MEDIA INFORMASI
Center for Research and Community Service
Health Polytechnic of the Ministry of Health Tasikmalaya
https://ejurnal2.poltekkestasikmalaya.ac.id/index.php/bmi

Implementation of SIMRS Authorization System in Supporting the Competency Achievement of Poltekkes Kemenkes Tasikmalaya Students

Ida Wahyuni[1], Dedi Setiadi[1], Diana Barsasella[1], Ulfah Fauziah[1]*

[1]Health Polytechnic of the Ministry of Health Tasikmalaya

***Co-responding author:**
ullfahirpan@gmail.com

Article Info
Submitted 05 09 2025
Revised 31 10 2025
Published 31 10 2025

Keywords:
Implementation, Competency, Clinical Practicum, Authorization System, SIMRS

P-ISSN : 2086-3292
E-ISSN : 2655-9900

National Accreditation:
Sinta 4

Abstract

Background: Digital transformation in healthcare is a strategic priority to achieve the National Medium-Term Development Plan (RPJMN) 2025–2045. Hospital Information Systems (SIMRS) play a key role in improving service quality and supporting the competency development of health professionals. However, challenges such as unrestricted access, weak confidentiality culture, and inadequate authorization mechanisms remain critical issues. **Objective:** This study aimed to examine the implementation of the SIMRS authorization system in supporting clinical practicum competency while ensuring patient data security. **Methods:** A quantitative cross-sectional design was used, involving 79 practicum students and 8 clinical instructors from 8 hospitals affiliated with Poltekkes Kemenkes Tasikmalaya. Data were collected through structured questionnaires assessing four key variables: access policies, role-based access control (RBAC), data security, and audit trails. Data were analyzed descriptively. **Results:** Findings showed that access policies and RBAC effectively supported practicum needs by enabling students to access learning modules without altering patient records. However, weaknesses were found in data security, including shared accounts and the absence of confidentiality agreements. Audit trails were functional but weakened by account sharing. Clinical instructors noted positive aspects such as regular policy updates but identified insufficient individual access control. **Conclusion:** Overall, SIMRS authorization supports clinical competency development. Strengthening data security enforcement, confidentiality agreements, and user accountability is necessary to enhance privacy protection and maintain trust in digital health systems.

INTRODUCTION

The transformation of the health sector outlined in Indonesia's 2025–2045 National Medium-Term Development Plan (RPJMN) requires synergy across six main pillars, particularly in the area of health technology transformation, through the integration of quality healthcare human resources. The quality of healthcare services is inseparable from the availability and qualifications of various types of health professionals, including medical record and health information personnel, who are responsible for managing data and information. Hospitals, as one of the supporting infrastructures for health development in Indonesia, require an integrated information system (Kementerian Kesehatan Republik Indonesia, 2023). The Hospital Management Information System (SIMRS) serves as a strategic tool to support and enhance the effectiveness of healthcare service delivery (Kementerian Kesehatan Republik Indonesia, 2013).

Today, SIMRS has been developed for the management of clinical patient services and has the capability to integrate various service components, including diagnostics, procedures, medical records, pharmacy, billing, and management control (Sianturi et al., 2016). In the context of health education, students need practical experience to develop relevant competencies. However, access to hospital information systems must be carefully managed to ensure patient data security and privacy.

A study by Jethwa et al. (2009) involving health students in the UK found that students had relatively unrestricted access to patient medical records, there was a lack of a confidentiality-preserving culture in the workplace, and students perceived a hierarchy of confidentiality violations—often mimicking the behavior of senior staff.

Digital transformation is central to Indonesia's 2025–2045 National Medium-Term Development Plan (RPJMN). Within the health sector, Hospital Management Information Systems (SIMRS) support clinical decision-making, billing, inventory management and reporting (Kementerian Kesehatan RI, 2013). Integrating students into such systems is critical for developing competent health-information professionals. Yet granting students access to hospital information systems presents ethical and logistical challenges: students require meaningful hands-on experience while patient confidentiality must be safeguarded (Jethwa et al., 2009). Studies in the UK and India have highlighted risks when student access is inadequately controlled—ranging from unrestricted access to sensitive records to lax confidentiality cultures (Purkayastha et al., 2017; Jethwa et al., 2009). In Indonesia, preliminary observations at Poltekkes Kemenkes Tasikmalaya's practicum hospitals revealed inconsistent authorization practices, with students reporting limited access or, conversely, unsupervised use of shared accounts. This raised concerns about data security and educational quality. While previous research has discussed single sign-on systems and RBAC frameworks, there is limited empirical evidence on how SIMRS authorization is implemented in teaching hospitals and how it influences students' perceptions of their practicum learning.

