

An Overview of the Implementation of Data Security Principles in Electronic Medical Records at Kota Tengah Community Health Center

Ismail S. Ahmad¹, Riska Ahmad², Moh Ichsan Arifin Antu³

^{1,2,3}Prodi D-III Rekam Medis Dan Informasi Kesehatan, Stikes Bakti Nusantara Gorontalo,

*Corresponding author: ia7097333@gmail.com

Article Info

Article history:

Received 26 May, 2026

Revised 08 July, 2026

Accepted 25 July, 2026

Keywords:

Electronic Medical Records;
Data Security;
Confidentiality; Integrity;
Availability; Authentication;
Access Control

ABSTRACT

Electronic Medical Records (EMR) are an important component of the digital transformation of healthcare services because they support efficiency, accuracy, and access to patient information. However, the use of EMR must be accompanied by appropriate data security measures to protect sensitive health information. This study aimed to describe the implementation of data security principles in EMR at Kota Tengah Community Health Center based on confidentiality, integrity, availability, authentication, and access control. A qualitative descriptive approach was used. Data were collected through interviews, observation, and documentation involving five informants selected by purposive sampling: the head of the community health center, the person responsible for medical records, an IT officer, a physician, and a nurse. Data were analyzed using the Miles, Huberman, and Saldaña interactive model through data condensation, data display, and conclusion drawing and verification. The findings indicate that the five data security aspects had generally been implemented adequately. Confidentiality was supported by individual accounts and restricted access; integrity was supported by data checking and correction procedures; availability was supported by daily system use and data backup; authentication was implemented through individual usernames and passwords; and access control was arranged according to users' duties and responsibilities. Nevertheless, several weaknesses remained, including insecure password storage practices, suboptimal use of audit trails, occasional internet network disruptions, and the need for periodic review of user access rights. Continuous improvement in password management, audit trail utilization, access review, and network infrastructure is therefore required.

INTRODUCTION

Community health centers (Puskesmas) are first-level healthcare facilities that provide comprehensive and continuous services to communities. Patient care activities must be documented through medical records, which function not only as communication and information tools but also as sources for service evaluation, legal evidence, and clinical decision-making. The development of information technology has transformed conventional medical records into Electronic Medical Records (EMR), enabling faster access to patient information and more efficient management of health data.

In Indonesia, EMR implementation has expanded following the issuance of Minister of Health Regulation No. 24 of 2022 on Medical Records. EMR can improve access to information, service efficiency, and data integration, but increased digitalization also creates greater requirements for information security. Health information is sensitive personal information, making confidentiality, integrity, availability, authentication, and access control essential components of secure EMR management.

The context of Kota Gorontalo also reflects this digital transformation. Previous work cited in the original study reported that EMR implementation can improve administrative efficiency and patient services. However, preliminary observations at Kota Tengah Community Health Center identified several security concerns. These

included access rights that required better alignment with users' duties, simple username-and-password authentication, intermittent internet disruptions, the need for stronger backup arrangements, and audit trails that had not yet been optimally utilized. The facility also had limited IT human resources, with one IT officer responsible for information-system management and network maintenance.

These conditions demonstrate the importance of evaluating how data security principles are applied in daily EMR operations. Therefore, this study aimed to describe the implementation of confidentiality, integrity, availability, authentication, and access control in EMR at Kota Tengah Community Health Center.

METHODS

This study used a qualitative descriptive design. The research was conducted at Kota Tengah Community Health Center, Kota Gorontalo, in 2026. Five informants were selected purposively based on their involvement in EMR use and management. They consisted of the head of the community health center, the person responsible for medical records, an IT officer, a physician, and a nurse.

Data were collected through semi-structured interviews, direct observation, and documentation. The data focused on five security principles: confidentiality, integrity, availability, authentication, and access control. Data processing included editing, transcription, reduction, presentation, and verification. Analysis followed the interactive model of Miles, Huberman, and Saldaña, consisting of data condensation, data display, and conclusion drawing and verification. Triangulation of interviews, observations, and documentation was used to strengthen the credibility of the findings.

