IMPACT OF ELECTRONIC MEDICAL RECORDS PRIVACY PROTECTION ON STARKES MRMIK ELEMENT II

Diansyah[1], Ramdhan Gunawan[2], Lucky Nurul Iqbal [3]
Medical Records and Health Information, Health Faculty, Politeknik Piksi Ganesha [1]
diansyahrm1@gmail.com; ramdhangunawan29@gmail.com; Iqballucky26@gmail.com;

Abstract: *This study aims to analyze the impact of electronic medical records (EMR) confidentiality protection on Hospital Accreditation Standards - Medical Records and Health Information Management (STARKES MRMIK) Element II in hospitals. The protection of EMR confidentiality is crucial as it contains patients' medical history, in line with the established accreditation standards. This research employs a descriptive quantitative approach, with data collected through questionnaires, literature reviews, observations, and interviews, and analyzed statistically. Studies have shown that ESDM heating systems significantly affect MRMIK Level II STARKES. At the 10% level of significance, the computed T-value of 15.182 is higher than the T-table value of 1.812. The impact size is 95.8%, while the effect sizes of other factors are just 4.2%.*

Keywords: Protection of electronic medical records, STARKES MRMIK Element II, hospital accreditation, health data security.

Introduction

Electronic Medical Records (EMR) are digital systems used to record, store, and manage patient health data electronically, replacing traditional paper-based medical records. With the advancement of technology in the healthcare sector, EMR have become an essential part of efforts to improve the efficiency, accuracy, and quality of healthcare services. This system enables authorized healthcare professionals to quickly access real-time medical information, thereby supporting better care coordination and more effective clinical decision-making. According to the World Health Organization (2022), EMR not only accelerate information access but also play a role in enhancing the overall quality of healthcare services. Given the sensitive nature of patients' medical records, maintaining their privacy is an important consideration in this setting. Therefore, the security and privacy of data in RME should always be maintained so that only authorized parties can access it, in line with applicable regulations. (Belrado et al., 2024; Faida & Ali, 2021; Indra et al., 2024).

Protection of RME confidentiality has significant implications for various elements of hospital management, including compliance with hospital accreditation standards (Belrado et al., 2024; Faida & Ali, 2021; Indra et al., 2024). One of the relevant standards is STARKES MRMIK Element II, which emphasizes the importance of medical data protection as well as processes to maintain confidentiality, security, privacy, and integrity of information. The implementation of technologies such as encryption, access control, and security audits are recommended measures in maintaining this confidentiality. In addition, training of medical staff is also important to ensure that patient data is managed properly and securely. (Asgiani et al., 2022; Indra et al., 2024; Setyadi & Nadjib, 2023).

Although many studies have addressed the importance of medical data security and confidentiality in RME, there are still gaps related to the impact of RME confidentiality protection on hospital compliance with accreditation standards, specifically STARKES MRMIK Element II. This study aims to explore the direct influence of RME confidentiality protection on the fulfillment of this element in the hospital accreditation process. By understanding the influence of confidentiality protection on accreditation standards, this study is expected to provide new insights for health institutions in improving the quality of medical information management and ensuring compliance with applicable regulations.

Literature Review

According to Sinsky et al. (2023), Electronic Medical Records are described as a digital-based system that records patient medical information and serves as a tool for managing health data. EMRs have the capability to share information among various healthcare institutions and play an important role in supporting clinical decision-making processes and facilitating care coordination among healthcare providers.

According to the World Health Organization (2022), Electronic Medical Records are considered a vital component of the health information system, serving to document an individual's medical history, treatments, and healthcare services received digitally. These records replace paper-based systems and enable faster, safer, and more integrated access, aimed at improving the efficiency and quality of healthcare services.

According to Menachemi and Collum (2023), maintaining the confidentiality of electronic medical records is an effort to protect patient health information through the implementation of strict policies and technologies. This endeavor is crucial for preventing data breaches and building trust between patients and healthcare providers.

