IJPHS:
International Journal of Psychology and Health Science
GREENATION PUBLISHER
+62 812 1046 7572 http://greenpub.org greenation.info@gmail.com
DOI: https://doi.org/10.38035/ijphs.v3i4

Analysis of Information Security Aspects of Patient Data in Electronic Medical Records at Kebonjati Hospital

Nadya Muthiara Putri[1], Sali Setiatin[2]
[1]Politeknik Piksi Ganesha, Bandung, Indonesia, nadyamuthiara@gmail.com
[2]Politeknik Piksi Ganesha, Bandung, Indonesia, salisetiatin@gmail.com

Corresponding Author: nadyamuthiara@gmail.com[1]

Abstract: The development of information technology in the healthcare sector has driven the implementation of Electronic Medical Records (EMR) systems, which play a crucial role in the efficient and effective management of patient data. However, information security in these systems remains a major challenge, given the high sensitivity of patient data and the need to maintain confidentiality. This study aims to analyze the information security aspects of patient data in the Hospital Management Information System at Kebonjati Hospital. A descriptive qualitative approach was used, with data collected through semi-structured interviews with three hospital registration officers. The results indicate that SIMRS already implements user authentication and access control, but significant weaknesses exist, such as the lack of an auto-logout feature, a weak audit trail mechanism, and data validation and integrity issues. Furthermore, IT infrastructure constraints and a lack of staff training also impact patient data security. Based on these findings, it is recommended that the hospital update its system, enhance information security training, and adopt security policies based on international standards such as ISO 27001. Implementing these measures is expected to strengthen patient data security and improve the quality of healthcare services at Kebonjati Hospital.

Keyword: Information Security, Electronic Medical Records, Hospital Management Information System

INTRODUCTION

The development of information technology has had a significant impact on various aspects of life, including the healthcare service sector. One of the most substantial transformations is the implementation of the Electronic Medical Record (EMR) system, which replaces manual paper-based medical records with a more integrated and easily accessible digital system (Saputra, 2025). The Electronic Medical Record is an information technology tool used to collect, store, process, and access patient medical data stored in a data-based management system, serving as both a clinical decision support system and an integrated medical documentation platform (Rosalinda, Setiatin, & Susanto, 2021). EMR not

only functions as an aid for recording clinical data but also plays a crucial role in supporting quick and accurate medical decision-making, improving healthcare workers' efficiency, and simplifying documentation and reporting processes for management and third parties such as BPJS Kesehatan.

The implementation of EMR provides many benefits, especially in terms of fast information access and reduced risk of errors caused by illegible handwriting. However, along with these benefits come new challenges, particularly in the aspect of information security (Ikawati & Ilmawati, 2025). Patient data is sensitive information that must be protected from unauthorized access, unauthorized modification (integrity), and must remain available to authorized personnel when needed. These three aspects — confidentiality, integrity, and availability — form the core pillars of information security management that must be strictly maintained within healthcare information systems.

In Indonesia, attention to patient data security in medical record systems has become more emphasized with the issuance of the Regulation of the Minister of Health of the Republic of Indonesia No. 24 of 2022 concerning Medical Records. The regulation states that every healthcare facility must maintain medical records that are complete, accurate, and confidential. In addition, healthcare facilities are responsible for ensuring the security of electronic systems used for storing and managing patient data. This regulation serves as an essential guideline in the implementation and evaluation of EMR systems, particularly concerning information security aspects, including access rights, user authentication, data backup management, and security incident reporting systems.

However, in many hospitals—especially those of medium and small scale—the implementation of EMR systems is often not fully supported by adequate technological infrastructure. Many hospitals still face limitations in terms of computer networks, server capacity, and human resources trained in health information technology. As a result, systems that should improve the quality of healthcare services instead create new problems, such as service delays due to system downtime, data input errors, and potential data breaches caused by weak access control and the absence of user activity log systems (Kapitan, Farich, & Perdana, 2023).

Moreover, low user awareness of the importance of maintaining data security is a major factor in security breaches. For example, shared accounts, leaving computers unlocked when not in use, and failing to change passwords regularly are still common practices. These practices can create entry points for unauthorized parties to illegally access patient data. Violations of patient privacy can lead to legal consequences and damage public trust in healthcare services (Hendra & Halbadika Fahlevi, 2024).

Previous studies have stated that the success of EMR implementation largely depends on the alignment between technology, people, and existing policies. In the context of information security, hospitals must not only provide technically secure systems but also ensure that all staff understand security policies, receive regular training, and uphold moral responsibility in maintaining patient data confidentiality. Even the most sophisticated systems will be ineffective if users do not operate them with the required discipline and adherence to security procedures.

