International Journal of Health Science & Medical Research
Vol 5. No. 2 (2026) : August

Analysis of Data Security Governance and Interoperability of the Nationally Integrated Electronic Medical Record: A Policy Evaluation at Puskesmas Siontapina

Hamsia L Waru[1*] , La Ode Muh. Armadi. Am[2] , Nurhayati[3]

[1]Health Administration, Institut Kesehatan dan Teknologi Buton Raya , Baubau, Indonesia
[2]Infromation Technology, Institut Kesehatan dan Teknologi Buton Raya, Baubau, Indonesia
[3]Health Administration, Institut Kesehatan dan Teknologi Buton Raya , Baubau, Indonesia
Email : hamsia.lw@gmail.com

Abstract

This study evaluates the effectiveness of security governance and Electronic Medical Record (EMR) interoperability policies at *Puskesmas* Siontapina using a mixed-methods approach based on the CIPP and CIA Triad frameworks. Data were collected from 30 users through interviews, observations, and questionnaires. The results indicate that the implementation is not yet aligned with existing regulations. The practice of account sharing threatens confidentiality, driven by the staff's low security literacy (80% in the moderate-to-low categories). System availability is hindered by downtime caused by the absence of an Uninterruptible Power Supply (UPS). Application Programming Interface (API) synchronization failures, resulting from mismatches between local codification and HL7 FHIR as well as ICD-10 standards, impede semantic interoperability, thereby triggering administrative redundancy. In conclusion, EMR governance is not yet optimal; there is an urgent need for cybersecurity education, infrastructure reinforcement, and proactive vendor audits.

Keywords: Electronic Medical Records; Data Governance; Data Security; Interoperability; Policy Evaluation

INTRODUCTION

Digital transformation in the healthcare sector has become a global inevitability that redefines the delivery and management of healthcare services. At the center of this transformation, Electronic Medical Records (EMR) play a crucial role as the foundation of modern health information systems. EMRs do not merely digitize paper documents but integrate patients' clinical data in a real-time, structured, and longitudinal manner (1). The optimal utilization of EMRs has been empirically proven to improve administrative efficiency, minimize medical errors, support the continuity of care, and enhance overall clinical outcomes (2).

Received:Aug14th, 2026;1st Revised: Aug29th,2026;
Accepted forPublication:Aug31th, 2026

In Indonesia, the commitment to healthcare digitization is realized through assertive policies by the central government. The Ministry of Health of the Republic of Indonesia issued the Minister of Health Regulation (Permenkes) No. 24 of 2022, which mandates all healthcare facilities to implement integrated EMRs no later than December 31, 2023 (3). Beyond mere system adoption, this policy requires healthcare facilities to connect and be capable of exchanging data (interoperability) with the national digital health ecosystem platform, SATUSEHAT. From a protection perspective, this data governance directly intersects with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which classifies health data as specific high-risk data, thereby demanding multi-layered security (4).

However, the transition toward a nationally integrated system introduces new complex challenges, particularly regarding data governance and security. EMRs store highly sensitive patient data; therefore, the principles of confidentiality, integrity, and availability must be guaranteed (5). Cybersecurity vulnerabilities, the lack of access control standards for healthcare professionals, and the potential for data breaches due to system weaknesses pose actual threats. Without adequate data security governance, EMR implementation could compromise patient privacy and trigger legal implications for healthcare facilities.

These governance issues become increasingly complicated when faced with the interoperability mandate. Interoperability is not merely the ability of healthcare facilities to have an internet connection for transmitting data, but rather the capability of different systems (across vendors/developers) to exchange, understand, and use clinical data uniformly at both the syntactic and semantic levels (6). The primary challenges in the field include the fragmentation of information systems at the primary healthcare facility level, variations in programming languages, and the lack of uniformity in data architecture. Interoperability failures have a direct impact on fragmented medical referral histories, the redundancy of diagnostic tests, and the financial inefficiency of the National Health Insurance (JKN) (7).

In the context of primary care in regional areas, these conditions present highly specific implementation challenges. *Puskesmas* Siontapina, as a strategic First-

Level Healthcare Facility (FKTP) in Buton Regency, is required to comply with this national integration mandate. As a primary care institution bordering archipelagic geographical characteristics, the operationalization of EMR at *Puskesmas* Siontapina faces issues regarding network infrastructure stability, the digital literacy readiness of its human resources for health (HRH), and the administrative governance of system bridging between third-party vendors and the SATUSEHAT servers.

