E-ISSN: 3025-2326
DINASTI HEALTH AND PHARMACY SCIENCE
https://dinastirev.org/DHPS dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/dhps.v3i1

Evaluation of Data Security and Patient Confidentiality in the Electronic Medical Record System at Santosa Hospital Bandung Central

Ogi Permana[1], Yayang Ayu Nuraeni[2]
[1]Politeknik Piksi Ganesha, Bandung, Indonesia, gigsgiw@gmail.com
[2]Politeknik Piksi Ganesha, Bandung, Indonesia, ayuyayang66@gmail.com

Corresponding Author: gigsgiw@gmail.com[1]

Abstract: This study evaluates the information security level of the Electronic Medical Record (EMR) system at Santosa Hospital Bandung Central using a gap analysis based on the ISO/IEC 27001 standard. The study addresses the growing need for robust patient data protection in the digital healthcare era, particularly in the face of increasing risks of data breaches and cyberattacks. A mixed-method case study design was employed, incorporating in-depth interviews, direct observations, and quantitative assessment using the ISO 27001 checklist. The findings show that several security aspects—such as confidentiality, integrity, and availability—are adequately implemented, although weaknesses remain in access control, multi-factor authentication, and documentation of information security policies. Overall, the hospital's compliance level with ISO 27001 falls into the "adequate" category, indicating a need for stronger policies, enhanced security technologies, and regular security audits. The study is expected to support the hospital in strengthening its information governance and improving patient data protection.

Keyword: Information Security, Electronic Medical Records, ISO/IEC 27001, Data Confidentiality, Gap Analysis

INTRODUCTION

Digital transformation in healthcare services has encouraged hospitals to adopt Electronic Medical Records (EMR) as the primary system for storing and managing patient data. This system offers efficiency, accuracy, and ease of access, but it also introduces increasingly complex information security risks. The main challenges include protecting confidentiality, integrity, and availability—known as the CIA Triad—which forms the foundation of modern information security. Several studies indicate that health data breaches have increased in line with the growing digitalization of healthcare services. Keshta & Odeh (2021) emphasize that EMR systems are vulnerable to threats such as unauthorized access, malware, and insider threats. In addition, the reliability of EMR security infrastructure is influenced by organizational readiness in implementing international security standards, particularly ISO/IEC 27001, which serves as a global reference for information security management.

Indonesia has issued regulations through the Ministry of Health Regulation (Permenkes) No. 24 of 2022 on Medical Records, which mandates hospitals to ensure the confidentiality, integrity, accuracy, and security of patient data. However, practical implementation varies and requires structured evaluation. As managers of highly sensitive data, hospitals carry legal, ethical, and technical responsibilities to ensure that all processes related to the storage, processing, and distribution of health information are conducted with adequate security safeguards. Therefore, this study is essential to assess information security readiness based on ISO/IEC 27001 standards while identifying gaps between current conditions and the expected standards. ISO/IEC 27001 is an international standard for Information Security Management Systems (ISMS) designed to protect information from threats through structured risk management. This standard emphasizes the three core principles of information security: confidentiality, integrity, and availability. In this study, the evaluation is carried out based on ten key ISO/IEC 27001 domains relevant to EMR, namely: (1) Confidentiality, ensuring data is accessible only to authorized parties; (2) Integrity, maintaining data accuracy through audit trails and prevention of unauthorized modifications; (3) Availability, ensuring data is continuously accessible to authorized users; (4) Authentication, verifying user identities; (5) Authorization, restricting access based on roles (RBAC); (6) Non-repudiation, tracing user activities; (7) Privacy, protecting patient personal information; (8) Operational Security, controlling operational activities such as patching and monitoring; (9) Infrastructure Security, securing networks and servers; and (10) Incident Management, systematically handling security incidents.

These ten domains serve as an analytical framework to assess the level of compliance with information security implementation in the EMR system at Santosa Hospital Bandung Central. Based on the background described, this study is designed to address several key issues related to information security in the Electronic Medical Record system at Santosa Hospital Bandung Central. The problem statements of this research include: first, the extent to which the implementation of information security in the Electronic Medical Record system complies with the international ISO/IEC 27001 standard. Second, which aspects of information security have been implemented effectively and which require further reinforcement to ensure the confidentiality, integrity, and availability of patient data. Third, this study aims to formulate strategic recommendations to strengthen patient data protection while ensuring the hospital's compliance with both national and international information security standards. The objectives of this research are to assess the level of conformity of information security implementation in the Electronic Medical Record system at Santosa Hospital Bandung Central to ISO/IEC 27001, to identify strengths and weaknesses within the applied information security aspects, and to provide recommendations that support improvements in patient data security and compliance with relevant regulations. Thus, this study is expected to serve as a reference for hospitals to strengthen their information security systems, prevent data breaches, and enhance patient trust in the digital services provided.