RESULTS

Table 1 Characteristics of Informants

No.	Category	Initials	Age	Position
1	Key informant	Y.M.U	49	Head of Community Health Center
2	Main informant	S.S	46	Person Responsible for Medical Records
3	Main informant	N.M	34	P-Care / IT Officer
4	Supporting informant	M.B	32	Physician
5	Supporting informant	Y.U	44	Nurse

Confidentiality

The confidentiality aspect was generally implemented adequately. Patient information in the EMR was intended for healthcare-service purposes and access was restricted to personnel with appropriate authority. Users operated individual accounts and were expected not to share their credentials. The informants reported that no patient-data misuse or data leakage had been identified during EMR use. Observation also indicated that access restrictions and individual accounts were part of routine practice. However, the study identified an important weakness: some staff members stored or wrote down passwords in the work area, which could create an avoidable security risk.

Integrity

The integrity aspect was also implemented adequately. Staff checked patient information before saving it and corrected errors when they were identified. These practices supported the accuracy and completeness of patient information. The study nevertheless found that the audit trail was not yet optimally utilized to document and monitor changes and user activities. Strengthening procedures for data correction, verification, and monitoring of changes was therefore identified as an area for improvement.

Availability

The EMR system was used daily to support healthcare services, including registration, examination, and documentation of patient care. A data-backup mechanism was available to support data availability when technical problems occurred. Nevertheless, internet-network stability remained a constraint and could interrupt access to the system during service delivery. Continued maintenance of network infrastructure and backup arrangements was therefore considered necessary.

Authentication

Authentication was implemented through individual usernames and passwords. Each user was expected to log in using a personal account and was prohibited from lending the account to another staff member. Account management was coordinated by the IT officer and adjusted according to the user's position and duties. Observation found no shared-account use or unauthorized access during the study period. However, the practice of writing or

storing passwords in work areas indicated that user awareness and password-management practices still needed improvement.

Access Control

Access control was implemented by assigning permissions according to users' positions, duties, and responsibilities. Users could access only the menus and patient information required for their work, while changes in staff assignments or new users were coordinated with the IT officer. This mechanism reduced the possibility of unauthorized access. The main operational challenges were forgotten passwords and the need to adjust permissions when duties changed. The study emphasized that access rights should be reviewed periodically so that permissions remain consistent with current organizational roles.

DISCUSSION

The findings show that the five assessed data security principles had been incorporated into the daily operation of EMR at Kota Tengah Community Health Center. This is consistent with the role of EMR as a digital system that requires not only efficient information management but also safeguards for sensitive patient information. The original study relates these practices to the information-security framework and to ISO/IEC 27001:2022, particularly the need to protect information through organizational policies, procedures, and technical controls.

For confidentiality, individual accounts and restricted access provide a basic layer of protection for patient information. However, secure credential management is equally important. Writing passwords in accessible work areas can weaken otherwise appropriate access restrictions. Routine information-security education and access audits can reinforce staff compliance.

For integrity, verification and correction of patient information help maintain data quality. The absence of optimal audit-trail utilization, however, limits the ability to trace changes systematically. Strengthening audit-trail monitoring and establishing clear procedures for data correction can improve accountability and facilitate investigation when discrepancies occur.

Availability depends not only on the EMR application itself but also on supporting infrastructure. The availability of backup procedures is positive, while unstable internet connectivity remains an operational vulnerability. Network maintenance, contingency procedures, and periodic testing of backup and recovery processes are therefore important for continuity of patient services.

Authentication through individual usernames and passwords establishes user accountability, but credential security remains dependent on user behavior. The findings indicate that the system-level mechanism is present, while password-management practices require improvement. Training and periodic reminders can help users understand that credentials are personal security controls.

Access control based on job roles is an important safeguard because users do not need unrestricted access to all patient information. The study found that permissions were generally aligned with duties, but organizational changes require continuous adjustment. Periodic access reviews should therefore be formalized so that permissions are promptly modified or revoked when employees change positions or no longer require access.