Kebonjati Hospital, as one of the healthcare facilities that has implemented the Hospital Management Information System (SIMRS) for patient data management, faces similar challenges. Although the SIMRS used has provided convenience in patient registration, procedure documentation, and data reporting, several issues related to information security have been identified. Some registration officers have reported the absence of security features such as auto-logout, weak control over data modifications, and frequent system errors causing patient data mix-ups. This indicates the need for a comprehensive evaluation of the system

used, particularly regarding the confidentiality and integrity of patient data (Hamson et al., 2021).

This study aims to analyze the extent to which the SIMRS system at Kebonjati Hospital supports the information security aspects of patient data. The main focus is to assess the implementation of security features such as user authentication, activity logs, data validation, and procedures for data deletion or modification. Additionally, this research seeks to identify key challenges faced by field staff in maintaining data security, both from technical and non-technical perspectives, and to develop recommendations for future improvements.

By comprehensively understanding the situation in the field, the results of this study are expected to serve as a reference for hospital management in developing better information security policies. Furthermore, this research can contribute to the development of a secure, reliable, and patient rights–oriented health information system. Since patient data is a vital asset that must be protected, the integration of technology systems, management policies, and user awareness is the key to creating a secure and trustworthy hospital information system.

METHOD

This study employs a qualitative descriptive approach, aiming to obtain an in-depth understanding of information security aspects in the use of Electronic Medical Records (EMR) at Kebonjati Hospital. This approach was chosen because it allows the researcher to directly understand the phenomena occurring in the field from the informants' perspectives, particularly in the context of the implementation of the Hospital Management Information System (SIMRS) and how the system ensures the security of patient data. The main focus of this research is to explore the staff's understanding of data security policies, technical features within SIMRS, and the practices applied in managing and protecting patient data.

Data collection was carried out through semi-structured interviews with three informants who work as registration officers at Kebonjati Hospital. The first informant is an admission staff member with approximately 1.5 years of experience. The second informant is an outpatient registration officer who has been working since 2021. The third informant is also an outpatient registration officer who began working in March 2025. These three informants were selected purposively because they possess direct and relevant knowledge of the system being analyzed, particularly regarding the processes of data input, editing, and deletion within SIMRS.

The interviews were conducted in person using a set of open-ended guiding questions prepared in advance. This method enabled informants to provide free and detailed responses based on their experiences and understanding. The topics explored included the use of user accounts (username and password), system security mechanisms such as auto-logout, validation and modification processes of patient data, as well as the challenges faced in maintaining confidentiality and data integrity. The interview results were then analyzed using a thematic analysis method to identify patterns, key findings, and recommendations for improving the information security system at Kebonjati Hospital.

RESULT AND DISCUSSION

1. Authentication and Data Access

Authentication is the initial step in securing digital data, especially within the Electronic Medical Record (EMR) system that stores sensitive patient information. The results of interviews with three informants at Kebonjati Hospital revealed that each staff member has their own username and password used to access the Hospital Management Information System (SIMRS) (Rohman & Prasetyo, 2023). This represents a form of individual access control aligned with the principles of information security, ensuring that every transaction is recorded and traceable based on user identity.

The second informant, an outpatient registration officer, stated:

"Yes, that's right, because every registered patient must have a record of which staff registered them."

This reinforces that the system already implements user accountability, allowing activity tracking based on individual accounts. Furthermore, the same informant added:

"Each patient registration must be clear about who registered them, and this can be seen from the username."

This statement shows that staff members are aware of the importance of user identity within the system.

However, in terms of user session security, a significant weakness was found — the absence of an auto-logout feature. Auto-logout is a feature that automatically logs users out of the system after a period of inactivity, preventing unauthorized use when a user leaves the computer without logging out. The lack of this feature creates a security gap because accounts may remain active and be accessed by others without permission.

The first informant expressed this concern directly:

"The current SIMRS doesn't have an automatic logout feature, so the account can still be opened on another computer."

This statement also indicates that accounts can be accessed from multiple computers without session limits, which poses a risk of multi-session access that is difficult to monitor. If not properly controlled, this can result in data entry errors, data conflicts, and potential privacy violations, as user activities are not strictly monitored.

From an effectiveness standpoint, some informants mentioned that while auto-logout could technically enhance security, it might also hinder work efficiency if not adjusted to field conditions. As Ramadhanti explained:

"There's no auto-logout feature, and even if there were, it wouldn't be effective because when we're registering a patient, if it suddenly logs out automatically, the data won't be saved."

