Multidisciplinary Output Research For Actual and International Issue (MORFAI Journal) ISSN (e): 2808-6635
Volume 5 No. 4 (2025)

ANALYSIS OF IMPROVING ORGANIZATIONAL COMPETITIVENESS THROUGH IMPLEMENTATION OF SIMRS SECURITY SYSTEM IN HOSPITALS: LITERATURE REVIEW

Ranita Rizky Putri[1]*, Kosasih[2]
Universitas Sangga Buana Bandung
E-mail: ranitarizkyp@gmail.com[1], kosasih@usbypkp.ac.id[2]

Received	: 01 August 2025	Published	: 04 October 2025
Revised	: 15 August 2025	DOI	: https://doi.org/10.54443/morfai.v5i4.4201
Accepted	: 25 September 2025	Publish Link	: https://radjapublika.com/index.php/MORFAI/article/view/4201

Abstract

This literature review aims to analyze the role of Hospital Management Information System (SIMRS) security in enhancing the organizational competitiveness of hospitals in Indonesia. SIMRS has become a crucial instrument in supporting efficiency, transparency, and the quality of healthcare services. However, the growing use of electronic medical records also presents serious challenges related to patient data security and privacy. This study reviews 10 national publications issued between 2017 and 2025, focusing on SIMRS security issues. The findings reveal that the main challenges lie in weak access control, insufficient encryption, limited audit logs, and the suboptimal implementation of basic security features such as auto logout. Moreover, patient privacy aspects such as consent mechanisms, role-based access, and the principle of data minimization are rarely applied. Managerial factors, including low awareness among healthcare staff and weak internal policies, further exacerbate security risks. Overall, the success of SIMRS implementation is determined not only by technological sophistication but also by regulatory compliance, managerial commitment, and ethical awareness among healthcare workers. Strengthening SIMRS security is considered a strategic investment to enhance patient trust, strengthen hospital reputation, and support organizational competitiveness in the digital era.

Keywords: ***confidentiality, hospital management information system, information security, patient data, privacy***

INTRODUCTION

In an era of rapidly developing technology and information, hospitals need to improve their performance and competitiveness without neglecting their social mission. This effort is carried out by developing strategic policies for the organization, management, and human resources, as well as making decisions quickly and accurately. This way, the quality of healthcare services can be improved, while hospitals remain innovative, efficient, and profitable organizations while maintaining their social commitments (Handiwidjojo, 2015). The development of information technology in the healthcare sector has brought about significant changes in patient data management. Organizational competitiveness is now determined not only by the quality of clinical services but also by the ability to manage data and information securely, efficiently, and in accordance with regulations. The Hospital Management Information System (SIMRS) is a crucial instrument in supporting service efficiency, medical record management, and strategic decision-making. However, with the increasing use of SIMRS, serious challenges have emerged regarding the security of sensitive patient data that must be kept confidential. Cases of patient data leaks in several hospitals in Indonesia demonstrate the weaknesses of the SIMRS security system, both technically and non-technically (Wibowo, 2020). The security of patient data in SIMRS is crucial, considering that medical confidentiality is a patient right guaranteed by law. Several studies have shown that threats to the security of SIMRS information are real. Listyorini (2021) highlighted that patient data can be exposed due to security gaps, both technical and system management. Meanwhile, research by Lestari and Nugroho (2022) using the HOT-FIT framework emphasized that technological, organizational, and human aspects are often weak points that have the potential to compromise SIMRS reliability. In Indonesia, the importance of patient data protection in SIMRS is further emphasized by regulations such as Minister of Health Regulation No. 24 of 2022 concerning Electronic Medical Records and Law No. 27 of 2022 concerning Personal Data Protection (PDP). These regulations emphasize that SIMRS implementation must prioritize the principles of security, integrity, and confidentiality of patient data. However, various studies have shown that weaknesses in the implementation of SIMRS data security remain, such as limited infrastructure, lack of

user awareness, and the ever-growing threat of cyberattacks. Therefore, analyzing SIMRS security systems through literature review is crucial to provide an overview of research findings, existing weaknesses, and efforts made in the context of hospitals in Indonesia.

