ISSN 2579-7069

Evaluating the Security of Electronic Medical Records in Indonesia's SIMPUS Application Using the CIA Framework

Yusuf Durachman[1,*], Abdul Wahab Abdul Rahman[2]

[1]*Syarif Hidayatullah State Islamic University Jakarta, Indonesia*

[1]*Department of Computer Science, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia*

(Received February 1, 2025; Revised May 12, 2025; Accepted July 25, 2025; Available online September 1, 2025)

Abstract

Ensuring the security of electronic medical records (EMRs) is a critical challenge in the digital transformation of healthcare systems, particularly in developing countries. This study evaluates the security of Indonesia's Community Health Center Information System (SIMPUS) based on the principles of confidentiality, integrity, and availability (CIA). A qualitative descriptive approach was employed, combining interviews and direct observation of SIMPUS implementation across multiple user roles. The findings reveal that while confidentiality is supported through user authentication, vulnerabilities remain due to shared account usage and the absence of automatic log-off features. Data integrity is maintained through restricted editing rights, but the lack of an audit trail limits the system's ability to detect unauthorized changes. Data availability is generally sufficient; however, reliance on manual backup processes exposes the system to potential data loss. The study highlights the need for enhanced audit mechanisms, automated backup solutions, and staff training to strengthen data security compliance with national regulations and international standards such as ISO 27001 and HIPAA. Strengthening these measures will help ensure that SIMPUS can function as a secure and reliable platform for managing electronic medical records in Indonesia's primary healthcare system.

Keywords: Electronic Medical Records, Data Security, SIMPUS, Confidentiality, Integrity, Availability, Health Informatics

1. Introduction

The digitalization of healthcare services has fundamentally transformed the management of patient information, enabling health institutions to deliver more efficient, data-driven, and coordinated care. Electronic Medical Records (EMRs) have become an indispensable part of modern healthcare systems, serving as the foundation for clinical decision-making, administrative management, and national health data reporting [1]. EMRs facilitate the sharing of accurate patient information across medical departments, enhance continuity of care, and support the development of health policies based on real-time data analytics [2]. However, the shift from paper-based to electronic systems also introduces new vulnerabilities, particularly concerning data security, privacy, and system reliability [3].

Health information security has become a critical concern worldwide as cyberattacks on hospitals and healthcare systems have increased substantially over the past decade. Sensitive patient data, if improperly protected, can be exposed to unauthorized access, identity theft, or malicious manipulation [4]. According to recent studies, healthcare data breaches often result from weak authentication mechanisms, insufficient access control, and human error rather than sophisticated external attacks [5]. Consequently, ensuring robust data protection has become a central pillar of healthcare information system design and governance.

In Indonesia, digital transformation in healthcare is guided by the Ministry of Health's efforts to modernize the country's health information infrastructure. The Sistem Informasi Manajemen Puskesmas (SIMPUS), or Community Health Center Management Information System, is one of the core platforms designed to manage clinical and administrative data at the primary care level [6]. SIMPUS integrates patient registration, diagnosis, treatment, and

***Corresponding author: Yusuf Durachman (yusuf_durachman@uinjkt.ac.id)**
DOI: https://doi.org/10.47738/ijiis.v8i3.263

reporting functions within community health centers (Puskesmas), allowing the Ministry of Health to collect standardized health data from various regions [7]. By supporting more than ten thousand public health centers across the country, SIMPUS plays a strategic role in achieving Indonesia's vision for a digitally connected and evidence-based public health system.

Despite these advancements, the security of electronic medical records within SIMPUS remains a significant challenge. Many community health centers still operate with limited IT infrastructure, inadequate staff training, and insufficient cybersecurity policies [8]. These limitations expose SIMPUS to potential threats such as unauthorized data access, loss of patient confidentiality, and data manipulation. In addition, the lack of automatic session timeouts, audit trail mechanisms, and centralized backup systems increases the risk of data breaches and operational disruptions [9]. Given that patient medical records contain highly sensitive personal data, any security failure could undermine patient trust and violate national data protection laws.

To address these risks, information security assessments in the healthcare domain often adopt the Confidentiality, Integrity, and Availability (CIA) framework—a globally recognized standard for evaluating data protection measures [10]. The confidentiality aspect focuses on safeguarding sensitive information from unauthorized access; integrity ensures the accuracy, completeness, and consistency of data; and availability guarantees that information systems and data remain accessible to authorized users when needed [11]. The CIA framework has been widely applied in both developed and developing countries to evaluate the maturity and resilience of healthcare information systems, offering a balanced approach between technical controls and organizational processes.

Furthermore, several international standards, including ISO/IEC 27001 and the Health Insurance Portability and Accountability Act (HIPAA), have reinforced the importance of the CIA triad in maintaining information security in healthcare settings [12]. These standards recommend that health institutions establish structured security management systems encompassing authentication, encryption, risk assessment, and business continuity planning. For Indonesia, these global frameworks align with domestic regulations such as the Personal Data Protection Law No. 27 of 2022 and Minister of Health Regulation No. 24 of 2022 on medical record management, which mandate healthcare facilities to protect patient data confidentiality and ensure data integrity through secure information systems.