Preliminary studies conducted at three hospital practicum sites affiliated with Poltekkes Kemenkes Tasikmalaya revealed variations in the implementation of authorization systems for practicum students. About 65% of students reported limited access that hindered their learning, while 58% of clinical supervisors expressed concerns about data security if students were granted broader access (Kedokteran BI, Kusumaningtyas, Utarini, & Pinzon, 2017). Previous studies have examined the implementation of Single Sign-On (SSO) systems linking electronic medical records with learning management systems in a major academic institution in India (Purkayastha, Gichoya, & Addepally, 2017), and the behavior of UK medical students regarding patient information confidentiality (Jethwa et al., 2009) using qualitative methods.

This study evaluates SIMRS authorization policies at eight hospitals affiliated with Poltekkes Kemenkes Tasikmalaya. Specifically, we assess the clarity of access policies, the assignment of user roles via RBAC, adherence to data-security practices (e.g., unique credentials, confidentiality agreements) and the use of audit trails. Rather than measuring competency outcomes directly, we explore how students perceive these policies in relation to their practicum experiences. Findings will inform recommendations for balancing educational needs with privacy and security requirements.

METHOD

Study design and setting

A descriptive, cross-sectional survey was conducted in February–March 2025 across eight hospitals serving as clinical practicum sites for students from the Health Polytechnic of the Ministry of Health Tasikmalaya. The hospitals included type B, C and D facilities; most were type D, reflecting typical practicum environments.

Participants

Eligible participants were students enrolled in clinical practicum courses related to medical records and health information, aged 19–23 years, and clinical instructors overseeing practicum activities. Purposive sampling was used due to logistical considerations. In total, 59 students and eight instructors participated (92.3 % response rate). Ethical approval was granted by the institutional review board, and written informed consent was obtained from all respondents.

Instruments and variables

A structured questionnaire, adapted from established information-security frameworks and prior studies, assessed four constructs:

1. Access policy clarity (10 items) – respondents indicated their awareness of hospital policies governing SIMRS access, including whether policies were updated regularly and whether data-access limitations were clearly defined.
2. Role-Based Access Control (12 items) – items measured whether students were assigned specific roles within SIMRS, the extent of their viewing rights and restrictions on editing or deleting data.
3. Data-security practices (8 items) – this construct assessed the use of strong passwords, possession of unique credentials, awareness of confidentiality obligations and frequency of automatic logout features.
4. Audit-trail implementation (3 items) – items evaluated respondents' awareness that SIMRS records user activity, including login/logout times and data accessed.

Each item used a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). Cronbach's alpha values indicated good to excellent reliability ($\alpha = 0.81–0.96$), and validity was confirmed via Pearson correlation coefficients ($r > 0.444$, $p < 0.05$) on a pilot sample of 20 students.

Data collection and analysis

Participants completed the online questionnaire during scheduled practicum periods. Data were analysed using SPSS 25.0 to calculate frequencies, percentages and mean scores for each item and variable. Because the study's aim was descriptive and the sample size limited, inferential tests (e.g., correlations between variables and competency outcomes) were not performed. Future studies should consider such analyses to explore relationships.

RESULTS AND DISCUSSION

The initial stage of this study involved instrument testing, which consisted of four main variables: access policy, implementation of Role-Based Access Control (RBAC), data security, and audit trail. The instrument was administered to 20 students who had completed their clinical practicum with competencies including the use of SIMRS, from two hospitals: RSUD dr. Soekardjo and RSUD Ciamis. Data collection was conducted through an online questionnaire and analyzed using SPSS.

Validity testing showed that all 33 items were valid based on Pearson product-moment correlation analysis at a 95% confidence level. The correlation coefficients (r-count) for each item exceeded the critical value of r-table (0.444), with significance values below 0.05, indicating that each item accurately measured the intended variable.