LITERATURE REVIEW

The Hospital Management Information System (SIMRS) is an integrated system applied to support the entire healthcare process, from administration and clinical services to patient medical record management. Regulations require every hospital to implement SIMRS to improve efficiency, transparency, and the quality of healthcare services. According to Minister of Health Regulation No. 82 of 2013, SIMRS aims to improve the efficiency, effectiveness, and quality of healthcare services in hospitals. In its implementation, SIMRS can reduce recording errors, accelerate workflows, and facilitate real-time access to patient data (Kurniawati, Wulandari, & Priyono, 2020). Optimal SIMRS implementation can drive improvements in service quality and hospital management effectiveness. However, along with its use, significant challenges arise regarding patient data security. Health data is sensitive and protected by regulations, such as Law No. 27 of 2022 concerning Personal Data Protection and Minister of Health Regulation No. 24 of 2022 concerning Electronic Medical Records. Therefore, data leaks can have legal, ethical, and social consequences (Wibowo, 2020). However, these benefits can only be achieved if the system is supported by adequate technological infrastructure and strict security policies.

With the increasing prevalence of digitalization, data security and privacy have become crucial issues. Patient data and sensitive hospital information are more vulnerable to cyber threats such as hacking and data theft (Kosasih et al. 2025). Information security in the Hospital Management Information System (MISRS) is a crucial issue because it directly relates to the protection of sensitive patient data. Listyorini (2021) emphasized that weaknesses in security management, such as the lack of data encryption or weak access controls, can open up opportunities for information leaks. Furthermore, Lestari and Nugroho (2022) found that human factors, such as a lack of training among healthcare workers in information security, contribute to increasing the risk of system vulnerabilities. Therefore, the SIMRS security approach must encompass three main aspects: technology, organization, and people, to ensure service continuity and maintain patient trust in the hospital institution.

Furthermore, research by Yaner, Tanuwijaya, and Sutomo (2022) conducted an information security audit of the SIM-RS installation at Haji General Hospital in Surabaya based on ISO 27002 standards. The audit revealed weaknesses in physical and operational access controls, including external access to the data center space, data manipulation, and inadequate user authorization. Similar findings emerged at the Tasikmadu Community Health Center in Karanganyar, where the SIMPUS application had not implemented automatic log-off, increasing the risk of misuse of user access (Amir & Fadlil, 2021). Furthermore, recent research reinforces the importance of security aspects in SIMRS. Laila, Sulistyawati, and Hidayat (2024) stated through a literature review that although SIMRS has been widely implemented in Indonesia, security aspects such as authentication, access control, and data protection remain inconsistent. Firmansyah et al. (2023) in their research at Bunda Margonda General Hospital found that despite the existence of security SOPs, many staff still do not use unique credentials, and the absence of an automatic logout feature has the potential to lead to unauthorized access. Meanwhile, Sihole, Lesmana, and Wasir (2024) emphasized that the SIMRS development strategy needs to incorporate cybersecurity elements from the planning stage, so that the system focuses not only on efficiency but also on resilience against digital threats.

Data securityThe SIMRS refers to the fulfillment of the principles of confidentiality, integrity, and availability. Research by Wilar (2023) confirms that weaknesses in access control, encryption, and backup systems can open up opportunities for data leaks. Meanwhile, Listyorini and Sintya (2021) highlight threats originating from cyberattacks and insider threats, necessitating mitigation strategies such as audit logs, multi-factor authentication, and security training for staff. A study at Sukapura Islamic Hospital in Jakarta also showed that basic security features, such as auto-logout, are still suboptimal, increasing the risk of unauthorized access (Wardani et al., 2024). Patient data privacy is another equally important aspect. Afifah, Suhariyono, and Ikawati (2025) in their research at Karangploso Community Health Center found that privacy practices often do not fully meet standards, particularly in the regulation of role-based access rights. This aligns with Bahaji's (2025) findings, which identified a lack of awareness among healthcare workers, a lack of internal policies, and weak regulatory enforcement as key challenges in maintaining patient data privacy and security in Indonesia. Overall, the literature indicates that implementing a SIMRS requires not only robust technological tools but also a risk management system, consistent regulations, and compliance from all parties involved. Without further security and privacy management, SIMRS implementation has the potential to cause significant losses for both hospitals and patients.