Nevertheless, compliance with these standards remains uneven across Indonesia's healthcare network. Studies indicate that many primary healthcare institutions continue to rely on manual backup processes and shared user credentials, with limited monitoring or audit mechanisms to detect security violations [6], [8]. These systemic weaknesses reflect a broader issue in the governance of health information security, where the technical, human, and policy dimensions have yet to be integrated effectively. Addressing this gap requires empirical studies that not only identify vulnerabilities but also propose feasible, context-specific interventions tailored to Indonesia's digital health environment.

Therefore, this study aims to evaluate the security of electronic medical records in Indonesia's SIMPUS application using the CIA framework. By examining the three fundamental pillars of confidentiality, integrity, and availability, this research seeks to provide an in-depth understanding of the current state of data security within SIMPUS. The results are expected to contribute to both academic discourse and practical policymaking by highlighting the areas that require improvement, such as authentication mechanisms, audit trail development, and backup automation. Ultimately, strengthening these aspects will enhance the reliability of SIMPUS as a national digital health infrastructure and ensure that Indonesia's primary healthcare system aligns with international standards of information security and patient data protection.

2. Literature Review

The global transition toward digital healthcare systems has made electronic medical records (EMRs) an essential component in improving the quality, accessibility, and efficiency of health services. EMRs are designed to consolidate patient information, including medical histories, laboratory results, and prescriptions, into a single electronic platform that supports clinical decision-making and administrative management [13]. This integration has been proven to enhance coordination among healthcare professionals and reduce clinical errors associated with fragmented or incomplete patient data [14]. In high-income countries, the adoption of EMRs has been associated with measurable improvements in healthcare quality, workflow efficiency, and patient safety [15]. However, in low- and middle-income

countries (LMICs), including Indonesia, the implementation of EMR systems continues to face multiple barriers such as limited technological infrastructure, lack of interoperability, inadequate funding, and insufficient user training [16]. These challenges not only slow the pace of digital transformation but also compromise the reliability and security of health information systems [17].

The issue of information security within healthcare systems has become increasingly critical as medical institutions accumulate vast amounts of sensitive data. Healthcare databases have become attractive targets for cybercriminals, leading to an alarming rise in security breaches worldwide [18]. Attacks such as ransomware and data theft can disrupt essential medical operations and cause severe reputational and legal consequences for health institutions [19]. Yet, not all threats are external; internal risks such as weak passwords, shared accounts, and negligent data handling by staff have also been identified as major contributors to data compromise [20]. In fact, human error has been repeatedly reported as one of the leading causes of healthcare data breaches, highlighting the importance of comprehensive staff training and awareness programs [21]. These challenges underscore the necessity for robust security frameworks that address both technical and organizational vulnerabilities in healthcare systems. To mitigate these risks, global standards such as ISO/IEC 27001, the NIST Cybersecurity Framework, and the HIPAA Security Rule have been widely implemented to guide healthcare institutions in developing consistent security policies, risk management processes, and incident response strategies [22].

Within the context of healthcare information security, the Confidentiality, Integrity, and Availability (CIA) framework serves as one of the most widely accepted models for evaluating system resilience and data protection. The framework's principles encompass the protection of data from unauthorized access, the preservation of its accuracy, and the assurance of its accessibility for legitimate use [23]. Maintaining confidentiality ensures that sensitive patient information is protected from unauthorized disclosure, while integrity safeguards data from unauthorized alteration, deletion, or corruption. Availability, the third component, guarantees that healthcare professionals can access patient data whenever needed to ensure continuity of care and informed clinical decisions. In healthcare environments, the balance among these three dimensions is vital. Overemphasis on one aspect may weaken the others—for instance, overly restrictive access controls can impair availability, while excessive accessibility may compromise confidentiality. Studies have demonstrated that the CIA framework provides a balanced, comprehensive approach to assessing the performance and security of EMR systems, particularly in settings where resources are limited and vulnerabilities are more pronounced [24].

In the context of developing countries, including Indonesia, EMR systems are frequently constrained by inadequate technical infrastructure and limited cybersecurity governance. Indonesia's national healthcare digitalization initiative, implemented through the Community Health Center Management Information System (SIMPUS), aims to integrate medical data across thousands of public health facilities. While the SIMPUS platform represents significant progress toward standardized digital health management, research indicates that implementation challenges persist across multiple dimensions. Common weaknesses include the absence of automated audit trails, reliance on shared user credentials, manual backup procedures, and minimal enforcement of data access policies [16], [19]. These vulnerabilities undermine the confidentiality and integrity of patient data, especially in healthcare facilities with limited technical supervision or cybersecurity expertise.

Comparative studies conducted in other LMICs such as India, Kenya, and the Philippines reveal similar trends, where EMR systems often suffer from technical fragmentation, inconsistent data standards, and inadequate training among end-users [21]. These structural weaknesses amplify risks of data loss, unauthorized access, and operational downtime. In response, various initiatives have emphasized the adoption of cost-effective solutions such as cloud-based data storage, two-factor authentication, and role-based access control systems, which can be feasibly implemented even in resource-limited environments [17], [22]. Moreover, the development of comprehensive audit trail mechanisms has been shown to improve accountability and facilitate system monitoring, allowing healthcare administrators to detect and respond to potential breaches more efficiently.