Based on a literature review of national publications in the field of health information systems, there is a significant research gap following the enactment of Minister of Health Regulation No. 24 of 2022. The majority of previous studies conducted before the national integration deadline tended to focus on analyzing institutional readiness in adopting basic technologies. This is evident in studies (8) and (9), which still centered on measuring the cognitive readiness of human resources and physical infrastructure using basic frameworks such as DOQ-IT.

Furthermore, policy and administrative studies during that phase primarily highlighted the barriers to the initial adoption of EMRs in healthcare facilities. Systematic evaluations conducted by (10) and (11) confirmed that user resistance, limited budgets, and the complexity of interface designs remained the main topics investigated as implementation barriers in *Puskesmas* and other primary care institutions.

Entering the current post-mandatory implementation phase of the SATUSEHAT ecosystem, the urgency and direction of digital health evaluation in Indonesia have shifted. As asserted by (12,13,14), EMR challenges no longer merely demand hardware availability at registration counters, but rather the quality of cross-system data interoperability and the guarantee of privacy protection. Unfortunately, comprehensive evaluations examining cybersecurity governance (the principles of Confidentiality, Integrity, and Availability) in first-level healthcare facilities located in archipelagic or coastal areas remain severely understudied.

The urgency of this study lies in the pressing need to ensure that the mandate for national EMR integration does not merely become a regulatory box-ticking exercise, but is genuinely implemented with secure technical and ethical governance. The results of this study will provide practical contributions in the form of evaluative recommendations for the management of *Puskesmas* Siontapina and the Buton Regency Health Office in formulating Standard Operating Procedures (SOPs) for infrastructure improvement and data

security access management.

Academically, this study enriches the literature on health administration and policy regarding the implementation of digital health ecosystems in developing countries, particularly in regions with infrastructure disparities.

RESEARCH METHOD

This study employed a Mixed Methods approach with a Concurrent Embedded design, in which the qualitative method served as the primary method and the quantitative method as the secondary support (15). Specifically, this type of research is a policy evaluation study. The evaluation framework utilized was the CIPP (Context, Input, Process, Product) Model (16). This model was selected because it is the most comprehensive for evaluating a program from upstream to downstream, starting from the legal basis of EMR integration (Context), infrastructure readiness and security SOP governance (Input), the implementation of system bridging and data access (Process), to the final outcomes in the form of service efficiency and smooth data interoperability with the SATUSEHAT platform (Product).

The focus of this study was divided into two main dimensions integrated within the CIPP model. First, Data Security Governance, which was analyzed using the core information security principles of the CIA Triad: Confidentiality (access right control for healthcare professionals and patient privacy protection), Integrity (completeness and audit trails of medical data modifications), and Availability (system availability, downtime mitigation, and server backup) (17). Second, EMR Interoperability, which focused on the success of data exchange (bridging) between the vendor system of *Puskesmas* Siontapina and the Ministry of Health's database, compliance with data standardization formats, and technical network constraints.

Based on the background, problem identification, and aforementioned urgency, this study aims to analyze data security governance and evaluate the effectiveness of the nationally integrated Electronic Medical Record interoperability policy at *Puskesmas* Siontapina, Buton Regency.

The determination of qualitative informants employed a purposive sampling technique based on the principles of adequacy and appropriateness (authority and knowledge). The key informants consisted of: (1) the Head of *Puskesmas* Siontapina as the internal policymaker; (2) the Person in Charge of Information Systems/IT at the *Puskesmas*; and (3) the

Medical Record Coordinator. For quantitative data collection, a total sampling technique was used, encompassing all healthcare professionals and administrative staff utilizing the EMR system at *Puskesmas* Siontapina.

The primary instrument in the qualitative research was the researcher themselves, assisted by an interview guide. Supporting instruments included a data security governance observation checklist, an SOP document evaluation sheet, and a closed-ended Likert scale questionnaire to measure user perception and readiness. Quantitative data analysis was conducted using univariate descriptive statistics to generate percentages and frequencies.

Qualitative data analysis utilized the interactive model by Miles, Huberman, and Saldaña (18), which encompasses three concurrent stages: (1) Data condensation, namely sorting and summarizing interview transcripts related to data security; (2) Data display in the form of a thematic narrative based on the CIPP evaluation matrix; and
(3) Conclusion drawing and verification regarding the effectiveness of the policy in the field. The qualitative and quantitative data were then interpreted concurrently to answer the research questions.