Hospital Information System security is not only related to data protection but also has strategic implications for organizational competitiveness. The competitiveness of hospital organizations in the digital era is greatly influenced by the ability to maintain the security of health information. In the hospital context, patient data security is a critical differentiation factor. Hospitals that are able to protect data effectively will gain greater trust from patients and partners, thereby enhancing their reputation and expanding market share. This aligns with Ningsih's (2023) findings that transparency and consent mechanisms in Hospital Information System contribute to patient loyalty, which in turn strengthens the hospital's competitive position. Afifah, Suhariyono, and Ikawati (2025) found that role-based access control improves service effectiveness while maintaining patient privacy. Bahaji's (2025) research confirms that weak internal regulations and low awareness among healthcare workers weaken hospital competitiveness, while consistent implementation of security policies can strengthen the institution's reputation. Furthermore, research by Wardani, Andriani, and Salsabila (2024) shows that basic security features, such as auto-logout and dual authentication, can increase patient trust in hospital service systems. Furthermore, organizational competitiveness is closely related to compliance with international regulations and standards. Putri and Saputra (2024) showed that hospitals that adopt the ISO 27001 standard in their security systems have higher credibility than those that do not. This compliance not only minimizes legal risks but also increases the organization's marketability in the face of competitive healthcare services. Therefore, implementing a standardized SIMRS security system can be seen as a long-term strategy to ensure the sustainability and competitive advantage of hospitals.

METHOD

This article uses a literature review method by extracting 10 research titles conducted in Indonesia that are relevant to the topic of SIMRS security. The literature search process was conducted through Google Scholar and national journal portals with the keywords 'SIMS security', 'electronic medical records', and 'hospital patient data'. Inclusion criteria were articles in Indonesian, published between 2015–2025, and focused on the hospital context.

RESULTS AND DISCUSSION

The implementation of SIMRS in Indonesian hospitals generally still faces several obstacles, particularly in infrastructure, human resources, and regulatory compliance. Although the Ministry of Health (2013) has emphasized the mandatory implementation of SIMRS, many hospitals still face budget constraints and a lack of integration between units. This situation impacts the quality of service and the speed of data-driven decision-making (Listyorini & Sintya, 2021).From a security perspective, research by Wardani, Andriani, and Salsabila (2024) shows that basic security features, such as auto-logout and access control, have not been fully implemented, leaving patient data vulnerable to unauthorized access. Wilar (2023) also highlighted threats such as malware attacks, network hacking, and insider threats from internal hospital staff. The lack of encryption and weak audit logs increase the potential for information leaks, which can be detrimental to both hospitals and patients.

To minimize these threats, several security strengthening strategies have been recommended. Commonly used technical approaches include multi-factor authentication, data encryption, scheduled backup systems, and firewalls (Listyorini & Sintya, 2021; Wilar, 2023). Furthermore, managerial policies also play a crucial role, such as through routine audits, healthcare worker training, and the development of clear standard operating procedures (SOPs) regarding data access mechanisms. Research by Afifah, Suhariyono, and Ikawati (2025) emphasized the need for role-based access control to ensure that medical information can only be accessed according to professional needs and authority. However, patient privacy remains a low priority in most healthcare facilities. Afifah et al. (2025) found that patient consent and data minimization principles are often neglected in the implementation of a Hospital Management Information System (MISRS).

This is further supported by Bahaji's (2025) findings, which state that low awareness among healthcare workers and weak internal regulations are key barriers to patient data protection. Therefore, transparency in data management and ensuring patients' rights to know how their data is used are crucial steps in maintaining public trust. Overall, the literature review confirms that the success of a SIMRS implementation is determined not only by the sophistication of technological devices but also by regulatory synergy, ethical awareness of healthcare workers, and support from hospital managers. Without strong integration between technical and non-technical aspects, a SIMRS has the potential to pose greater legal, ethical, and social risks (Bahaji, 2025). The implementation of a Hospital Information System (SIMS) security system has been proven to have a direct impact on increasing hospital competitiveness. Data security increases patient trust, which simultaneously strengthens loyalty and expands the reach of healthcare services (Ningsih, 2023). A strong security system is certainly a supporting factor for service efficiency because it reduces the risk of operational disruptions due to data leaks or cyberattacks (Yuniarti & Hidayat,

2022). Compliance with national regulations increases credibility, making hospitals more competitive in the competitive healthcare market (Wibowo, 2020). Furthermore, the organizational reputation created by successfully maintaining patient data security serves as a strategic differentiation compared to other hospitals that are still weak in this aspect. From a managerial perspective, Hospital Information System (SIMS) security should be viewed as a strategic investment. Hospitals that allocate resources to strengthening infrastructure, training human resources, and consistently implementing security policies will reap long-term benefits in the form of service sustainability and competitive advantage. This aligns with Bahaji's (2025) statement that the success of healthcare organizations in the digital era is determined not only by technological sophistication but also by regulatory synergy, managerial commitment, and ethical awareness of healthcare workers.