This indicates that the design of a security system must also consider usability. A system that is too strict without considering the workflow of the staff can reduce productivity and lead to complaints. Therefore, a compromise solution is needed — such as setting a longer idle time before auto-logout or providing a warning before the system logs out automatically.

In conclusion, user authentication at Kebonjati Hospital is functioning, but weaknesses remain in session management. The absence of an auto-logout system and the potential for multi-login access pose serious threats to patient data security. Therefore, system updates or internal policy adjustments are needed — including user education on the importance of manual logout and IT team supervision to detect unusual account activity.

2. Data Input and Editing Mechanism

In a Hospital Management Information System (SIMRS), the process of inputting and editing patient data is a highly critical component. This process not only concerns the completeness and accuracy of administrative data but also serves as the foundation for medical service validation and insurance claims (Marwati, 2021). Therefore, the system must ensure that all entered data is correct, accurate, and not mistakenly interchanged between patients. At Kebonjati Hospital, data input is carried out by registration officers who fill in patients' identity information in an integrated manner, both for new and returning patients. This process includes entering full names, national identification numbers (NIK), BPJS numbers (if applicable), birth dates, addresses, phone numbers, and selecting the clinic and guarantor.

However, based on interviews with registration officers, complaints were identified regarding system errors where data from a previous patient was automatically retrieved into the new patient form. The first informant stated:

"Sometimes there's an error, for example, the input data from the previous patient gets pulled into the new patient's record in SIMRS."

This phenomenon indicates a failure in the system's buffer or caching management, as well as weaknesses in session data separation within the SIMRS application used. From an information security perspective, this issue represents a threat to data integrity. If a new patient's record contains information belonging to another patient, it may result in incorrect diagnoses, inappropriate medical actions, or inaccurate insurance claims. Furthermore, such incidents could also constitute a breach of confidentiality, as a previous patient's personal data could become visible to staff handling a different patient.

Although the system already includes input validation features—such as checking the format of NIK, BPJS number, and phone number length—these are not sufficient to ensure information security if the data editing process remains open without adequate control. According to the second informant, editing can be performed by staff when errors are found in certain data elements, such as date of birth or phone number. Gita explained:

"If there's data that needs to be changed, like a phone number or an incorrect date of birth, we search by the patient's medical record number, edit the element we want to change, then save it, and the system displays a message saying 'patient data successfully saved.'"

While this process appears simple and efficient, it also highlights the absence of a strong audit trail or data change log. In an ideal system, every modification to patient data should be recorded in detail—indicating who made the change, when it was made, what was changed, and the reason for the change. This audit trail is essential for security, transparency, and accountability, especially if future errors affect medical actions or financial claims. Without such a feature, hospitals may face difficulty tracing incidents or data manipulation, whether intentional or accidental.

Additionally, another staff member (the second informant) mentioned that merging duplicate patient data with double medical record numbers (double RM) is also part of the editing process handled by registration officers. If this merging process is not performed correctly or without confirmation from authorized departments such as the medical records or IT unit, the potential for identity errors increases significantly.

This situation demonstrates that, although Kebonjati Hospital's data input system generally follows initial validation procedures, it lacks sufficient security in the editing process and internal control mechanisms. Ensuring data security requires not only accuracy at the point of entry but also consistency, integrity, and protection throughout the entire data lifecycle.

To address these issues, it is recommended that SIMRS administrators evaluate data validation and integrity features and develop a transparent audit trail system. Furthermore, editing access rights should be restricted to specific, authorized, and trained users, and data modification reports should be documented through an internal reporting mechanism. By doing so, the data input and editing processes can operate not only efficiently but also securely-minimizing errors and preventing potential information security breaches.

3. Access Authority and Data Modification

The management of patient data in an electronic medical record (EMR) system involves not only data entry but also strict regulation of access rights related to data modification and deletion (Suwani et al., 2024). Based on interview findings, registration officers at Kebonjati Hospital have the authority to directly edit certain data, particularly for administrative corrections such as updating a patient's phone number or address. However,

the deletion of more complex transactional data, such as registration records that may affect other datasets, requires stricter procedures.

The first informant explained:

"Deletion of data, such as registration transactions for a particular reason, can be done directly by the registration staff as long as it does not affect other data, and it must be reported through the data deletion link. Meanwhile, changes to transactions related to billing, supporting units, etc., must be submitted to the IT department by creating an official report (Berita Acara/BA) signed by the staff and unit head, which will then be forwarded to IT."

This procedure reflects a layered authorization and documentation process for risky data deletion actions, which is a positive step toward maintaining the integrity and accountability of patient data. The creation of an official report (Berita Acara) also facilitates audits and data tracking when needed.