Reliability testing further confirmed that the instrument was consistent. The Cronbach's Alpha values were 0.937 for the access policy variable (10 items), 0.955 for RBAC implementation (12 items), 0.811 for data security (8 items), and 0.950 for the audit trail (3 items). These results indicate excellent reliability for access policy, RBAC, and audit trail, and good reliability for data security. Since all values exceeded the minimum threshold of 0.7, the research instrument can be considered reliable and suitable for data collection.

The second stage, following the testing of the research instrument, involved measuring the implementation of the SIMRS authorization system based on system acceptance by respondents, consisting of 59 students undergoing clinical practicum, whose competencies include the use of SIMRS from six hospitals, through questionnaire distribution. The following data were obtained:

Table 1. Distribution of Respondents by Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	19-20	15	25.4	25.4	25.4
	21-23	44	74.6	74.6	100.0
	Total	59	100.0	100.0	

Source: Primary Data, 2025

Based on Table 3, the distribution of respondents by age shows that out of 59 respondents, the majority (44 respondents or 74.6%) were aged 21–23 years, while a smaller portion (15 respondents or 25.4%) were aged 19–20 years.

Table 2. Distribution of Respondents by Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	12	20.3	20.3	20.3
	Female	47	79.7	79.7	100.0
	Total	59	100.0	100.0	

Source: Primary Data, 2025

Based on Table 4, the distribution of respondents by gender shows that out of 59 respondents, 79.7% were female and 20.3% were male.

Table 3. Distribution of Respondents by Type of Clinical Practicum Hospital

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Type B	1	12.5	12.5	12.5
	Type C	2	25	25	37.5
	Type D	5	62.5	62.5	100
	Total	8	100.0	100.0	

Source: Primary Data, 2025

Based on the data from clinical practicum sites, 62.5% of the eight hospitals were classified as Type D hospitals, whereas only 12.5% were classified as Type B hospitals.

To assess the implementation of SIMRS authorization for clinical practicum students, data were processed using a quantitative approach with SPSS software for the four research variables. The data are presented in the form of frequency distributions for each variable item.

To determine the application of access policy as part of the authorization process for clinical practicum students, the questionnaire included 10 statement items as follows:

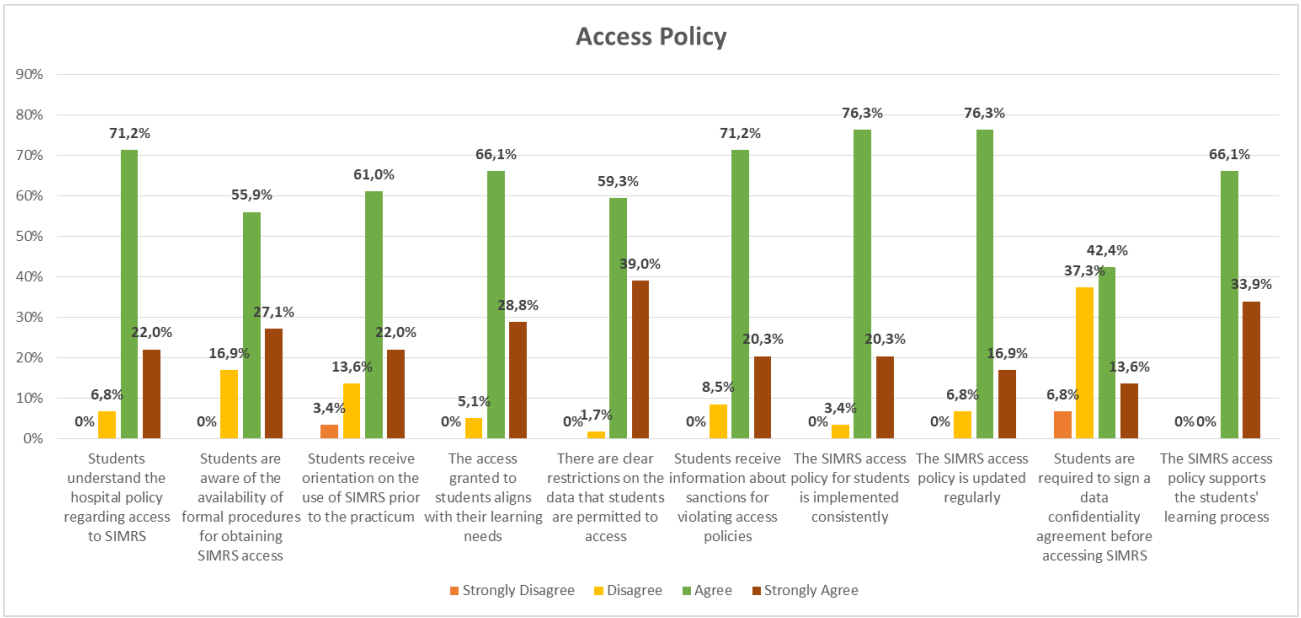

Figure 1. Access Policy Variable

In the implementation of SIMRS access policies for clinical practicum students, 10 statement items were measured. The results in the table show that most respondents (71.2%) strongly agreed that they were aware of the hospital's policy regarding student access to SIMRS, and 76.3% agreed that the SIMRS access policy was consistent. The strongest point was the clear limitation on the type of data that clinical practicum students could access, with 71.2% of respondents strongly agreeing. However, only 42.4% of respondents agreed and 37.3% disagreed that they were required to sign a confidentiality agreement before accessing SIMRS, making it the lowest point of this variable. This indicates that the hospital does not have a strict policy regarding the obligation for clinical practicum students to sign an integrity agreement.The measurement of the implementation of student access

authorization to SIMRS under the RBAC (Role-Based Access Control) variable was conducted using 12 statement items regarding the basic rules of data and information access control. The results are as follows:

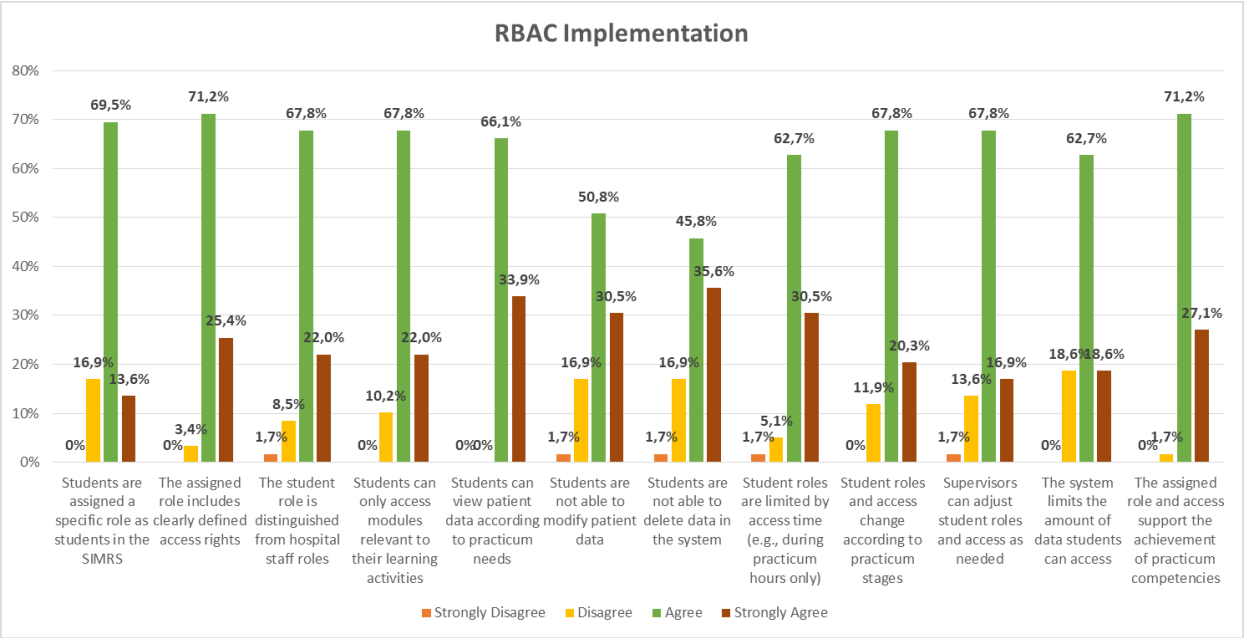

Figure 2. RBAC Implementation Variable

The measurement of RBAC implementation involved 12 statement items. The data in the table show that the majority of respondents (69.5%) agreed that they were assigned a specific role as students within the SIMRS. The strongest point was the ability of students to view patient data according to practicum needs (66.1% agreed, 33.9% strongly agreed). Most respondents also indicated that they could not modify patient data (50.8% agreed, 30.5% strongly agreed) and could not delete data from the system (45.8% agreed, 35.6% strongly agreed), demonstrating strong access control. The item regarding system restrictions on the number of data records students could access showed comparatively lower agreement (62.7% agreed, 18.6% strongly agreed) than other items.

The measurement of access authorization implementation for students regarding SIMRS in the data security variable was assessed through 8 statement items related to data and information security policies. The results are as follows:

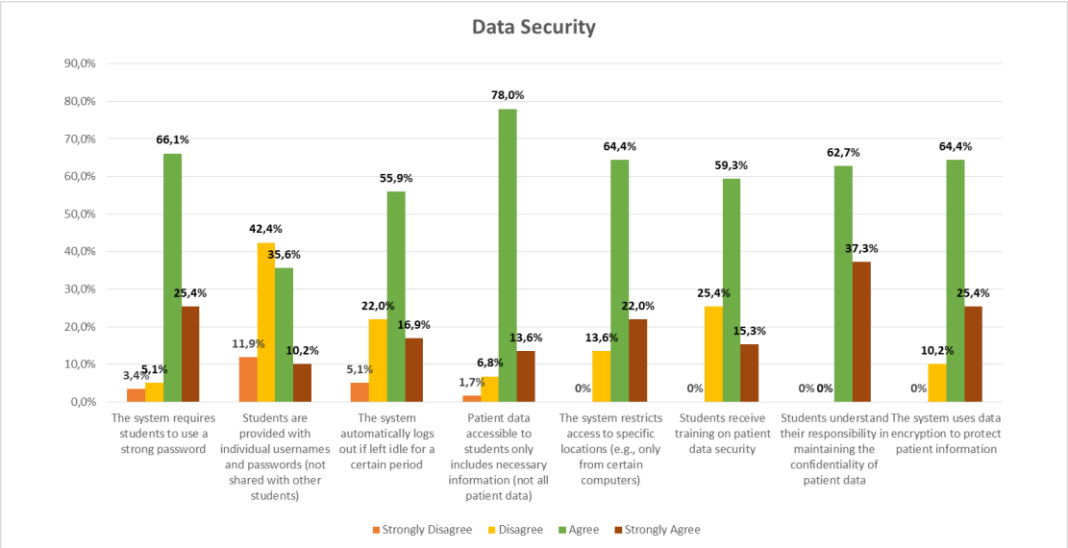

Figure 3. Data Security Variable

The data security variable was measured using 8 statement items. The majority of respondents (66.1% agreed, 25.4% strongly agreed) stated that the system required them to use a strong password. The strongest point was respondents' understanding of their responsibility to maintain patient data confidentiality (62.7% agreed, 37.3% strongly agreed). However, only 35.6% agreed that they had their own username and password (42.4% disagreed), indicating the practice of account sharing. The automatic system logout feature when not in use also needs improvement (55.9% agreed, 16.9% strongly agreed).

The measurement of the implementation of access authorization for students in SIMRS under the Audit Trail variable was assessed using 3 statement items related to SIMRS audit trail policies. The results are presented below:

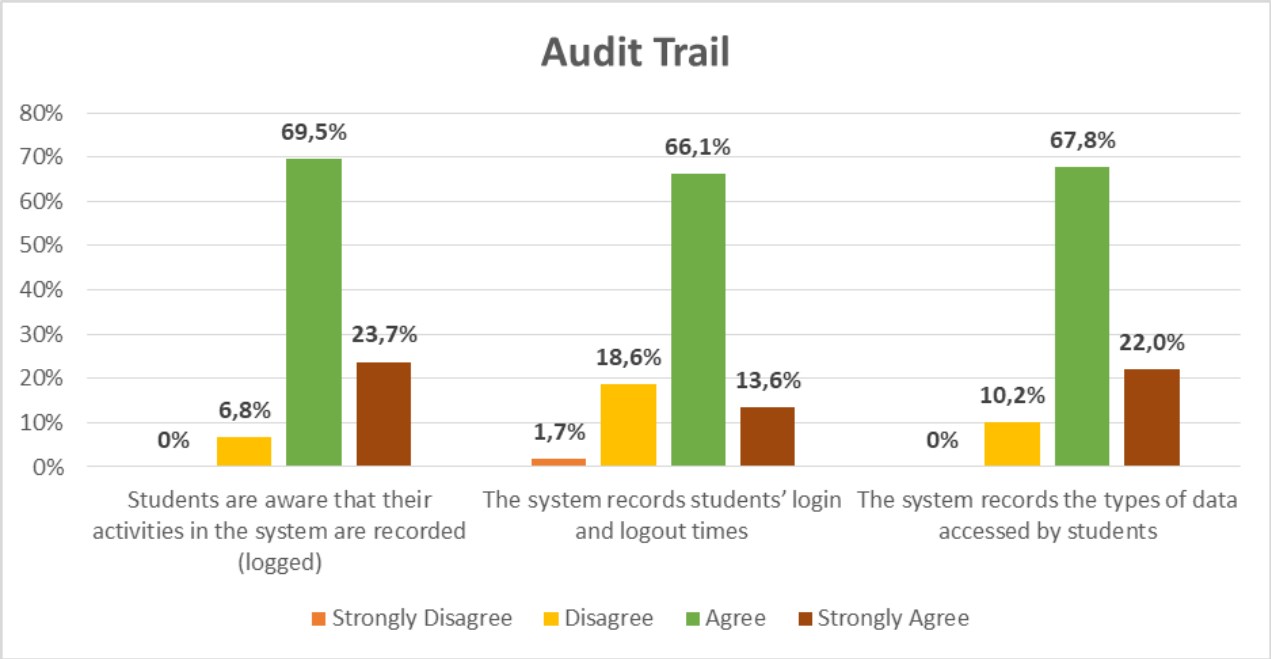

Figure 4. Audit Trail Variable

The audit trail variable was measured using 3 statement items. Most respondents were aware that their activities in the system were recorded (69.5% agreed, 23.7% strongly agreed), and the system documented login/logout times (66.1% agreed) as well as the data accessed (67.8% agreed). These findings indicate transparency in monitoring user activities.

This study provides a comprehensive overview of the implementation of the SIMRS authorization system from the perspective of clinical practicum students, as well as a preliminary evaluation of the implementation of the Electronic Clinical Pathway (E-CP) at the Poltekkes Kemenkes Tasikmalaya and its main clinical practicum sites. The high validity and reliability of the instrument (r-value > 0.444 and significance < 0.05 for validity; Cronbach's Alpha 0.811–0.955 for reliability) ensure the quality of the data collected.

The implementation of access policies and RBAC (Role-Based Access Control) in SIMRS is considered satisfactory by students. They feel that the access granted aligns with their learning needs and that clear data limitations are in place. A distinct role has been assigned to students, separate from hospital staff, indicating that the RBAC principle has been applied in the system's authorization design. The RBAC concept itself emphasizes assigning access rights based on user roles to ensure efficiency and security. Access tailored to learning needs and clearly defined access restrictions greatly support students in gaining relevant experience without the risk of accessing or modifying unauthorized data. This is crucial in supporting students' competency development, as hands-on experience with health information systems is vital to building competencies relevant to the professional world. There is a positive correlation between access to hospital information systems and the achievement of clinical practicum competencies among health students.

However, a significant gap was identified in the aspect of data security, particularly regarding the practice of account sharing. Only 35.6% of respondents agreed that they had their own username and

password, while 42.4% disagreed, indicating the occurrence of account sharing practices. Account sharing represents a serious security vulnerability, as it may lead to breaches of patient data confidentiality and hinder accurate tracking of user activities. Moreover, it may instill poor habits among students who will become future healthcare professionals. This finding is reinforced by the fact that most students were not required to sign a data confidentiality agreement (only 42.4% agreed), highlighting weaknesses in the administrative dimension of data security. The Health Act emphasizes the critical importance of maintaining patient data confidentiality.