According to Ismail and Nugroho (2023), Starkes MRMIK consists of various methods and practices designed to effectively manage health information. This includes processes for the collection, storage, processing, and distribution of medical data, aimed at improving the quality of healthcare services while ensuring the security of patient information.

According to Harahap (2023), Starkes MRMIK encompasses the management of electronic medical records and health information by applying principles of security, confidentiality, and traceability. This approach is crucial for meeting regulatory standards and maintaining patient trust.

[1]diansyahrm1@gmail.com
[2]ramdhangunawan29@gmail.com
[3]Iqballucky26@gmail.com

Methodology

This study approach uses a quantitative methodology that is descriptive in nature. The questionnaire is the main data collection tool in this survey research (Sugiyono, 2022). According to Ningsih et al. (2021), the impact of securing electronic medical records is the independent variable in this study, with STARKES MRMIK ELEMENT II as the dependent variable. Using a questionnaire with 12 statements, 12 PMIK officers were selected to represent the population in this study. The research hypothesis formulates two possibilities: H0 (null

hypothesis) which states that the protection of confidentiality of electronic medical records does not affect the STARKES MRMIK ELEMENT II in one of the hospitals in Bandung city, and H1 (alternative hypothesis) which states that the protection of confidentiality of electronic medical records affects the STARKES MRMIK ELEMENT II in the hospital. (Yam & Taufik, 2021). Data collection techniques include questionnaires, literature studies, observations, and interviews. The collected data were analyzed using *IBM SPSS* Statistics software. (Robinson Sihombing, 2022).. Data analysis includes validity tests to ensure the validity of the data with a minimum correlation coefficient of 0.3. There are various tests that can be used in statistics, such as reliability, simple linear tests to determine how X and Y are related, and hypothesis testing to see if the independent variable has a significant influence on the dependent variable, with an acceptance criterion of $\alpha = 0.1$. Furthermore, to find out the extent to which electronic medical record security has an impact on STARKES MRMIK ELEMENT II, the coefficient of determination test was also conducted.

Results & Discussion

The validity test results in Table 1 show that the rcount value of each statement item on the *Corrected Item-Total Correlation* is positive. This indicates that each statement item has a good correlation with the total score. To determine validity, the rcount value is compared with the rtable, where at a confidence level of 90% and a significance level of $\alpha = 0.1$ with the number of respondents (N = 12), the degree of freedom (df) is 10. Based on the rtable for df = 10, the value obtained is 0.4971. All statements in the instrument can be considered valid because all rcount values are greater than rtable. In other words, you can trust this instrument to assess the relationship between X and Y because each statement item is significantly related to the overall score. As a result, researchers can confidently use this tool.

Table 1. Validation test results

rcount	rtabel	Data Validity
0.722	0,4971	Valid
0.737	0,4971	Valid
0.749	0,4971	Valid
0.751	0,4971	Valid
0.743	0,4971	Valid
0.762	0,4971	Valid
0.767	0,4971	Valid
0.722	0,4971	Valid
0.758	0,4971	Valid
0.812	0,4971	Valid
0.758	0,4971	Valid
0.741	0,4971	Valid

The results of the reliability test with *Cronbach's Alpha Based on Standardized Items* in Table 2 show a value of 0.775. With a total of 12 statements, this value indicates that the instrument has a good level of reliability. The rtable value of 0.4971 is used as a reference limit, and the reliability of the research instrument is indicated by the fact that rcount is higher than rtable. Therefore, it is safe to proceed with further analysis of all statement items in the instrument as they are all consistent in assessing the target variable.

Table 2. Reliability test results

Case Processing Summary		
	N	***%***
Valid Case	***12***	***100.0***
Excluded[a]	***0***	***.0***
Total	***12***	***100.0***

Reliability Statistics	
Cronbach's Alpha	***N Of Items***
.755	***12***

The results of the simple linear regression test in Table 3 show that the coefficient value for the variable security and confidentiality of Medical Records is 0.775. To determine whether this result is significant or not, the researcher conducted a hypothesis t test. In this test, the tcount value is compared with the ttable.