No	Author & Year	Research Title	Focus / Key Findings	Relevance to Competitiveness
1	Listyorini & Sintya (2021)	SIMRS security system in hospitals	Identifying SIMRS security threats; the need for audit logs & layered authentication	Audit logs & authentication increase patient trust and prevent reputational loss.
2	Wilar (2023)	SIMRS security analysis	Encryption & access control weaknesses; cyber attack risks	Strong encryption enhances data protection & competitive advantage
3	Wardani, Andriani, & Salsabila (2024)	SIMRS Security at Sukapura Islamic Hospital, Jakarta	The auto logout feature is not optimal; access control is weak.	Access control both improves service efficiency & reduces legal risks
4	Afifah, Suhariyono, & Ikawati (2025)	Patient data security at Karangploso Community Health Center	Access rights are not yet role-based; policies are not yet consistent.	*Role-based access*improve service effectiveness & maintain patient privacy
5	Bahaji (2025)	SIMRS data security challenges in Indonesia	Weak internal regulations & low HR awareness	Regulatory compliance & HR improvement strengthen organizational competitiveness
6	Yuniarti & Hidayat (2022)	Implementation of web-based SIMRS in regional hospitals	SIMRS improves efficiency; constraints on server disruptions	System stability supports fast & efficient service
7	Rachmawati et al. (2021)	Evaluation of electronic medical records in teaching hospitals	Data duplication & risk of losing technical information	Good data management improves service accuracy & patient satisfaction
8	Pratama & Setiawan (2022)	SIMRS security analysis at RSUD	The need for firewalls, IDS/IPS, & encryption	Security infrastructure improves service resilience & competitiveness
9	Ningsih (2023)	Patient data privacy in SIMRS	Patients are less aware of their right to privacy; there is no consent mechanism.	Transparency & consent increase patient loyalty & hospital reputation
10	Princess & Saputra (2024)	ISO 27001 based SIMRS security audit	Low maturity level on security standards	ISO certification improves the credibility & competitive position of hospitals

Table 1. Data Extraction Results

Table 1 shows that the majority of research in Indonesia highlights technical security issues such as weak encryption, access control, and server vulnerabilities (Listyorini & Sintya, 2021; Wilar, 2023; Pratama & Setiawan, 2022). Furthermore, several studies also confirm that basic security features such as auto-logout and audit logs are often neglected, opening up opportunities for unauthorized access (Wardani et al., 2024). On the other hand, patient privacy still faces significant challenges. Research by Ningsih (2023) and Afifah et al. (2025) shows that patient privacy rights are often poorly managed, particularly regarding consent and role-based access rights. Afifah, Suhariyono, and Ikawati (2025) found that implementing role-based access control contributes to increased service effectiveness and data privacy, while Bahaji (2025) highlighted that weak internal regulations and low awareness among healthcare workers are major obstacles to maintaining data security. This demonstrates that the competitiveness of a hospital organization is determined not only by its technological infrastructure, but also by management policies, regulatory compliance, and the ethical awareness of all parties involved. Furthermore, a study by Putri and Saputra (2024) confirmed that ISO 27001 certification can be a crucial instrument in enhancing a

hospital's credibility in the public eye. This is reinforced by the findings of Ningsih (2023), who emphasized that transparency in data management and consent mechanisms are crucial factors in building patient trust. Thus, the empirical study table shows that the security of a hospital's information system (MISRS) has dual implications: as a technical instrument for protecting data, and as a differentiation strategy that serves to strengthen hospital competitiveness by increasing trust, efficiency, reputation, and regulatory compliance.

CONCLUSION

This literature review shows that the implementation of the Hospital Management Information System (SIMRS) in Indonesia has provided significant benefits in improving service efficiency, administrative transparency, and supporting data-driven decision-making. However, SIMRS implementation still faces several challenges, particularly in terms of patient data security and privacy. From a security perspective, various studies have revealed weaknesses in access control, encryption, audit logs, and suboptimal basic security features. Meanwhile, patient privacy remains under-appreciated, as evidenced by the weak implementation of the principles of consent, data minimization, and transparency. However, SIMRS security should also be viewed as a strategic investment that supports hospital sustainability, competitive advantage, and differentiation amidst increasingly fierce healthcare competition. Overall, this study confirms that SIMRS success is determined not only by technological sophistication, but also by the commitment of hospital management, regulatory compliance, and healthcare personnel's awareness of maintaining patient data security and privacy.