RESULTS AND DISCUSSION

Result

Based on the study utilizing the CIPP evaluation framework and the CIA Triad principles, a comprehensive overview of data security governance and EMR interoperability at *Puskesmas* Siontapina was discovered. The research findings are presented in three main aspects: Data Security Governance, System Interoperability, and Human Resources (HR) Literacy Readiness.

Data Security Governance

In the Process and Product stages, the interoperability of *Puskesmas* Siontapina's EMR with the national SATUSEHAT platform has generally been operational, although not yet fully stable. Frequent technical barriers encountered include API synchronization failures due to mismatches in mapping the local *Puskesmas* data with the HL7 FHIR (Fast Healthcare Interoperability Resources) architectural standards mandated by SATUSEHAT. An informant stated, "Error notifications frequently appear when the API attempts to send visit data..." This failure predominantly occurs during the semantic interoperability process, particularly when the system attempts to synchronize disease diagnostic code variables (based on ICD-10) that have not been uniformly mapped by third-party vendors. Frequent technical

barriers encountered include API synchronization failures due to mismatches in mapping the local *Puskesmas* data with the HL7 FHIR architectural standards mandated by SATUSEHAT. An informant stated, "Error notifications frequently appear when the API attempts to send visit data..." This failure predominantly occurs during the semantic interoperability process, particularly when the system attempts to synchronize disease diagnostic code variables (based on ICD-10) that have not been uniformly mapped by third-party vendors.

Data Security Literacy Readiness

The results of quantitative data collection from 30 EMR user respondents at *Puskesmas* Siontapina regarding data security literacy readiness can be seen in Table 1 below:

Table 1. Data Security Literacy Readiness Category

Data Security Literacy Category	Score Range	Number of Respondents (N)	Percentage (%)
High	37–48	6	20%
Moderate	25–36	16	53.33%
Low	12–24	8	26.67%
Total		**30**	**100%**

Sources: Primary Data, 2026

Based on Table 1 above, it is indicated that the majority of staff possess a data security literacy level in the Moderate category, amounting to 16 respondents (53.33%). Meanwhile, 8 respondents (26.67%) are in the Low category, and only 6 respondents (20%) are classified in the High category.

This suboptimal literacy level aligns with the Input evaluation findings in the qualitative analysis, where HR training by the vendors has thus far only focused on the technical use of the application, while specific training related to cybersecurity and data protection remains scarce or inadequately provided.

Electronic Medical Record Interoperability

In the Process and Product stages, the interoperability of *Puskesmas* Siontapina's EMR with the national SATUSEHAT platform has generally been operational, although not yet fully stable. Frequent technical barriers encountered include API synchronization failures due to mismatches in mapping the local *Puskesmas* data with the HL7 FHIR (Fast Healthcare Interoperability Resources) architectural standards mandated by SATUSEHAT.

An informant stated, "Error

notifications frequently appear when the API attempts to send visit data..." This failure predominantly occurs during the semantic interoperability process, particularly when the system attempts to synchronize disease diagnostic code variables (based on ICD-10) that have not been uniformly mapped by third-party vendors. Frequent technical barriers encountered include API synchronization failures due to mismatches in mapping the local *Puskesmas* data with the HL7 FHIR architectural standards mandated by SATUSEHAT. An informant stated, "Error notifications frequently
appear when the API attempts to send visit data..." This failure predominantly occurs during the semantic interoperability process, particularly when the system attempts to synchronize disease diagnostic code variables (based on ICD-10) that have not been uniformly mapped by third-party vendors.

Discussion

Analysis of Data Security Governance

The finding regarding the ongoing practice of account sharing among staff at the polyclinic service level is a critical phenomenon. This condition can be explained by the staff's low data security literacy, where a cumulative 80% of the staff are at the Moderate to Low literacy levels, triggered by the lack of cybersecurity education from both the vendors and management. From the perspective of the CIA Triad theory, the practice of account sharing directly violates the confidentiality principle (Confidentiality) and obscures the audit trail of access, thereby threatening the integrity principle (Integrity) as well, because the system can no longer identify the actual user who modifies the data.

These findings indicate a misalignment between upstream policies and downstream implementation in primary healthcare facilities. The policy mandates the protection of patients' medical data as specific high-risk data; however, workload pressure and the pragmatic habits of healthcare professionals (prioritizing service speed) cause security SOPs to be ignored. The availability condition (Availability) which is frequently disrupted due to infrastructure barriers in coastal or archipelagic areas (weather and electricity).