Table 3. Simple linear regression test results

ANOVA[a]					
Model	Sum Of Squares	Df	Mean Square	F	Sig.
1. Regression	145.680	1	145.680	230.492	.000[b]
Residuals	6.320	10	.632		
Total	152.000	11			

a. Dependent Varible : STARKS MRMIK
b. Predictors: (Constant), Security

Coefficients[a]					
Model	**Unstandart Coefficients**		**Standardized Coefficients**	**T**	**Sig**
	B	**Std.Eror**	**Beta**		
1. (Constant)	**2.425**	**1.570**		**1.545**	**.153**
Security	**.940**	**.062**	**.979**	**15.182**	**.000**

a. Dependent Varible : STARKES MRMIK

With a significance level of α = 0.1 (10%) and the number of respondents N = 12, the degree of freedom (df) is calculated as N - 2, so df = 10. The ttable value for df = 10 at the 0.1 significance level is 1.812. The tcount value of 15.182 is higher than the ttable of 1.812, in accordance with the test findings. We accept the alternative hypothesis (HI) and reject the null hypothesis (Ho) because tcount is greater than ttable. This means that the findings indicate a substantial relationship between the electronic medical record confidentiality protection variable and STARKES MRMIK Element II in one of the hospitals in Bandung.

Table 4. Coefficient of determination test results

Model	R	R.Square	Adjusted R Square	Std. Eror of The Estimate
1	.979	.958	.954	.795

In a simple linear regression test conducted by researchers using SPSS, the Coefficient of Determination (R^2) is used to measure how much influence the variable of confidentiality protection of Electronic Medical Records has on the MRMIK Element II STARKES. The analysis results show that R^2 is 95.8%. This shows that 95.8% of the variation in STARKES MRMIK Element II can be explained by the Electronic Medical Record confidentiality protection variable. The remaining 4.2% is influenced by other variables or is part of the *error* (e). In other words, the regression model used is very effective in explaining the effect of the confidentiality protection variable on STARKES MRMIK Element II, while the rest includes factors not explained by the model or measurement error.

Security and Confidentiality Issues of Electronic Medical Records

In the context of protecting the security and confidentiality of Electronic Medical Records, there are several significant issues that need to be addressed. First, the login system for PMIK (Morbis) officers is not equipped with two-step verification, resulting in potential access by unauthorized parties. This problem is compounded by the fact that some officers who are not part of PMIK can still access the Electronic Medical Record system (Morbis), reducing control over sensitive data.

In addition, the inadequate temperature of the server room causes computers to overheat frequently and shut down suddenly. This contributed to hardware damage and operational disruptions. Lack of regular maintenance also resulted in frequent system errors, which compromised data accessibility and reliability.

Reliance on IT vendors to handle server problems also increased the time required for repairs due to the absence of IT vendors in the hospital. Furthermore, serious problems arise when there is a version update of the Morbis system, which often causes loss of patient data, such as medical record numbers and old medical record contents that cannot be accessed again. This resulted in old patients having to get a new medical record number, so the previous data was lost.

Finally, the lack of CCTV security monitoring the server computers and file storage rooms also adds to the security risk. Without adequate visual surveillance, the chances of unauthorized access or data theft are higher. All of these issues point to an urgent need to improve the security and data protection of Electronic Medical Record systems in hospitals.

Troubleshooting the Security and Confidentiality of Electronic Medical Records

To address various issues related to the security and confidentiality of Electronic Medical Records, several solutions have been taken. First, PMIK has proposed to the vendor to implement two-step verification on the data access system, so that only authorized PMIK officers can open the system, reducing the risk of access by unauthorized parties. In addition, PMIK officers are encouraged to maintain strict confidentiality of system PINs and passwords, to prevent other parties from gaining access that could pose a security risk.