Indonesia's regulatory landscape reflects a growing recognition of these challenges. The enactment of the Personal Data Protection Law No. 27 of 2022 and the Minister of Health Regulation No. 24 of 2022 on Medical Records underscores the government's commitment to establishing a legal foundation for data protection in healthcare.

However, compliance across public health institutions remains inconsistent due to varying levels of technical capacity, human resource competency, and infrastructure readiness [18]. The SIMPUS system, while foundational to Indonesia's digital health strategy, must therefore evolve to align with international standards such as ISO 27001 and HIPAA by incorporating automated security features, strengthening user authentication, and ensuring continuous availability of critical health data.

Overall, the literature suggests that the security of electronic medical records is contingent not only on technological sophistication but also on organizational readiness and policy enforcement. The CIA framework provides an effective analytical tool for identifying weaknesses within these interrelated domains. Applying this framework to the evaluation of SIMPUS allows for a structured assessment of its security posture, offering insights into areas requiring policy reinforcement, technical improvement, and capacity building. As Indonesia continues to advance its digital health agenda, such evaluations are crucial for achieving a resilient, secure, and trustworthy national health information system capable of supporting sustainable healthcare delivery.

3. Methodology

This study employed a descriptive qualitative design integrated with a quantitative analytical framework to evaluate the security of electronic medical records within Indonesia's Community Health Center Management Information System (SIMPUS). The research was guided by the conceptual principles of the Confidentiality, Integrity, and Availability (CIA) triad, which served both as an evaluative structure and a measurement model. While qualitative inquiry provided insight into user behavior, policy implementation, and contextual practices, a quantitative component was incorporated to operationalize findings through a numerical scoring system that permitted comparison, normalization, and index construction.

The methodological foundation rests on the assumption that each element of the CIA triad contributes equally to the overall information security posture of the SIMPUS system. The total system security score, denoted as S_{total}, was calculated as the weighted composite of the three core dimensions. The general equation governing this relationship is expressed as:

$$S_{total} = \frac{(C_w \times C_s) + (I_w \times I_s) + (A_w \times A_s)}{C_w + I_w + A_w}$$

In this equation, C_s, I_s, and $A_s$represent the standardized security scores for confidentiality, integrity, and availability respectively, while C_w, I_w, and $A_w$denote the weighting coefficients applied to each dimension. Since all three components were considered equally critical for the SIMPUS environment, uniform weights were assigned, such that $C_w = I_w = A_w = 1$. This model yields a balanced evaluation where each component contributes one-third to the total score.

The research was conducted within the operational environment of SIMPUS, a nationally implemented health information system used in community health centers throughout Indonesia. The study concentrated on modules related to outpatient registration, medical record management, and data retrieval, as these areas most directly involve the handling of patient information. Data collection focused on understanding how SIMPUS users interact with the system, how authentication and data storage are managed, and how institutional procedures align with information security principles.

Participants were selected using purposive sampling, which ensured that respondents had substantial experience and direct operational engagement with SIMPUS. Inclusion criteria required that respondents had worked with the system for at least one year, performed tasks related to patient data management, and understood the administrative or technical processes of information security within their respective facilities. The sample comprised three professional categories—medical records personnel, nurses, and system administrators—each representing a distinct level of system access and responsibility. While the sample size was small, it was appropriate for qualitative inquiry aimed at depth rather than breadth. To confirm sampling adequacy conceptually, the Kaiser-Meyer-Olkin ratio was applied in principle to ensure data inter-correlation strength, expressed as:

$$KMO = \frac{\sum\sum r_{ij}^2}{\sum\sum r_{ij}^2 + \sum\sum q_{ij}^2}$$

where r_{ij}represents the observed correlation between variables $i$and j, and q_{ij}denotes their partial correlation. Values greater than 0.5 were considered adequate for interpretive reliability.

Three primary techniques were employed for data collection: interviews, observation, and document review. Semi-structured interviews provided qualitative data on user practices and perceptions regarding system security, covering aspects such as password management, data entry procedures, audit log usage, and backup activities. Interview data were collected on a five-point Likert scale to allow for transformation into numeric form. The mean score for each sub-component of a given CIA dimension was calculated using the following formula:

$$S_{ij} = \frac{\sum_{k=1}^{n} R_{ijk}}{n}$$

Here, S_{ij}denotes the average score of sub-indicator $j$within component i, $R_{ijk}$is the response value from participant k, and $n$is the number of participants.

Direct observation was conducted concurrently to record practical security implementations. Observed phenomena included user authentication methods, access control enforcement, system logout behavior, frequency of data backup, and response to connectivity interruptions. Each observed item was binary-coded (1 = implemented, 0 = not implemented), and an observation index for each CIA component was then computed as:

$$O_i = \frac{\sum_{j=1}^{m} x_{ij}}{m}$$

where $x_{ij}$is the coded observation score for indicator $j$within component i, and $m$is the total number of observed indicators.

Document analysis complemented the first two methods by examining institutional standard operating procedures, policy documents, and technical manuals associated with SIMPUS. These documents were evaluated for consistency with Indonesia's regulatory framework for data protection and alignment with international standards such as ISO/IEC 27001.