Analysis of System Interoperability and Integration

Interoperability is not merely the availability of a connection, but rather the ability of two different systems to understand the meaning of the transferred data. Barriers to API transmission due to unsynchronized code formats indicate that

the EMR system at *Puskesmas* Siontapina has not fully achieved semantic-level interoperability. This API synchronization failure proves that the interoperability achievement at *Puskesmas* Siontapina is only at the syntactic interoperability stage (basic connectivity) but still fails at the semantic interoperability level. The Minister of Health Regulation No. 24/2022 policy has indeed encouraged healthcare facilities to connect, but the lack of technical oversight over system provider vendors in regional areas causes data standard fragmentation (such as mismatches in the ICD-10 master data).

Consequently, instead of reducing the workload, this digitization actually creates administrative redundancy because staff must manually correct JSON payloads for the data to be accepted by the central server.

Analysis of Policy and Implementation Gaps

To measure policy effectiveness, this evaluation compares the prevailing regulatory standards with the operational reality in the field. The gap analysis of EMR implementation at *Puskesmas* Siontapina is classified into the following three critical aspects:

Gaps in the Confidentiality Aspect

1. **Gap Point:** Regulatorily, the PDP Law and Minister of Health Regulation No. 24/2022 mandate the protection of specific data privacy and compliance with exclusive access. However, in its implementation, violations of Standard Operating Procedures (SOPs) regarding Role-Based Access Control (RBAC) were found, such as the common practice of account sharing among healthcare professionals and weak physical security (monitor screens vulnerable to peeking or *shoulder surfing*).
2. **Causes and Impacts:** This gap is triggered by the dominance of staff with moderate-to-low security literacy levels (80%) faced with the pressure of a heavy burden of patient queues. Consequently, this condition obscures the audit trail, making medical accountability difficult to justify, and increases the risk of internal data manipulation.
3. **Recommendations:** Interventions are required in the form of periodic cybersecurity training, the activation of the auto-lock screen feature, and repositioning the monitors in the polyclinic rooms.

Gaps in the Availability Aspect

1. **Gap Point:** Digital transformation standards mandate healthcare facilities

to have systems that support real-time continuous medical services (business continuity). In fact, the system availability level does not reach 100% due to frequent downtime during power outages (waiting for the generator transition period) and internet disconnections caused by weather.

2. **Causes and Impacts:** The root of this instability is the absence of critical security infrastructure in the form of an Uninterruptible Power Supply (UPS) at workstations and the lack of a backup internet network. This impacts delayed medical services and forces staff to revert to manual paper recording methods, which triggers high administrative work redundancy.
3. **Recommendations:** Healthcare facility management must prioritize the procurement of individual UPS for each service computer and install a balancer router equipped with a backup internet connection (cellular/satellite).

Gaps in the Interoperability (Data Integration) Aspect

1. **Gap Point:** The Ministry of Health's SATUSEHAT ecosystem demands seamless data exchange in accordance with the HL7 FHIR architectural standards. However, the achievement at *Puskesmas* Siontapina shows that the vendor system has not fully reached the semantic interoperability level. This is evidenced by the frequent appearance of error notifications (payload rejected) when the API (Application Programming Interface) sends data to the central server.
2. **Causes and Impacts:** This failure is predominantly caused by code mapping (particularly ICD-10 diagnoses) in the vendor's system that is not yet synchronized with the national master data. This operational failure results in delayed national health data reporting and burdens staff with administrative redundancy, as they must manually correct the data format and resend it.
3. **Recommendations:** The *Puskesmas* needs to urge the developer vendor to conduct proactive API system audits and provide a dynamic ICD-10/KFA code mapping module to align with the Ministry of Health's parameters.

CONCLUSION AND RECOMMENDATION

This study concludes that the implementation of the nationally integrated Electronic Medical Record (EMR) governance and interoperability policy at *Puskesmas* Siontapina still faces significant operational gaps, although managerially it

has been founded on an understanding of Personal Data Protection regulations. In terms of security governance, the fulfillment of confidentiality and integrity principles is hindered by weak physical access controls and the practice of account sharing among healthcare professionals, triggered by the heavy burden of patient queues and uneven cybersecurity literacy levels.

Furthermore, operational reliability (availability) is highly vulnerable to electrical and network infrastructure instability without adequate backup power support. From the interoperability aspect, the integration achievement with the SATUSEHAT platform has only reached the basic connectivity (syntactic) stage but remains constrained at the semantic interoperability level due to the misalignment of diagnostic code mapping between third-party vendor systems and national architectural standards (HL7 FHIR and ICD-10).