REFERENCES

Afifah, N., Suhariyono, US, & Ikawati, FR (2025). Analysis of information security aspects of patient data in electronic medical records at the Karangploso Community Health Center. Indonesian Journal of Health Information Management (JMIKI), 13(1).

Amir, MS, & Fadlil, A. (2021). Security analysis of the community health center management information system using COBIT 5 at the Tasikmadu Karanganyar Community Health Center. Indonesian Journal of Health Information Management, 9(2), 142–153.

Bahaji, AF (2025). Analysis of data security challenges and strategies in health service information systems in Indonesia: Literature review. ResearchGate.

Firmansyah, MP, Utama, T., Sadikin, H., Romlah, SN, & Apriliyanti, R. (2023). Review of the implementation of Hospital Management Information System (SIMRS) security features in the medical records unit at Bunda Margonda General Hospital in 2023. EDU RMIK: Journal of Medical Records Education and Health Information, 2(2), 112–120.

Handiwidjojo, W. (2015). Hospital Management Information System. Journal of Exploration of Information Systems and Science Works, 2(2).

Kosasih, D., Paramarta, HV, & Kosasih, AL (2025). CONTEMPORARY HUMAN RESOURCE MANAGEMENT CONTEMPORARY ISSUES AND HR STRATEGIES. CV Rey Media Grafika.

Kurniawati, D., Wulandari, S., & Priyono, A. (2020). Evaluation of the implementation of the Hospital Management Information System (SIMRS) using the HOT-FIT method. Manarang Health Journal, 6(1), 50–59.

Laila, L., Sulistyawati, S., & Hidayat, M. (2024). Evaluation of the implementation of the Hospital Management Information System (SIMRS): Literature study. Journal of Preventive Promotion, 7(4), 710–723.

Lestari, I., & Nugroho, H. (2022). Evaluation of the implementation of SIMRS using the HOT-FIT approach in regional hospitals. Indonesian Journal of Health Information Systems, 7(2), 112–123.

Listyorini, PI (2021). SIMRS security system in hospitals: Identification of threats and security recommendations. National Seminar on Health Information Systems, 3(1), 45–53.

Listyorini, PI, & Sintya, I. (2021). SIMRS security system in hospitals. Proceedings of the National Health Information Seminar (SIKENAS). Duta Bangsa University.

Ningsih, AS (2023). Analysis of patient data privacy in the implementation of SIMRS in private hospitals. Indonesian Journal of Medical Records and Health Information, 4(2), 112–120.

Pratama, R., & Setiawan, A. (2022). Analysis of SIMRS data security at RSUD using firewall and IDS/IPS. Journal of Health Information Technology and Systems, 7(1), 45–53.

Putri, DA, & Saputra, H. (2024). Security audit of ISO 27001-based health information systems in hospitals. Indonesian Journal of Health Information Systems, 6(2), 77–89.

Rachmawati, N., Sulistyo, H., & Lestari, F. (2021). Evaluation of electronic medical records in teaching hospitals: A data security perspective. Andalas Public Health Journal, 15(2), 124–133.

Sihole, PO, Lesmana, AE, & Wasir, R. (2024). Strategy and evaluation of health information systems in Indonesia: A literature review. Tambusai Health Journal, 5(2), 512–523.

Wardani, AP, Andriani, D., & Salsabila, N. (2024). Security of electronic medical record information system at Sukapura Islamic Hospital, Jakarta. RAMMIK: Journal of Medical Records and Health Information Management, 3(2).

Wibowo, H. (2020). Implementation of ISO 27001 in hospital management information systems. Journal of Health Information Technology, 5(1), 44–53.

Wilar, YA (2023). Security analysis of hospital information management systems. MAHESA: Malahayati Health Student Journal, 3(2), 132–141.

Yaner, A., Tanuwijaya, H., & Sutomo, Y. (2022). Information security audit of SIM-RS based on ISO 27002 standard at RSU Haji Surabaya. Journal of Accounting Information Systems and Computerization (JSIKA), 1(1), 25–33.

Yuniarti, S., & Hidayat, T. (2022). Implementation of web-based SIMRS in a regional hospital: A case study of efficiency and safety. Scientific Journal of Health, 14(1), 55–63.