However, the access control system has not yet fully implemented the principle of least privilege, which dictates that users should be granted only the minimum level of access necessary to perform their duties. In some cases, registration staff are still able to modify important data without multi-level authorization or automatic system supervision. This creates potential risks of human error or misuse of access that could compromise the security and accuracy of patient information.

Ideally, modifications to critical data—especially those impacting financial aspects, insurance claims, or medical information—should go through a tiered authorization process with strong documentation, restricted only to users with higher-level access, such as senior medical record officers or authorized IT personnel. Moreover, the system should include an automated audit trail to record every change, ensuring no room for undetected data manipulation.

4. System and Infrastructure Availability

The availability of the Hospital Management Information System (SIMRS) is a vital factor in supporting the smooth delivery of healthcare services, especially during peak hours when patient flow is high. All three informants confirmed that, in general, the SIMRS can still be accessed properly during hospital operating hours, allowing registration and data management processes to run relatively smoothly (S. Yuliana & Hartono, 2024).

However, all informants also acknowledged that system disruptions (downtime) frequently occur, rendering the application temporarily inaccessible. The first informant stated:

"Sometimes the SIMRS cannot be accessed, which hinders the service process."

Such disruptions not only delay the registration and input of patient data but also cause patient backlogs and increase the administrative workload. From the perspective of information security, availability is one of the core pillars that must be maintained to ensure the system functions optimally when needed.

These disruptions may stem from several factors, including technological infrastructure limitations, inadequate server capacity, or the absence of effective system backups. Furthermore, outdated systems or suboptimal IT management can also contribute to these issues.

To enhance system availability, the hospital should conduct a comprehensive evaluation of its IT infrastructure—this includes improving network capacity, utilizing reliable servers, and implementing well-tested disaster recovery and backup mechanisms. In addition, training and coordination between IT staff and system users are essential to ensure that any disruption can be addressed quickly and effectively.

5. Security Challenges

Information security within the electronic medical record (EMR) system at RS Kebonjati faces several key challenges that may hinder the effectiveness of patient data protection. Based on interviews with registration officers, these challenges encompass both technical and non-technical aspects that are interrelated (Budiman, Isa, & Soekiswati, 2025).

First, the lack of adequate information technology (IT) infrastructure poses a significant challenge. Reliable IT infrastructure is the foundation for ensuring the availability, integrity, and confidentiality of data within a hospital information system. Insufficient infrastructure—such as limited server capacity, unstable network connections, and outdated hardware—can cause system downtime, slow access, and potential data breaches due to weak physical and digital safeguards.

Second, human error contributes greatly to data security risks. Registration staff who have not received sufficient training often make data entry mistakes, inaccuracies during data editing, or fail to protect account credentials—for instance, by forgetting to log out of the system. The second informant clearly emphasized this issue:

"The lack of adequate technological infrastructure and weak staff awareness and training lead to human errors."

Third, from a system standpoint, the absence of automatic protection features such as auto-logout and audit trails represents a tangible technical deficiency. Auto-logout helps prevent unauthorized access when users leave devices unattended, while an audit trail provides a transparent record of all data modifications, ensuring accountability. The lack of these features creates vulnerabilities for potential account misuse and undetected data manipulation. As noted by the second informant:

"The biggest challenge in maintaining patient data security is not just about technology."

This statement reinforces that human and organizational factors are just as crucial as technological ones. Information security is not solely a technological responsibility—it requires a strong culture of security, regular training, and clear policies and procedures for all staff members.

To address these challenges, a comprehensive approach is necessary, including upgrading IT infrastructure, developing systems with complete yet user-friendly security features, and conducting continuous training and awareness programs for staff on the importance of protecting patient data. Furthermore, strict implementation of Standard Operating Procedures (SOPs) and enhanced internal monitoring mechanisms are essential to minimize human error and strengthen security awareness across the organization.

CONCLUSION

Based on interviews with registration officers and an analysis of information security aspects within the Hospital Management Information System (SIMRS) at Kebonjati Hospital, it can be concluded that the system has generally implemented several fundamental principles of information security—particularly in terms of user authentication through the use of individual usernames and passwords. This is an important step to ensure that all patient data recording activities can be traced to the responsible staff member.

However, this study also reveals several fundamental weaknesses that potentially threaten patient data security and require serious attention from hospital management.

First, the absence of an auto-logout feature in the system presents a significant security vulnerability, as user accounts may remain active even when devices are left unattended. This creates opportunities for unauthorized access, which could result in data breaches or unauthorized data manipulation.