Furthermore, PMIK has asked the hospital to provide server room cooling facilities to keep the room temperature stable. This aims to prevent the server computers from overheating which can cause damage or sudden system shutdown. In addition, a request has been made for the vendor to perform regular system maintenance, including data backups, to ensure that existing data remains safe and available in case of problems.

PMIK has also requested that IT personnel from the vendor be at the hospital, so that if there are problems or errors in the system, the problem can be resolved immediately without requiring a long time. To avoid data loss during system version updates, the head of medical records has socialized to PMIK the importance of filling in manual medical record files as data backup.

Finally, a proposal has been made to add a CC TV facility that leads to a storage room or server, with the aim of preventing data theft and loss of important information. These measures are expected to strengthen the security and confidentiality of the Electronic Medical Record system, and support compliance with the STARKES MRMIK Element II standard.

Conclusions

On March 1 to April 30, 2024, the author conducted research at one of the hospitals in Bandung and found that there were still some deficiencies in the security and confidentiality of the hospital's Electronic Medical Record (RME). The security and confidentiality aspects of RME have not been fully met, especially in relation to the system managed by the vendor (Morbis). The RME system has not been well optimized, as seen from the infrequent maintenance performed, which could potentially lead to data loss after version updates. In addition, the system is not equipped with two-step verification at login, allowing unauthorized access by parties other than PMIK officers. Limited IT manpower from the vendor is also an issue, as the absence of adequate technical support can hinder the system's performance and address obstacles quickly. This conclusion shows that improvement efforts are needed in the aspects of system maintenance, access security, and technical support to ensure that the security and confidentiality of medical data in the hospital can be well guaranteed.

References

Asgiani, P., Suryawati, C., & Agushybana, F. (2022). A literature review: Security Aspects in the Implementation of Electronic Medical Records in Hospitals. *HEALTH SCIENCE MEDIA*, *10*(2 SE-). https://doi.org/10.30989/mik.v10i2.561

Asih, H., & Indrayadi, I. (2023). The Development of Electronic Medical Records in Indonesia: Literature Review. *Journal of Preventive Promotions*, *6*(1 SE-Articles). https://doi.org/10.47650/jpp.v6i1.736

Belrado, R., Harmendo, H., & Wahab, S. (2024). Analysis of the Use of Electronic Medical Records in Hospitals. *Journal of Professional Nurse Research*, *6*(4 SE-Articles). https://doi.org/10.37287/jppp.v6i4.3039

Faida, E. W., & Ali, A. (2021). Readiness Analysis of Electronic Medical Record Implementation with the DOQ-IT (Doctorâ€™s Office Quality-Information Technology) Approach. *Indonesian Journal of Health Information Management*, *9*(1 SE-), 67. https://doi.org/10.33560/jmiki.v9i1.315

Indra, I., Dewi, T. N., & Wibowo, D. B. (2024). Protection of Patient Data Confidentiality vs.

Obligation to Open Access to Electronic Medical Records. *Soepra Journal of Health Law*, *10*(1), 97-117.

Ningsih, W., Kamaludin, M., & Alfian, R. (2021). The Relationship between Learning Media and Increased Student Learning Motivation in PAI Subjects at SMP Iptek Sengkol South Tangerang. *Tarbawai: Journal of Islamic Religious Education*, *6*(01), 77-92.

Robinson Sihombing, P. (2022). *SPSS application for beginners*.

Setyadi, D., & Nadjib, M. (2023). The Effect of Electronic Medical Records on Service Quality and Patient Satisfaction: A Literature Review. *Journal Research of Social Science, Economics, and Management*, *2*(12 SE-Articles), 2780-2791. https://doi.org/10.59141/jrssem.v2i12.500

Sugiyono. (2022). The Influence of Lifestyle, Peers and Pocket Money on Student Consumption Patterns. *Journal of Research Methodology*, 1-20.

Yam, J. H., & Taufik, R. (2021). Quantitative Research Hypothesis. *Perspective: Journal of Administrative Sciences*, *3*(2), 96-102. https://doi.org/10.33592/perspektif.v3i2.1540