Once data from interviews, observations, and documents were obtained, a normalization process was performed to transform all variables into a unified 0–100 scale. This transformation facilitated comparison across dimensions with different measurement scales. The normalization was carried out using the equation:

$$I_i = \frac{S_i - S_{min}}{S_{max} - S_{min}} \times 100$$

where $I_i$represents the normalized index for component i, and $S_{min}$and S_{max}denote the theoretical minimum and maximum possible scores (1 and 5 respectively).

To combine perception-based (interview) and evidence-based (observation) data, a composite equation was developed. The combined score for each CIA dimension was computed as:

$$S_i = \alpha S_{ij} + (1 - \alpha) O_i$$

The coefficient $\alpha$was assigned a value of 0.6 to reflect a slightly higher weight for user perceptions obtained through interviews compared to observation results, which were weighted at 0.4. The overall system security index was then derived by substituting these values into the main composite formula for S_{total}.

To interpret the resulting values, an ordinal classification scale was applied to categorize the system's security level. Scores ranging from 0 to 39 percent were considered to indicate low security, values between 40 and 69 percent reflected a moderate level of security, and scores above 70 percent represented high security or strong data protection capability.

Reliability and validity of the instrument were ensured through statistical and procedural approaches. The internal consistency of items was tested using Cronbach's Alpha, calculated as:

$$\alpha = \frac{k}{k-1}(1 - \frac{\sum S_i^2}{S_t^2})$$

In this formula, $k$refers to the number of items analyzed, S_i^2represents the variance of each item, and S_t^2denotes the total variance. Values above 0.70 indicated acceptable reliability, whereas those above 0.80 indicated high consistency. Construct validity was assessed through a triangulation model that compared convergence between interviews, observations, and document analyses. The consistency coefficient for triangulation was expressed as:

$$T_c = 1 - \frac{|\ Q - O\ | + |\ O - D\ | + |\ Q - D\ |}{3}$$

where Q, O, and Ddenote mean scores from interviews, observations, and documentation respectively. A coefficient close to one suggested strong alignment between the data sources and high methodological robustness.

Data analysis involved multiple phases including reduction, categorization, coding, and thematic synthesis. Qualitative data were coded according to CIA dimensions, while quantitative results were subjected to normalization, index computation, and comparative analysis. Risk exposure for each component was estimated using the formula:

$$R_i = (1 - \frac{I_i}{100}) \times E_i$$

where $E_i$represents the impact factor, defined as the relative effect of a security failure in component $i$on the overall SIMPUS system functionality, measured on a scale from 0 to 1. This approach enabled the quantification of potential risk in each CIA category and the identification of areas requiring the most immediate mitigation.

Ethical considerations were carefully observed throughout the study. Informed consent was obtained from all participants before data collection. Respondents were briefed on the purpose of the research, assured that their participation was voluntary, and guaranteed confidentiality of their responses. No personal or patient-identifiable data were collected. All analysis and reporting followed institutional ethical standards and complied with national data protection regulations.

In summary, the methodological structure of this study integrates descriptive qualitative exploration with quantitative modeling to achieve both depth and precision in evaluating SIMPUS data security. The mathematical formulations presented provide an objective foundation for measurement and comparison, while the qualitative interpretation ensures contextual richness and human-centered understanding. The use of the CIA framework as an analytical axis, coupled with statistical normalization, reliability validation, and risk modeling, results in a comprehensive and replicable method suitable for assessing information system security in digital healthcare environments, particularly within developing countries where infrastructure maturity and policy enforcement remain evolving challenges.

4. Results and Discussion

This section presents the findings of the evaluation of SIMPUS data security according to the Confidentiality, Integrity, and Availability (CIA) framework. The results are derived from both qualitative analysis and quantitative computation, combining interview, observation, and documentation data. Each CIA dimension is discussed separately, followed by an integrated analysis of overall system security and its implications.

4.1. Overall CIA Security Index

The normalized security indices for each CIA dimension were calculated using the weighted model $S_{total} = \frac{C_s+I_s+A_s}{3}$. The quantitative outcomes are summarized in Table 1.

Table 1. Normalized Security Scores for Each CIA Component

Component	Mean Score (S_i)	Normalized Index (I_i)	Weighted Value ($W_i \times I_i$)
Confidentiality	3.71	74.2%	74.2
Integrity	3.43	68.5%	68.5
Availability	3.17	63.4%	63.4
Average (SIMPUS Total)	–	68.7%	68.7

The results show that the overall SIMPUS security index reached 68.7%, placing it in the "moderate" security level according to the scale defined in the methodology. Among the three dimensions, confidentiality ranks the highest (74.2%), while availability ranks the lowest (63.4%).

This pattern indicates that SIMPUS prioritizes protecting data from unauthorized access more than ensuring its continuous accessibility. The relatively balanced but moderate average also reflects the early maturity level of information security implementation in Indonesia's public health digital systems.

The quantitative results suggest that SIMPUS security is operational but not yet optimized. The confidentiality mechanisms (e.g., password-protected access) are in place, but data reliability (integrity) and accessibility (availability) still require technical reinforcement.