Second, the audit and data change tracking mechanism (audit trail) within the system is still very limited or even unavailable. Without a proper audit trail, it becomes difficult to monitor and investigate any modifications made to patient medical records. This limitation reduces accountability and transparency in data management and makes it challenging to detect security violations.

Third, data validation and integrity remain issues that need improvement. Instances of incorrect data entry—such as previous patient information being automatically pulled into a new patient form—indicate that the system's reliability is not yet optimal. Such weaknesses can lead to duplicate records, patient misidentification, and inaccurate health service and insurance claim data.

Fourth, technical constraints, including suboptimal IT infrastructure and system downtime, hinder the availability and smooth access to SIMRS. In addition, non-technical factors, such as insufficient staff training and lack of awareness regarding the importance of information security, further increase the risk of human error in patient data management.

Overall, although Kebonjati Hospital has established a reasonably good security foundation, there remains significant room for improvement to ensure comprehensive protection of patient data—aligned with existing regulations, standards, and best practices in healthcare information security.

REFERENCES

Ansori, S., Sari, I., & Sufyana, C. (2022). Sistem Informasi Distribusi Rekam Medis (Studi Kasus: RSAU Lanud Sulaiman). *Jurnal Sains Dan Informatika*, *8*(1), 70-79.

Budiman, Arief, Muzakar Isa, and Siti Soekiswati. 2025. "Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta." Ranah Research : Journal of Multidiscipcclinary Research and Development 7(3): 2118–27. doi:10.38035/rrj.v7i3.1421.

Hamson, Zulkarnain, Gandika Supartha, Muhamad Hasan Wahyudi, and Muntasir Muntasir. 2021. Researchgate Informasi Teknologi Di Bidang Kesehatan.

Hendra, Hendra, and Arry Halbadika Fahlevi. 2024. "Implementation of Good Corporate Governance (GCG) Principles in PDAM Tirta Ogan, Ogan Ilir District." Iapa Proceedings Conference: 187. doi:10.30589/proceedings.2024.1052.

Ikawati, Fita Rusdian, and Sindi Adita Ilmawati. 2025. "Tinjauan Implementasi Rekam Medis Elektronik Rawat Jalan Di Puskesmas Jabung Kabupaten Malang." Prepotif : Jurnal Kesehatan Masyarakat 9(1): 1946–57. doi:10.31004/prepotif.v9i1.41218.

Kapitan, Rifki, Achmad Farich, and Agung Aji Perdana. 2023. "Analisis Kesiapan Penerapan Rekam Medis Elektronik RSUD Bandar Negara Husada Provinsi Lampung Tahun 2023." Jurnal Kebijakan Kesehatan Indonesia 12(4): 205. doi:10.22146/jkki.89841.

Marwati. 2021. Analisis Sistem Informasi Registrasi Pasien Dengan Metode PIECES Di Rumah Sakit Umum Daerah Syekh Yusuf Kabupaten Gowa.

Rohman, Hendra, and Rizki Adi Prasetyo. 2023. "PERANCANGAN SISTEM INFORMASI MANAJEMEN KLINIK BERBASIS WEB DI KLINIK MITRA HUSADA NGLIPAR." : 167–86.

Rosalinda, Revi, Sali Setiatin, and Aris Susanto. 2021. "EVALUASI PENERAPAN REKAM MEDIS ELEKTRONIK RAWAT JALAN DI RUMAH SAKIT UMUM X BANDUNG TAHUN 2021" Cerdika: Jurnal Ilmiah Indonesia 1(8): 1045–56.

S Yuliana, and Budi Hartono. 2024. "Penerapan Sistem Informasi Manajemen Rumah Sakit Dalam Menunjang Peningkatan Pelayanan Di Rumah Sakit." Jurnal Kesehatan Masyarakat 17(2): 64–69.

Saputra, Wahyu. 2025. "Jurnal Ilmu Kesehatan Masyarakat Dampak Digitalisasi Manajemen Rumah Sakit Terhadap Efisiensi Pelayanan : Literature Review." Jurnal Ilmu Kesehatan Masyarakat 14(3): 245–54.

Santika, F., Gumanti, N. A., Herfiyanti, L., & Sufyana, C. M. (2021). Outpatient Medical E-Resume in Support INA-CBGs Claims for Covid-19 Patients at Hospital. *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, *21*(1), 87-98.

Suwani, Suwani, Teguh Prasetyo, Diah Arimbi, and Ahmad Jaeni. 2024. "Kerahasiaan Medis Dan Data Pasien Dalam Catatan Rekam Medis Elektronik Sesuai Dengan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022." Jurnal Cahaya Mandalika ISSN 2721-4796 (online): 2626–34. doi:10.36312/jcm.v3i3.3658.