JURNAL KESEHATAN
JURNAL ILMU-ILMU KEPERAWATAN, KEBIDANAN, FARMASI & ANALIS KESEHATAN
DOI : https://doi.org/10.52221/jurkes
JURKES
ISSN : 2089-3906

Level Of Staff Compliance with Procedures Information Security in Management Electronic Medical Records (ELMR) at Annisa Hospital, Bogor

Ferawati[1], Winda Dwi Lestari[2], Rahma Sari Fadilah[3]
[1-3]Bachelor of Hospital Administration Study Program, Annisa Health and Business Institute, Bogor

Article Information

Revised: October 2024
Available online: October 2024

Keywords

Compliance level; information security; electronic medical records; EMR; risk management

Correspondence

Email: verawatiikbis@gmail.com

ABSTRACT

Staff compliance is a crucial factor in maintaining the confidentiality, integrity, and availability of patient data, in line with the Minister of Health Regulation No. 269/2008 and the ITE Law No. 11/2008. EMR also increases the risk of sensitive patient data leakage if not managed with strict security procedures. Annisa Hospital Bogor, as an institution that has implemented EMR, is obliged to ensure the confidentiality, integrity, and availability of data. This study aims to measure and analyze the level of compliance of medical and non-medical staff at Annisa Hospital Bogor with information security procedures in managing Electronic Medical Records (EMDR). The method used is descriptive quantitative by distributing questionnaires to the EMR user staff population. The results showed that the average compliance rate was 81.6%, but vulnerabilities were found in the use of passwords and log-out protocols after accessing the system. The study recommends the need for regular training and systematic audits to improve staff awareness and discipline.

INTRODUCTION

Digital transformation in the healthcare sector, particularly the implementation of Electronic Medical Records (EMR), brings significant efficiency to services. However, EMR also increases the risk of sensitive patient data leaks if not managed with strict security procedures. Annisa Hospital, Bogor, as an institution that has implemented EMR, is required to ensure data confidentiality, integrity, and availability (the CIA triad). Staff compliance with established security procedures is the first line of defense (humanware defense). Low staff compliance can trigger security incidents, resulting in ethical and legal violations, and a decline in public trust. Therefore, this study is crucial to capture the actual level of compliance at Annisa Hospital, Bogor.

The problem formulation in this study is how the level of compliance of medical and non-medical staff at Annisa Hospital Bogor with information security procedures in the management of EMR. The purpose of this study is to determine the level of compliance of Annisa Hospital Bogor staff with EMR information security procedures, and to specifically identify aspects of EMR information security procedures that need to be improved in terms of compliance.

METHOD

This study used a quantitative descriptive design to describe and measure staff compliance levels. The study population comprised all medical (doctors, nurses) and non-medical (administrative, IT support) staff at Annisa Hospital in Bogor who have access to and are actively involved in EMR management. Sampling was conducted using a purposive sampling technique with 80 respondents.

The instrument used is the RME information security compliance questionnaire consisting of 18 questions with a Likert scale (1 (Never to 5 = Always). The questionnaire indicators are Access and identity management, procedures for exiting the system after work is completed, data confidentiality and prohibition on sharing passwords, incident reporting and securing work devices. Data analysis uses descriptive univariate statistics (percentage, mean, and standard deviation) to determine the level of compliance overall and per indicator.

RESULTS AND DISCUSSION

1. Respondent Profile

The total number of respondents in this study was 80 staff with an average working period of 4.5 years, indicating that most of them had sufficient experience with RME.

Table 1. Research Respondent Categories

Variables	Frequency	Percentage (%)
Medical Staff (Doctors and Nurses)	55	68.75
Non-Medical Staff	25	31.25

2. Description of Staff Compliance Data

Table 2. Respondent Compliance Data

Variables	Percentage (%)
Access and Identity Management	80.2%
Log-in and Log-out Activities	75.0%
Sharing Information and Data	87.0%
Incident Reporting	82.0%
Work Equipment Security	84.0%
Average	81.6%

The level of compliance of respondents at Annisa General Hospital with RME information security procedures showed an average of 81.6% with the highest aspect being the aspect of sharing information and data and the lowest compliance aspect being the aspect of log-in and log-out activities.

