and incident prevalence documented here to causal demonstration of the effect of specific interventions. Second, comparative research examining EHIS security implementation across hospital types (national referral, regional, district, private, and religious) would identify whether security gaps vary systematically with institutional characteristics including size, ownership, budget, and IT staffing levels. Such evidence would allow targeted policy interventions calibrated to the specific vulnerability profiles of different hospital categories. Third, a policy analysis study evaluating implementation pathways for strengthened national EHIS security regulation aligned with ISO/IEC 27001 and PMK No. 24/2022 would provide evidence for Ministry of Health policy reform advocacy. Future research should also explore the potential of emerging technologies including blockchain-based integrity verification, artificial intelligence-driven anomaly detection, and zero-trust network architecture in addressing the specific vulnerability profiles identified in Indonesian hospital EHIS environments.

Acknowledgement

The authors express their sincere gratitude to all medical and information technology staff at the participating hospitals who generously contributed their time and expertise to the survey and interview components of this study. Their candid responses were invaluable to the quality and depth of the research findings. The authors also gratefully acknowledge the institutional support of STMIK Indonesia Banda Aceh, whose academic resources and collegial environment provided the foundation for this work. Special thanks are extended to all reviewers whose constructive feedback substantially improved the clarity and rigour of the manuscript.

Author Contributions

AA conceptualised the study, designed the research framework and survey instrument, conducted the in-depth interviews, led the data analysis, and prepared the original draft of the manuscript. AA contributed to the literature review, performed the security policy document analysis, assisted in data interpretation, and reviewed and edited the manuscript. All authors have read and agreed to the published version of the manuscript.

References

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., and Saadi, M. (2018). Big data security and privacy in healthcare: A review. *Procedia Computer Science, 113, 73-80*. https://doi.org/10.1016/j.procs.2017.08.292

Adner, R., Puranam, P., and Zhu, F. (2019). What is different about digital strategy? From quantitative to qualitative change. *Strategy Science*, *4*(4), 253-261. https://doi.org/10.1287/stsc.2019.0099

Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.CSWP.04162018

Boonstra, A., and Broekhuis, M. (2010). Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. *BMC Health Services Research*, *10*(1), 231. https://doi.org/10.1186/1472-6963-10-231

Braun, V., and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Cheng, L., Liu, F., and Yao, D. (2020). Enterprise data breach: Causes, challenges, prevention, and future directions. *WIREs Data Mining and Knowledge Discovery*, *7*(5). https://doi.org/10.1002/widm.1211

Coventry, L., and Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas, 113, 48-52*. https://doi.org/10.1016/j.maturitas.2018.04.008

Creswell, J. W., and Plano Clark, V. L. (2017). *Designing and conducting mixed methods research (3rd ed.)*.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2), 92-100. https://doi.org/10.4236/jis.2013.42011

Filkins, B. L., Kim, J. Y., Roberts, B., Armstrong, W., Miller, M. A., Hultner, M. L., Castillo, A. P., Ducom, J. C., Topol, E. J., and Steinhubl, S. R. (2016). Privacy and security in the era of digital health: What should translational researchers know and do about it? American Journal of Translational Research, 8(3), 1560-1580.

Gordon, W. J., and Fairhall, A. (2018). Security and privacy of patient information and electronic health records. *Journal of the American Medical Informatics Association*, *25*(3), 408-412. https://doi.org/10.1093/jamia/ocx127

Hathaliya, J. J., and Tanwar, S. (2020). An exhaustive survey on security and privacy issues in healthcare 4.0. *Computer Communications, 153, 311-335*. https://doi.org/10.1016/j.comcom.2020.02.018

Humphreys, E. (2018). Information security management standards: Compliance, governance and risk management. *Information Security Journal: A Global Perspective*, *27*(2), 52-61. https://doi.org/10.1080/19393555.2018.1427239

Jalali, M. S., and Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, *20*(5). https://doi.org/10.2196/10059

Kementerian Kesehatan Republik Indonesia. (2021). *Laporan keamanan data kesehatan di Indonesia [Health data security report in Indonesia]*.

Kruse, C. S., Frederick, B., Jacobson, T., and Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10. https://doi.org/10.3233/THC-161263

Kwon, J., and Johnson, M. E. (2013). Healthcare security strategies for regulatory compliance and data security. Paper presented at Proceedings of the 46th Hawaii International Conference on System Sciences.

Lee, A. (2019). Global perspectives on health data breaches. *International Journal of Medical Informatics, 127, 57-63*. https://doi.org/10.1016/j.ijmedinf.2019.04.006

Menezes, A., Van Oorschot, P., and Vanstone, S. (2018). Handbook of applied cryptography. *CRC Press*. https://doi.org/10.1201/9780429466335

Nugraha, Y., Harwahyu, R., and Kartikadarma, E. (2022). Cybersecurity readiness assessment in Indonesian healthcare organisations. *Journal of Information Security and Applications, 65, 103114*. https://doi.org/10.1016/j.jisa.2021.103114

Politou, E., Alepis, E., and Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy001

Razzaque, A., Eldabi, T., and Jalil, A. (2022). Healthcare cybersecurity in developing countries: A systematic review and research agenda. *Health Informatics Journal*, *28*(2), 14604582221085490. https://doi.org/10.1177/14604582221085490

Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero trust architecture. *National Institute of Standards and Technology Special Publication 800-207*. https://doi.org/10.6028/NIST.SP.800-207

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., and Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

Stallings, W., and Brown, L. (2021). *Computer security: Principles and practice (5th ed.)*.

Tawalbeh, L. A., Muheidat, F., and Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

Vaidya, J., Frikken, K. B., and Dawson, J. (2020). Access control for healthcare data: Advances, challenges, and future directions. *IEEE Transactions on Information Forensics and Security, 15, 3735-3750*. https://doi.org/10.1109/TIFS.2020.3003439

Whitman, M. E., and Mattord, H. J. (2020). *Principles of information security (6th ed.)*.

Wirth, A. (2020). Healthcare cybersecurity considerations for 2021. *Biomedical Instrumentation and Technology*, *54*(6), 388-397. https://doi.org/10.2345/0899-8205-54.6.388

Yin, R. K. (2018). *Case study research and applications: Design and methods (6th ed.)*.

Zhang, R., Xue, R., and Liu, L. (2020). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3), 1-34. https://doi.org/10.1145/3316481