METHOD

This study employs a mixed-methods approach with a case study design. The qualitative component includes in-depth interviews with one key informant, document analysis, and observation of EMR access workflows. The quantitative component is used to assess the level of compliance with information security controls based on a Gap Analysis of ISO/IEC 27001. The research was conducted at Santosa Hospital Bandung Central in September 2025. The object of the study is the information security aspects of the Electronic Medical Record (EMR) system. The research subjects were selected using a non-probability purposive sampling technique, focusing on informants directly involved in the management and use of the EMR system. In this study, there was one informant, namely the Head of the Medical Record Installation. The informant was selected based on the consideration that the Head of the Medical

Record Installation has comprehensive knowledge of the policies, procedures, and implementation of information security within the hospital's EMR system.

This study received ethical clearance from the Health Research Ethics Committee (KEPK) of Politeknik Piksi Ganesha Bandung and permission from the management of Santosa Hospital Bandung Central. The ethical principles applied in this study include informed consent, anonymity, and confidentiality of both the informant's data and patient data.

The data collection instruments used in this study were:

1. **Gap Analysis: Status of ISO 27001 Implementation – Checklist**, used to assess the level of compliance with information security standards.

2. **Interview guidelines**, consisting of open-ended questions to explore policies, procedures, and challenges in the implementation of EMR security at Santosa Hospital Bandung Central.

Research procedures included:

1. Direct observation of the EMR system implementation in the medical record unit.
2. In-depth interviews with the key informant to obtain qualitative insights.
3. Assessment of the ISO 27001 checklist to determine the percentage of compliance with information security aspects.

Scoring was conducted through the following steps:

1. Identifying controls within ISO/IEC 27001 domains relevant to the EMR system (such as access control, encryption, audit logs, backup, and incident management).
2. Observing the implementation of each control through policy documents, SOPs, system configurations, and interview findings.
3. Assigning a score from 0–3 based on the level of implementation:
   a) 0 = Not implemented
   b) 1 = Partially implemented
   c) 2 = Implemented but not consistently
   d) 3 = Fully implemented and compliant with standards
4. Validating the results through triangulation of interviews, observations, and internal documents.
5. Using the final scores to identify security gaps in each domain.

RESULTS AND DISCUSSION

Research Findings

1. New User Access Provision

Observations show that access provisioning for new users is carried out through a formal request from the Head of Unit, followed by verification by the EMR Team or the IT Department. Access rights are assigned based on the user's position and job responsibilities. However, multi-factor authentication (MFA) has not yet been implemented.

2. Access Rights Monitoring

Periodic monitoring of access rights is conducted to ensure that only active employees can use EMR accounts. Nevertheless, the hospital has not yet implemented routine external security audits.

3. Reporting and Handling Mechanisms for Access Misuse

The hospital has established an incident reporting procedure through violation forms, email, or direct reporting. The report components include reporter identity, time, and type of violation; however, documentation of follow-up actions remains limited.

4. System Protection and Backup

The EMR system uses TLS 1.2/1.3 encryption for data in transit and AES-256 for data at rest. Audit logs are available, and backups are performed automatically every day, both on local servers and at an off-site location. The Disaster Recovery Plan (DRP) includes clear RTO and RPO parameters.

5. Integration with SATUSEHAT

Integration is carried out using HL7 FHIR API with OAuth 2.0 and JWT authorization. Data submission begins in the sandbox environment before moving to production, following interoperability best practices.

6. Access Rights Distribution (PPA EMR)

Based on observations, access rights in the EMR system are divided according to healthcare professional roles:

a) **Doctors:** full access to patient medical records, pharmacy orders, and laboratory results.
b) **Nurses:** access to input patient progress notes, nursing interventions, and vital sign monitoring.
c) **Pharmacists:** access to the pharmacy module, including prescriptions, drug inventory, and patient medication history.
d) **Nutritionists:** access to patient diet management according to physician recommendations.
e) **Therapists:** limited access to physiotherapy/rehabilitation treatment notes.
f) **Access** rights follow the *least privilege* principle. However, periodic re-evaluation of access rights has not been routinely conducted.