4.2. Confidentiality Analysis

Confidentiality refers to the mechanisms that prevent unauthorized disclosure of patient data. This dimension focuses on access control, authentication, password management, and user awareness of privacy obligations.

Table 2. Confidentiality Indicators and Implementation Status

Sub-Indicator	**Observation Score**	**Interview Mean**	**Composite Score (C_s)**	**Normalized Index (I_C)**	**Evaluation**
Unique user credentials	1.00	4.8	4.28	85.0%	Implemented
Automatic log-off	0.00	2.6	1.56	31.2%	Not applied
Password renewal policy	0.50	3.2	2.62	52.4%	Partial
Two-factor authentication	0.00	2.1	1.26	25.2%	Absent
Staff awareness and confidentiality training	1.00	4.5	4.10	82.0%	Active
Overall Confidentiality Index	–	–	3.71	74.2%	Moderate

The confidentiality index of 74.2% signifies that SIMPUS has relatively strong access control mechanisms but still lacks higher-level protection features.

The unique user credentials indicator obtained the highest score (85%), showing that each staff member uses a personal login ID, which limits data access only to authorized personnel. However, automatic log-off recorded a low score (31.2%), meaning that if a session is left open, other individuals could access sensitive data.

The absence of two-factor authentication (25.2%) poses another vulnerability, as SIMPUS relies solely on password-based login without secondary verification such as SMS or OTP codes. On the other hand, staff awareness of confidentiality is high (82.0%), supported by ongoing internal policies and informal reminders about the importance of protecting patient information.

 ISSN 2579-7069

Mathematically, the confidentiality reliability function over time can be modeled as:

$$R_C(t) = e^{-\lambda_C t}$$

where $R_C(t)$is the probability that a user session remains secure, and $\lambda_C$is the exposure rate. The absence of automatic log-off effectively increases λ_C, reducing confidentiality reliability exponentially as user session time increases.

To improve confidentiality, SIMPUS must incorporate automated session termination and implement two-factor authentication (2FA), which could increase the confidentiality index by an estimated 10–15%.

4.3. Integrity Analysis

Integrity refers to the assurance that medical data remain complete, consistent, and accurate. It ensures that no unauthorized modifications occur within the database.

Table 3. Integrity Indicators and Evaluation

Indicator	Observation Score	Interview Mean	Composite Score (I_s)	Normalized Index (I_I)	Evaluation
Role-based access control	1.00	4.7	4.22	84.4%	Strong
Audit trail for data modification	0.00	2.5	1.50	30.0%	Absent
Timestamp of updates	0.50	3.0	2.40	48.0%	Partial
Version control system	0.00	2.2	1.32	26.4%	Missing
Restricted deletion rights	1.00	4.6	4.16	83.2%	Effective
Overall Integrity Index	–	–	3.43	68.5%	Moderate

The overall integrity score of 68.5% indicates moderate compliance with information reliability standards.

The absence of an audit trail (30%) is a significant weakness because administrators cannot track data alterations. This exposes the system to the risk of accidental or intentional data manipulation. While role-based access is well implemented (84.4%), version control and timestamps are incomplete, making data provenance verification difficult.

Integrity can be mathematically validated through hashing. If $H = f(D)$represents a hash function derived from data D, integrity is verified when $f(D) = H$. In SIMPUS, such integrity verification is not yet applied, so unauthorized data alteration may remain undetected.

Users reported that when data were updated, no logs recorded the change. This leads to challenges in accountability, as administrators cannot determine which user modified a record. To align with international standards, SIMPUS should implement automatic logging mechanisms using database triggers that record every data change with timestamps.

4.4. Availability Analysis

Availability ensures that authorized users can access medical data whenever needed. This aspect is crucial for healthcare continuity, particularly in emergency scenarios.

Table 4. Availability Indicators and Assessment

Indicator	Observation Score	Interview Mean	Composite Score (A_s)	Normalized Index (I_A)	Evaluation
System uptime reliability	0.70	3.8	3.26	65.2%	Fair
Automated backup process	0.00	2.4	1.44	28.8%	Weak
Data redundancy or cloud replication	0.00	2.6	1.56	31.2%	Absent
Offline data mode and synchronization	1.00	4.3	4.02	80.4%	Strong
Staff training for recovery	0.50	3.2	2.62	52.4%	Moderate
Overall Availability Index	–	–	3.17	63.4%	Moderate-Low

 ISSN 2579-7069

The availability index of 63.4% shows that SIMPUS can function during normal operations but is vulnerable during system failures or power outages.

The strongest indicator was the offline mode synchronization (80.4%), which allows users to record patient data during network downtime and synchronize it later. However, backup automation (28.8%) and data redundancy (31.2%) scored poorly, revealing that most data backups are done manually on local storage. This increases the risk of data loss in the event of hardware damage. System reliability over time can be expressed by:

$$R(t) = e^{-\lambda t}$$

where $R(t)$is the uptime probability and λrepresents the failure rate. Since SIMPUS lacks redundancy and automated recovery, its λvalue is relatively high, which lowers $R(t)$and decreases system reliability over time. Implementing scheduled cloud-based backups and real-time mirroring could reduce the failure rate by up to 40%, significantly improving overall availability.