The lowest compliance was found in the log-in and log-out activity indicators with the following sub-indicator details:

Variables	Percentage (%)
Password Complexity Properties (Combinations)	78.0%
Periodic Password Change	74.0%
Log out after completing the task	71.0%
Lock the screen when leaving the desk	77.0%

The lowest value sub-category specifically was found in the sub-indicator "Logging out after completing a task" at 71.0%.

The average compliance rate of 81.6% indicates that the majority of staff at Annisa Hospital Bogor have good awareness and discipline in implementing RME information security procedures. High compliance with the Information and Data Sharing indicator ($\bar{x}=4.35$) demonstrates the hospital's success in instilling the ethical value of patient data confidentiality (privacy). Staff understand the legal and ethical consequences of medical information leaks, which aligns with the confidentiality principle in Health Information Management (Widodo & Sugiharti, 2020).

The main critical vulnerability point was found in log-in and log-out activities, particularly the sub-indicator of logging out after completing a task. Low compliance in this aspect can be explained by the theory of efficiency and usability. Staff tend to choose the quicker and easier route (not logging out) to avoid the perceived time-consuming re-login process, especially in busy and fast-paced work environments (Supriadi & Kurniawan, 2021).

This vulnerability creates a significant risk known as Unattended Workstation Risk. If a computer is left logged into the EMR system, anyone can access, modify, or print patient data without authorization. Although Annisa Hospital has strict procedures in place,

the failure to implement them in daily staff operations demonstrates a gap between policy and practice (Dwi & Hidayati, 2019).

These results underscore the need to shift the focus of information security risk management from solely technical aspects (hardware and software) to human aspects (humanware). Even with existing policies, management needs to strengthen technical controls: enable time-out or auto-lock features on RME systems after 2-3 minutes of inactivity. Continuous education: training should shift from policy socialization to case simulations and role-playing that emphasize the risks of negligent log-outs. Audits and sanctions: implement an audit log system that can track prolonged login sessions or conduct surprise audits to provide deterrence.

CONCLUSIONS AND RECOMMENDATIONS

Staff at Annisa Hospital Bogor's compliance with information security procedures for managing EMR is high. Staff have excellent awareness of data confidentiality. However, significant vulnerabilities exist in log-in and log-out activities, particularly the habit of not logging out after completing tasks or locking the screen when leaving a workstation. These vulnerabilities have the potential to lead to unauthorized access and data integrity breaches.

Recommendations for Annisa Hospital Bogor include revising and strengthening log-out procedures and implementing clear sanctions for repeat violations. Configuring the EMR system to implement an aggressive Auto-Lock or Time-Out Session feature (maximum 3 minutes). Conducting training and awareness campaigns by conducting behavior-based information security awareness campaigns, focusing on the dangers of unattended workstations.

REFERENCE

Ministry of Health of the Republic of Indonesia. (2008). Regulation of the Minister of Health Number 269/Menkes/Per/III/2008 concerning Medical Records. Jakarta: Ministry of Health of the Republic of Indonesia.

Republic of Indonesia. (2008). Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE).

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

Dwi, SA, & Hidayati, R. (2019). Analysis of User Compliance Levels with Electronic Medical Record Information System Security Standards. Indonesian Health Management Journal, 7(3), 185-192.

Kristanto, A., & Susanto, TH (2022). The Role of Human Error in Data Security Incidents in Digital Healthcare Services: A Systematic Review. Journal of Business Information Systems, 12(2), 75-84.

Supriadi, F., & Kurniawan, F. (2021). Factors Influencing User Compliance with UTAUT-Based RME Information Security Policies. Indonesian Journal of Hospital Administration (ARSI), 5(1), 1-8.

Widodo, A., & Sugiharti, E. (2020). Evaluation of the CIA Triad Implementation in

Electronic Medical Records Management to Ensure Patient Data Confidentiality. National Public Health Journal, 15(4), 180-188.