Table 1. ISO/IEC 27001 Gap Analysis

No	ISO 27001 Domain	Control Assessed	Score (0–3)	Notes
1	Confidentiality	User access, encryption	2	Good implementation, but MFA not applied
2	Integrity	Audit trail, data validation	2	Audit logs available; monitoring not optimal
3	Availability	Backup, DRP	3	Backup and DRP well implemented
4	Authentication	Password policy, MFA	1	MFA not implemented
5	Authorization	RBAC, access rights	2	Role-based access applied; review not routine
6	Non-repudiation	Activity logs	2	Logs available; verification limited
7	Privacy	Privacy policy	2	Policy exists; implementation needs strengthening
8	Operational Security	Patching, antivirus	2	No real-time monitoring
9	Infrastructure Security	Firewall, network protection	3	Strong infrastructure
10	Incident Management	Incident reporting	1	Documentation incomplete

Table 2. Recapitulation

Description	Value
Maximum Score	30
Total Score	18
Percentage	60%
Category	Fair / Needs Improvement

Research Discussion

1. New User Access Provision

The findings indicate that the account provisioning mechanism aligns with the principles of Role-Based Access Control (RBAC) as recommended by NIST (2023). Verification by the Head of Unit and the EMR Team ensures that access rights correspond to job responsibilities. WHO (2022) emphasizes the importance of formal verification workflows to prevent unauthorized access—an aspect already implemented, although the system still lacks Multi-Factor Authentication (MFA). According to HIMSS (2023), MFA is a minimum security control in healthcare information systems; thus, the absence of MFA represents a significant security gap.

2. Access Rights Monitoring

Periodic access reviews are already conducted and meet the ISO/IEC 27001:2022 requirements on Periodic Access Review. However, the absence of routine external security audits means that independent evaluation of the security controls has not yet reached an optimal level. HITRUST (2022) highlights the importance of external audits as part of comprehensive security compliance verification.

3. Reporting and Handling of Access Misuse

Incident reporting procedures are in place and adhere to the basic principles of ISO/IEC 27035:2023 regarding incident response. The reports already include the minimum required elements as suggested by the SANS Institute (2023). However, documentation and follow-up actions require strengthening to ensure that incidents are addressed comprehensively and systematically.

4. System Protection and Backup

The use of TLS 1.2/1.3 and AES-256 encryption complies with WHO and NIST (2023) standards. The implementation of audit logs is consistent with ISO/IEC 27001:2022, and the availability of daily backups and a Disaster Recovery Plan (DRP) with clear RTO and RPO parameters supports the availability aspect. HC3 (2023) stresses that recovery strategies are mandatory for healthcare facilities to prevent data loss and ensure service continuity.

5. Integration with SATUSEHAT

The implementation of HL7 FHIR APIs and OAuth 2.0/JWT-based authorization demonstrates compliance with both national and international interoperability standards. The use of a sandbox environment before production also follows best practices in software development to ensure security and minimize integration risks.

6. Access Rights Distribution for Healthcare Providers (PPA EMR)

The distribution of access rights based on healthcare professional roles reflects the application of the least privilege principle. HIMSS (2023) points out that differentiated access based on job roles is essential to reduce the risk of insider threats. However, the absence of routine access rights re-evaluation creates the potential for excessive or irrelevant privileges if user roles change.

7. Operational Definitions

Table 3. Operational Definitions

Variable	Operational Definition	Indicators	Scale
User Access Security	Mechanisms for granting, managing, and restricting EMR user access	RBAC, account verification, MFA	Nominal
Access Rights Monitoring	Periodic evaluation process for employee access rights	Periodic review, account deactivation	Nominal
Incident Management	Procedures for reporting and handling access misuse	Incident form, documentation, follow-up actions	Nominal
System Security	Technical protection of EMR against threats	Encryption, audit logs, patching, DRP	Nominal
System Integration	Implementation of interoperability with SATUSEHAT	FHIR API, OAuth 2.0, sandbox	Nominal
Healthcare Provider Access Rights (PPA)	Access restriction based on healthcare professions	Least privilege, role alignment	Nominal

Research Limitations

1. The study was conducted in a single hospital, which limits the generalizability of the findings.
2. Not all internal documents could be accessed due to institutional security policies.
3. Compliance assessment was based solely on observation and interviews without system penetration testing.
4. No external audit was available, thus preventing objective benchmarking.
5. The limited research timeframe did not allow full evaluation of patch updates or long-term log monitoring.