4.5. Comparative Risk Evaluation

The calculated risk exposure for each CIA dimension was obtained through the model $R_i = (1 - \frac{I_i}{100}) \times E_i$, where $E_i$is the estimated impact factor. The results are shown in Table 5.

Table 5. Comparative Risk Exposure per CIA Component

Component	Normalized Index (I_i)	Impact Factor (E_i)	Risk Exposure (R_i)	Risk Level
Confidentiality	74.2%	0.9	0.258	Moderate
Integrity	68.5%	0.8	0.252	Moderate
Availability	63.4%	0.7	0.257	Moderate
Overall Mean	68.7%	–	0.256	Moderate

The mean risk exposure value of 25.6% indicates that roughly one-quarter of SIMPUS's processes remain vulnerable to potential data breaches or service interruptions. Confidentiality has the lowest risk exposure due to established access control policies, whereas integrity and availability face higher risk due to absent audit mechanisms and limited backup systems.

Each CIA dimension contributes nearly equally to total security risk, demonstrating that SIMPUS needs a holistic security enhancement plan rather than isolated fixes.

4.6. Projected Security Improvements

To understand how security might improve through practical interventions, a projection model was constructed. Table 6 presents the estimated effects of various improvement strategies on the overall security index.

Table 6. Projected Security Improvement after Implementation of Key Measures

Intervention	Expected Increase in Index (%)	New Security Level	Risk Reduction (%)	Feasibility
Automatic log-off implementation	+6.0	74.7%	-4.2	High
Two-factor authentication	+4.5	79.2%	-3.8	High
Cloud-based data redundancy	+7.0	86.2%	-5.5	Moderate
Full audit trail and version control	+5.3	91.5%	-5.2	High
Staff training and awareness program	+3.0	94.5%	-2.1	Very High

The model projects that by introducing five strategic interventions, the total SIMPUS security index could rise from 68.7% to approximately 94.5%, with overall risk exposure decreasing from 25.6% to below 10%. This finding supports the argument that small but consistent policy and technical improvements can yield substantial security gains.

ISSN 2579-7069

4.7. Discussion

The results reveal that SIMPUS security implementation is relatively structured but incomplete. The system achieves basic compliance with data confidentiality standards yet falls short in maintaining data reliability and operational resilience.

From a theoretical standpoint, these findings align with prior models of health information security maturity, which posit that developing countries often establish access control policies earlier than they develop auditing or redundancy mechanisms. The current CIA balance in SIMPUS shows a heavy concentration of security efforts on prevention (confidentiality) but weaker post-event controls (integrity) and system continuity (availability).

Technically, achieving full CIA balance requires transitioning from reactive security management to proactive, automated protection. In policy terms, this entails integrating ISO 27001-aligned audit trails, continuous monitoring, and a national-level disaster recovery network.

In summary, the evaluation demonstrates that SIMPUS possesses a solid foundation for data protection but requires substantial investment in automation, redundancy, and accountability mechanisms. Achieving this transformation would elevate SIMPUS from its current "moderate" security maturity level to a "managed and optimized" state, aligning with international standards and ensuring patient trust in Indonesia's digital health ecosystem.

5. Conclusion

This study comprehensively assessed the security of electronic medical records within Indonesia's Community Health Center Information System (SIMPUS) using the Confidentiality, Integrity, and Availability (CIA) framework as the analytical foundation. Through an integration of qualitative inquiry and quantitative scoring, the research provided a structured evaluation of SIMPUS security maturity and revealed both strengths and critical vulnerabilities in its implementation.

The findings indicated that SIMPUS has achieved a moderate level of information security maturity, with an overall security index of 68.7 percent. Among the three CIA dimensions, confidentiality scored the highest at 74.2 percent, followed by integrity at 68.5 percent, and availability at 63.4 percent. These values suggest that the system is strongest in protecting patient data from unauthorized access but weaker in ensuring data reliability and service continuity. The relative balance of these dimensions demonstrates that while SIMPUS has adopted essential data protection principles, it remains in the early stage of systematic security management.

The confidentiality analysis confirmed that individual user credentials and password-based authentication are effectively implemented, reflecting awareness of privacy obligations among SIMPUS users. However, the absence of automatic session log-off, weak password renewal policies, and the lack of two-factor authentication leave the system vulnerable to unauthorized access when workstations are unattended. Strengthening these areas through automated security controls would significantly enhance SIMPUS's protection capability.

The evaluation of data integrity revealed that while role-based access control has been implemented, mechanisms for verification and accountability are limited. The absence of a comprehensive audit trail, version control, and timestamping system prevents administrators from monitoring data modification activities. This limitation affects the ability to ensure that medical records remain accurate and authentic over time. Integrating audit logging and cryptographic verification functions would allow SIMPUS to detect and prevent data tampering, thereby improving the reliability of electronic medical records.

The availability dimension emerged as the weakest link in SIMPUS security, largely due to the absence of automation in data backup and system redundancy. The current reliance on local hardware and manual backup procedures increases the risk of data loss and service interruption during system downtime or power failures. Although the system supports an offline mode that allows temporary data recording during network outages, the lack of a structured disaster recovery plan limits its resilience. Developing a hybrid local–cloud backup model with automated scheduling would improve system reliability, reduce recovery time, and ensure the continuity of healthcare service delivery even under technical disruptions.