LIMITATIONS

This study was conducted at only one community health center and involved five informants; therefore, the findings describe the conditions at the study site and should not be generalized to all community health centers. The qualitative design also means that findings depend partly on information obtained through interviews, observations, and documentation, despite the use of triangulation. In addition, the study focused specifically on five security aspects and did not comprehensively assess other information-security domains such as security-risk management, incident response, or detailed technical infrastructure assessment.

CONCLUSION

The implementation of data security principles in Electronic Medical Records at Kota Tengah Community Health Center has generally been carried out adequately across confidentiality, integrity, availability, authentication, and access control. Patient information is protected through individual accounts and restricted access; data integrity is supported through verification and correction; availability is supported through routine system use and backup; authentication is implemented through personal usernames and passwords; and access control is aligned with users' duties. Nevertheless, improvements are still needed in password management, audit-trail utilization, periodic review of user access rights, and network infrastructure. These improvements are important to strengthen patient-data protection and maintain continuity and accountability in EMR-based healthcare services.

RECOMMENDATIONS

Kota Tengah Community Health Center should strengthen password-management policies, conduct regular information-security training, optimize audit-trail functions, and establish scheduled access-right reviews. Network infrastructure and backup procedures should also be monitored and tested regularly. Future studies may involve multiple healthcare facilities and additional informants, and may examine other dimensions such as security-risk management, incident response, user awareness, and technical controls.