CONCLUSION

Based on the findings of the study, it can be concluded that the mechanism for granting access rights to the Electronic Medical Record (EMR) system at Santosa Hospital Bandung Central has been implemented in accordance with the principles of Role-Based Access Control (RBAC), although Multi-Factor Authentication (MFA) has not yet been adopted. Access monitoring is in place, but it is not supported by regular external security audits. Incident reporting procedures are available; however, documentation and follow-up actions need to be strengthened to ensure a more structured incident response. On the other hand, system protection measures—including encryption, audit logs, and backup processes—already meet relevant standards, and the integration with SATUSEHAT utilizes secure protocols aligned with interoperability requirements. The distribution of access rights based on professional roles is appropriate, although the periodic reevaluation of these permissions has not been conducted consistently.

Based on these findings, several recommendations can be proposed, both technically and administratively. From a technical standpoint, it is recommended that MFA be implemented for all EMR accounts to prevent credential theft; real-time network security monitoring and automated patch management should be enabled; an automatic deactivation mechanism for inactive accounts should be added; and Disaster Recovery Plan (DRP) simulations and backup recovery testing should be conducted regularly, for example every six months. From a policy perspective, it is advised that external security audits be conducted at least once per year; more detailed Standard Operating Procedures (SOPs) for incident reporting— including escalation pathways and response timeframes—be developed; annual information security training be mandated for all healthcare personnel; access rights evaluations be conducted every three to six months with formal documentation; and data privacy policies be strengthened in accordance with ISO/IEC 27001 standards and Ministry of Health regulations. The implementation of these recommendations is expected to enhance the security and confidentiality of patient data while simultaneously strengthening the hospital's compliance with national and international standards..

REFERENCES

Aprilia, C. S., & Rahmasari, G. (2022). Application users' experiences on the Santosa features of Bandung patients during the Covid-19 pandemic. Kanal: Jurnal Ilmu Komunikasi, 10(2), 39–44. https://doi.org/10.21070/kanal.v10i1.1580

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. Journal of Management Information Systems, 19(4), 9–30.

Hasanah, U., & Rachmawati, I. (2023). Analisis keamanan data rekam medis elektronik dengan pendekatan ISO/IEC 27001 pada rumah sakit X di Jawa Barat. Jurnal Rekam Medik dan Informasi Kesehatan, 15(2), 101–112.

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. ISO.

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis.

Lee, C., Jung, H., & Kim, Y. (2023). Cybersecurity challenges and strategies for electronic health records under GDPR. Health Information Science and Systems, 11(1), 23–34. https://doi.org/10.1007/s13755-023-00206-1

Nugraha, D., Sari, R., & Wibowo, A. (2024). Digital health apps and patient satisfaction: A case study in Indonesian hospitals. Jurnal Administrasi Kesehatan, 12(1), 15–25.

Putri, A., & Santoso, H. (2023). The impact of mobile health applications on patient satisfaction in outpatient services. Indonesian Journal of Health Information, 5(2), 88–96.

Rani, D. M., & Widyaningrum, B. N. (2025). Evaluasi keamanan informasi sistem rekam medis elektronik: Studi kasus rumah sakit di Jawa Tengah. Jurnal Manajemen Informasi Kesehatan Indonesia, 10(1), 45–56.

Santosa, I. V., Pratama, R., & Lestari, N. (2024). Analisis implementasi sistem informasi manajemen rumah sakit berbasis digital. Jurnal Inspirasi Mengabdi Untuk Negeri, 3(1), 77–85.

Sari, P., & Nugroho, W. (2023). Perlindungan hukum terhadap kerahasiaan data pasien dalam penerapan rekam medis elektronik di Indonesia. Jurnal Hukum dan Kesehatan, 9(1), 55–68.

Setiawan, A., & Marlina, R. (2022). Strategi penerapan keamanan informasi pada rekam medis elektronik berbasis cloud di rumah sakit daerah. Jurnal Teknologi Informasi Kesehatan, 8(2), 88–96.

Triplett, W. (2024). Exploring and mitigating cybersecurity challenges in electronic health records. Cybersecurity and Innovative Technology Journal, 2(1), 12–27. https://doi.org/10.5555/citj.2024.012

Ventola, C. L. (2014). Mobile devices and apps for health care professionals: Uses and benefits. P & T, 39(5), 356–364.

World Health Organization. (2021). Global strategy on digital health 2020–2025. https://apps.who.int/iris/handle/10665/344249

Wulandari, R., Sari, P., & Nugraha, D. (2022). Digital health application and its impact on patient queue reduction. Jurnal Kesehatan Masyarakat, 18(3), 220–229. https://doi.org/10.15294/kemas.v18i3.34567