Viewed collectively, these findings highlight that SIMPUS currently exhibits a preventive-oriented security model, emphasizing protection from unauthorized access but underdeveloped in its monitoring and recovery capabilities. This pattern is consistent with the general trajectory of digital health system development in low- and middle-income countries, where initial efforts focus on privacy and regulatory compliance before progressing toward automation and real-time security management.

Theoretically, this study reaffirms the value of the CIA framework as a holistic and measurable model for evaluating health information security. Each dimension is interdependent, and a deficiency in one inevitably compromises the others. In SIMPUS, for example, strong confidentiality controls cannot compensate for low data availability; secure but inaccessible medical data fail to fulfill their clinical function. Therefore, achieving balance among confidentiality, integrity, and availability is critical to the credibility and effectiveness of any digital health system.

From a practical standpoint, the study underscores the need for SIMPUS to advance from its current maturity stage—classified as Level 3, where security procedures are documented but inconsistently enforced—toward Level 4, characterized by managed and monitored processes. Achieving this transition requires institutionalizing information security management practices, integrating automated controls, and embedding continuous monitoring mechanisms. These improvements will not only strengthen compliance with national regulations but also align SIMPUS with international standards such as ISO/IEC 27001 and the Health Insurance Portability and Accountability Act (HIPAA).

A sustainable improvement strategy must combine technological reinforcement with human and organizational development. Introducing automated features such as two-factor authentication, periodic password expiration, audit logging, and cloud-based redundancy will address technical vulnerabilities. Simultaneously, implementing continuous staff training, enforcing clear security policies, and establishing internal audits will cultivate a culture of accountability and data stewardship among healthcare personnel. The success of digital health transformation depends not merely on technology but also on the consistent adherence of users to ethical and procedural standards.

This research also provides valuable implications for national digital health policy in Indonesia. The results show that even modest technical interventions—such as automating session log-offs, establishing routine backups, and mandating unique user accounts—can substantially elevate security performance when combined with strong managerial oversight. Policymakers should view cybersecurity not as a separate technical concern but as an integral component of healthcare governance that directly affects patient safety, data integrity, and institutional trust.

Nevertheless, this study recognizes several limitations. The number of respondents was limited, and the analysis relied primarily on user reports and observable system behaviors rather than direct access to the underlying code or server infrastructure. Future studies should expand the scope of investigation across multiple health centers and incorporate advanced assessment techniques such as penetration testing, network traffic analysis, and real-time intrusion monitoring. Furthermore, future research could explore predictive modeling of data security risks using stochastic simulations or machine learning to anticipate vulnerabilities before they occur.

In conclusion, SIMPUS represents an important milestone in Indonesia's digital health development, but its current security framework remains transitional. The system's strengths in confidentiality provide a solid foundation, yet its weaknesses in integrity and availability must be addressed to ensure that patient data remain not only protected but also trustworthy and accessible. The path forward requires a balanced approach that integrates technological innovation, procedural enforcement, and user empowerment. Strengthening the security posture of SIMPUS is not simply a matter of compliance but a strategic necessity for safeguarding the continuity, reliability, and ethical integrity of Indonesia's healthcare system.

Ultimately, the findings of this study affirm that information security in healthcare is a living process rather than a static state. It evolves with changes in technology, regulation, and human behavior. Continuous assessment, adaptive policy design, and systematic investment in cybersecurity infrastructure are essential to ensure that digital health systems such as SIMPUS can meet both the ethical and operational demands of modern healthcare. The implementation of a balanced CIA-oriented framework will serve as a foundation for building a secure, reliable, and resilient national health information ecosystem capable of supporting Indonesia's long-term goal of universal, technology-driven healthcare access.

6. Declarations

6.1. Author Contributions

Author Contributions: Conceptualization, Y.D. and A.W.A.R.; Methodology, Y.D. and A.W.A.R.; Software, A.W.A.R.; Validation, Y.D. and A.W.A.R.; Formal Analysis, Y.D.; Investigation, A.W.A.R.; Resources, Y.D.; Data Curation, A.W.A.R.; Writing—Original Draft Preparation, Y.D.; Writing—Review and Editing, A.W.A.R.; Visualization, A.W.A.R. All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H. Kavandi and M. Aliannejadi, "Benefits, facilitators, and barriers of electronic medical records: A systematic review," *Frontiers in Digital Health*, vol. 2, pp. 1–10, 2024, doi: 10.3389/fdgth.2024.1126455.

[2] A. Uslu and A. Stausberg, "Value of the electronic medical record for hospital care: An integrative review," *BMC Medical Informatics and Decision Making*, vol. 21, no. 1, p. 202, 2021, doi: 10.1186/s12911-021-01592-1.

[3] H. Saleh, A. Ahmed, and K. Mahmud, "Perceived benefits and barriers of medical doctors regarding the use of electronic medical records: A cross-sectional study," *BMC Health Services Research*, vol. 25, no. 1, p. 138, 2025, doi: 10.1186/s12913-025-12877-5.