BIBLIOGRAPHY

- Adryan, et al. (2025). Efisiensi Administrasi Kesehatan Sebagai Dampak Penggunaan Rekam Medis Elektronik di Puskesmas Kota Tengah Kota Gorontalo. *Jurnal Kolaboratif Sains*, 8(6). <https://doi.org/10.56338/jks.v8i6.7886>
- Anjayati, S. (2021). Review artikel: Analisis kualitas pelayanan terhadap kepuasan pasien di puskesmas menggunakan metode Servqual. *Nursing Care and Health Technology Journal (NCHAT)*, 1(1), 31–38. <https://doi.org/10.56742/nchat.v1i1.7>
- Arnaya, A. A., & Nirvana, I. W. (2021). Tingkat kepuasan dan harapan pasien rawat jalan terhadap kualitas pelayanan kesehatan di Puskesmas Mengwi I. *E-Jurnal Medika Udayana*, 10(9), 82. <https://doi.org/10.24843/MU.2021.V10.i9.P14>
- Furkan, M. A., Maruji, M., & Islah, A. M. (2021). Sistem informasi pelayanan kesehatan pada Puskesmas Kabaena Selatan berbasis WEB. *Simtek: Jurnal Sistem Informasi dan Teknik Komputer*, 6(1), 77–82. <https://doi.org/10.51876/simtek.v6i1.98>
- Gurning, F. P., Al Wafi Lubis, M. Z., Hasibuan, N. R., & Adeliyani, M. (2021). Manajemen sumber daya manusia pada penempatan tugas dan fungsi kerja di UPT Puskesmas Sering. *Jurnal Kesehatan Masyarakat (Undip)*, 9(5), 706–710. <https://doi.org/10.14710/jkm.v9i5.30764>
- Hasibuan, I. D., Silfani, D., Andreansyah, R., Harahap, R. S., & Auzi, S. (2024). Analisis penerapan SPM (Standar Pelayanan Minimal) bidang kesehatan pada Puskesmas Medan Tuntungan tahun 2021–2023, 5(2). <https://doi.org/10.31004/jkt.v5i2.28180>
- Hia, E., Purba, I. E., & Dachi, R. A. (2024). Penerapan manajemen puskesmas sebagai upaya peningkatan kinerja Unit Pelaksana Teknis Dinas Kesehatan Kabupaten Nias Barat tahun 2023. *Jurnal Kesehatan Masyarakat dan Lingkungan Hidup*, 9(2), 64–79. <https://doi.org/10.51544/jkmlh.v9i2.5544>
- Lisnawati, S., Karmanto, B., Mohammad, M. I., & Khasanah, L. (2025). Analisis implementasi E-Puskesmas rekam medis elektronik yang terintegrasi dengan aplikasi SATUSEHAT di Puskesmas Kesunean Kota Cirebon. *Jurnal Kesehatan, Sains, dan Teknologi (Jakasakti)*, 4(1), 145–156. <https://doi.org/10.36002/js.v4i1.381975>
- Meilani, A., & Tandy, D. Y. (2026). Analisis komprehensif implementasi, kesiapan, dan aspek yuridis rekam medis elektronik di fasilitas pelayanan kesehatan Indonesia pasca Permenkes Nomor 24 Tahun 2022. *PubHealth Jurnal Kesehatan Masyarakat*, 4(4), 434–441. <https://doi.org/10.56211/pubhealth.v4i4.1630>
- Puspita, K. M., Wijaya, A., & Darmawan, R. (2024). Analisis kesiapan rekam medis elektronik di Puskesmas Tempunak Kabupaten Sintang tahun 2024, 8(1). <https://doi.org/10.32585/jmiak.v8i1.6260>
- Rahardjo, D. P., & Nabila, A. (2025). Gambaran penerapan rekam medis elektronik di Klinik Pratama Polres Pelabuhan Tanjung Priok tahun 2024. *Jurnal Ilmiah Kedokteran dan Kesehatan*, 5(1), 488–502. <https://doi.org/10.55606/klinik.v5i1.5705>
- Ratnawati, & Iskandar, D. (2025). Constraints in the implementation of electronic medical records at Puskesmas in accordance with Permenkes 24 of 2022. *Saintika Medika*, 21(1), 27–45. <https://doi.org/10.22219/sm.Vol21.SMUMM1.40368>
- Riyani, Y., & Raharjo, B. B. (2021). Analisis penerapan fungsi manajemen pada sistem pengelolaan rekam medis pasien di Puskesmas Rembang 1 Kabupaten Rembang, 1(3). <https://doi.org/10.15294/ijphn.v1i3.46262>
- Saragi, I., Ulva, F., & Azkha, N. (2026). Hubungan dimensi mutu pelayanan kesehatan dengan kepuasan pasien di Puskesmas Mapaddegat Kabupaten Kepulauan Mentawai tahun 2024, 4(2). <https://doi.org/10.59435/gjik.v4i2.1989>
- Sugiyono. (2024). *Metode penelitian kuantitatif, kualitatif, dan R&D (Edisi terbaru)*. Alfabeta.
- Sunusi, S., Nasrudin, & Samsualam. (2025). Fungsi manajemen akreditasi Puskesmas Wolowa Kabupaten Buton, 6(2). <https://doi.org/10.52103/jahr.v6i2.2020>
- Telaumbanua, K. M. K., Syahrul'an, & Susilawati, E. (2026). Peran fungsi administrasi dalam kelancaran alur pelayanan pasien di Puskesmas Hibala. *Jurnal Kesehatan, Gizi, dan Psikologi (JKGP)*, 1(1), 13–18.
- Timbawa, R., Rompas, W., & Plangiten, N. (2021). Pelayanan kesehatan di Puskesmas Gemeh Kecamatan Gemeh Kabupaten Kepulauan Talaud. *Jurnal Administrasi Publik*, 7(112). <https://ejournal.unsrat.ac.id/v3/index.php/JAP/article/view/36331>
- Wardani, E., Happy Putra, D., Sonia, D., & Yulia, N. (2024). Keamanan sistem informasi rekam medis elektronik di Rumah Sakit Islam Jakarta Sukapura. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, 3(2), 31–38. <https://doi.org/10.47134/rmik.v3i2.1756>
- Zahroh. (2024). Tinjauan keamanan dan kerahasiaan data elektronik guna kesiapan penerapan rekam medis elektronik.