This condition conversely results in administrative redundancy for staff in primary care facilities. These findings imply that the success of digital health transformation in regions with geographical challenges cannot solely rely on fulfilling application connectivity mandates. This evaluation underscores the need for a policy paradigm shift, moving from a mere focus on technology adoption deadlines toward the holistic strengthening of an "information security culture." For healthcare facility management and regional health authorities, budgetary interventions must be prioritized for reinforcing critical security infrastructure (such as the provision of individual UPS), disciplined enforcement of Standard Operating Procedures (SOPs), and the execution of proactive API system audits in collaboration with developer vendors to ensure compliance with national data standards.

REFERENCES

1. Kruse CS, Smith B, Murphy H, Weston J. Utility, privacy, and security of electronic health records. J Med Syst. 2018;42(12):214.
2. Atasoy H, Greenwood BN, McCullough JS. The digitization of patient care: A review of the effects of electronic health records on health care quality and utilization. Annu Rev Public Health. 2019;40:487-500.
3. Kementerian Kesehatan Republik Indonesia. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022. Jakarta: Kementerian Kesehatan Republik Indonesia; 2022.
4. Pemerintah Republik Indonesia. Undang-Undang Republik Indonesia

Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Jakarta: Sekretariat Negara Republik Indonesia; 2022.

5. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egypt Inform J. 2021;22(2):177-83.
6. Lehne M, Sass J, Essenwanger A, Schepers J, Thun S. Why digital medicine depends on interoperability. NPJ Digit Med. 2019;2(1):79.
7. Kementerian Kesehatan Republik Indonesia. Cetak biru strategi transformasi digital kesehatan 2024. Jakarta: Kementerian Kesehatan Republik Indonesia; 2021.
8. Hapsari MA, Mubarokah K. Analisis Kesiapan Pelaksanaan Rekam Medis Elektronik (RME) Dengan Metode Doctor's Office Quality-Information Technology (DOQ-IT) di Klinik Pratama Polkesmar. J-REMI: Jurnal Rekam Medik dan Informasi Kesehatan. 2023 Mar 31;4(2):75-82.
9. Putra AW, Sutha DW. Analisis Kesiapan Penerapan Rekam Medis Elektronik dengan Metode DOQ-IT: Narrative Review. Jurnal Ilmiah Perekam dan Informasi Kesehatan Imelda (JIPIKI). 2025 Aug 31;10(2):132-47.
10. Prasojo IB, Ulfah NH, Mawarni D, Redjeki ES. Analisis faktor penghambat penerapan sistem informasi manajemen puskesmas di Indonesia: Literature review. Journal of Applied Science for Pharmaceuticals and Health. 2024;1(1):26-42.
11. Bella CR, Ummah S, Isnaeni R. Evaluasi Sistem Informasi Manajemen Puskesmas (SIMPUS) dengan Pendekatan HOT-Fit Model di Puskesmas Baturraden II. Indonesian of Health Information Management Journal (INOHIM). 2025 Jun 30;13(1):29-41.
12. Putri RD, Mulyanti D. Tantangan SIMRS dalam penerapan rekam medis elektronik berdasarkan Permenkes 24 Tahun 2022: Literature review. Jurnal Medika Nusantara. 2023 Feb 28;1(1):18-28.
13. Widasari IV, Ikawati FR, Ma'ruf AS. Literature Review: Tantangan Interoperabilitas Rekam Medis Elektronik di Fasilitas Kesehatan. Jurnal Manajemen Informasi Kesehatan (Health Information Management). 2025 Dec 4;10(2):238-46.
14. Pradita R, Fitriana SM. Implementasi standar interoperabilitas HL7-FHIR pada pertukaran rekam kesehatan elektronik di puskesmas. Jurnal Ilmiah Perekam dan Informasi Kesehatan

Imelda (JIPIKI). 2024 Feb 29;9(1):20-30.

15. Creswell JW, Creswell JD. Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications; 2017 Dec 12.
16. Suryadin A, Sari WP, Nurfitriani MP. Evaluasi program model CIPP (Context, Input, Process, and Product) antara teori dan praktiknya. SamudraBiru; 2022 Nov 30.
17. Kurniawan D, Rojabi MA. Mengenal profesi IT security. Afdan Rojabi Publisher; 2025 Nov 17.
18. Huberman AM. Qualitative data analysis a methods sourcebook;2014