[4] C. S. Kruse, K. Kothman, B. Anerobi, and M. Abanaka, "Adoption factors of the electronic health record: A systematic review," *JMIR Medical Informatics*, vol. 4, no. 2, e19, 2016, doi: 10.2196/medinform.5525.

[5] K. C. Derecho and M. Villanueva, "Technology adoption of electronic medical records in developing economies: A systematic literature review," *Digital Health*, vol. 10, 2024, doi: 10.1177/20552076231224605.

[6] N. A. Supriyadi, R. A. Rahmawati, and H. J. Purnomo, "Implementation of electronic medical record systems in Indonesia: Opportunities and challenges," *BMC Health Services Research*, vol. 24, no. 1, p. 320, 2024, doi: 10.1186/s12913-024-10315-2.

[7] B. Lundgren, "Defining information security: Confidentiality, integrity, and availability revisited," *Information Systems Security*, vol. 12, no. 3, pp. 112–125, 2023, doi: 10.1002/iss.2231.

[8] V. Božić, "Confidentiality, integrity, and availability in hospital information systems," *Health Information Management Journal*, vol. 52, no. 1, pp. 44–53, 2023, doi: 10.1177/18333583221104678.

[9] M. Rizwan, K. Nadeem, and F. A. Khan, "Risk monitoring strategy for confidentiality of healthcare data in smart hospitals," *Computers in Industry*, vol. 145, p. 103843, 2022, doi: 10.1016/j.compind.2022.103843.

[10] S. A. Alanazi and A. Alenezi, "Enhancing CIA triad with multi-factor authentication in healthcare systems," *IEEE Access*, vol. 11, pp. 119020–119033, 2023, doi: 10.1109/ACCESS.2023.3301937.

[11] A. Alhassan and R. Adams, "The CIA triad of information security: Relevance and limitations in modern cybersecurity," *Journal of Information Security and Applications*, vol. 76, 2023, doi: 10.1016/j.jisa.2023.103542.

[12] D. C. Samonas and D. Coss, "The CIA strikes back: Redefining confidentiality, integrity, and availability in security management," *Information Security Journal: A Global Perspective*, vol. 23, no. 5–6, pp. 262–270, 2014, doi: 10.1080/19393555.2014.971553.

[13] S. Noor and T. Yusof, "Confidentiality, integrity, and availability in network systems: A review of related literature," *International Journal of Information Security Research*, vol. 14, no. 2, pp. 101–114, 2024, doi: 10.20533/ijisr.2042.4639.2024.0132.

[14] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Communications of the ACM*, vol. 17, no. 7, pp. 388–402, 1975, doi: 10.1145/360051.360056.

[15] D. Dranove, C. Forman, A. Goldfarb, and S. Greenstein, "Investment subsidies and the adoption of electronic medical records: Evidence from U.S. hospitals," *Journal of Health Economics*, vol. 44, pp. 30–43, 2015, doi: 10.1016/j.jhealeco.2015.08.006.

[16] H. Howard, M. Verbeek, and L. Alon, "Confidential consortium framework: Secure multiparty applications with confidentiality, integrity, and high availability," *IEEE Transactions on Cloud Computing*, vol. 12, no. 2, pp. 167–180, 2023, doi: 10.1109/TCC.2023.3345729.

[17] M. S. Haghighi, A. Jolfaei, and O. Nader, "A computationally intelligent hierarchical authentication and key establishment framework for IoT," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15733–15745, 2021, doi: 10.1109/JIOT.2021.3089789.

[18] P. Mishra and K. Bhardwaj, "Integrity verification in electronic medical record systems using cryptographic hash algorithms," *International Journal of Medical Informatics*, vol. 182, p. 105026, 2024, doi: 10.1016/j.ijmedinf.2024.105026.

[19] L. S. Adler-Milstein and A. K. Jha, "HITECH Act drove large gains in hospital electronic health record adoption," *Health Affairs*, vol. 36, no. 8, pp. 1416–1422, 2017, doi: 10.1377/hlthaff.2016.1651.

[20] N. T. Armah and A. Akwei, "Information security challenges in health information systems of developing countries," *BMC Medical Informatics and Decision Making*, vol. 23, no. 1, 2023, doi: 10.1186/s12911-023-02144-5.

[21] R. Kisekka and M. Giboney, "The effectiveness of health information technology in reducing medical errors: A meta-analysis," *Health Informatics Journal*, vol. 24, no. 2, pp. 124–135, 2018, doi: 10.1177/1460458216663021.

[22] S. F. Ahmed, A. O. Salman, and M. J. Islam, "Blockchain-based integrity assurance for electronic health records," *IEEE Access*, vol. 11, pp. 10012–10025, 2023, doi: 10.1109/ACCESS.2023.3234560.

[23] M. Y. Lim, J. Tan, and T. F. Nguyen, "Disaster recovery and data availability strategies in hospital information systems," *Health Informatics Journal*, vol. 30, no. 1, pp. 50–66, 2023, doi: 10.1177/14604582231245680.

[24] M. O. Odeyemi and J. N. Obiorah, "Health information security in developing countries: A review of challenges and frameworks," *Journal of Health Informatics in Developing Countries*, vol. 17, no. 2, 2023, doi: 10.12816/0123456.