In the audit trail variable, most students were aware that their activities were recorded in the system, including login/logout times and accessed data. This awareness is important for accountability and the prevention of misuse. However, the effectiveness of the audit trail feature heavily depends on strong policies to prevent account sharing. If usernames are shared, the audit trail becomes less effective in tracking the individual responsible for a particular action. Overall, the implementation of the SIMRS authorization system has a solid foundation in supporting student competence through controlled and relevant access. However, weaknesses in data security and the low implementation of access authorization in the field remain significant challenges that must be addressed promptly so that the SIMRS can optimally support the achievement of student competencies, not only technical but also ethical and aligned with professional standards. The implementation of SIMRS should always refer to the Ministry of Health Regulation No. 82 of 2013 concerning Hospital Management Information Systems.

To obtain a comprehensive assessment, the study results require the perceptions of practice site facilitators. Therefore, the perceptions of hospital Clinical Instructors (CIs) were collected to better understand the extent to which authorization policies are actually implemented in the hospital for internship students. The results showed:

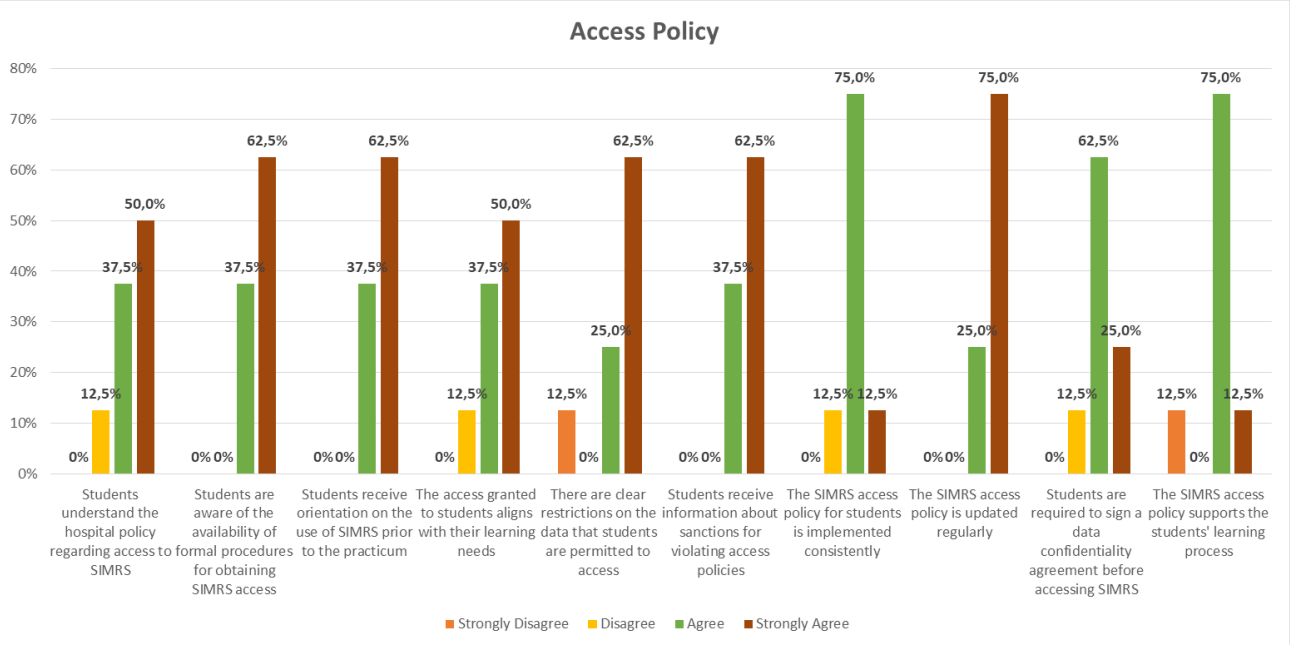

Figure 5. Access Policy Variable Based on CI Perceptions

In the access policy variable, CI perceptions indicated that the most positive aspect was the periodic updating of SIMRS access policies (75% strongly agreed). Conversely, the weakest aspect concerned the requirement to sign a data confidentiality agreement before accessing SIMRS, where the majority of respondents only agreed (62.5%) and 12.5% disagreed.

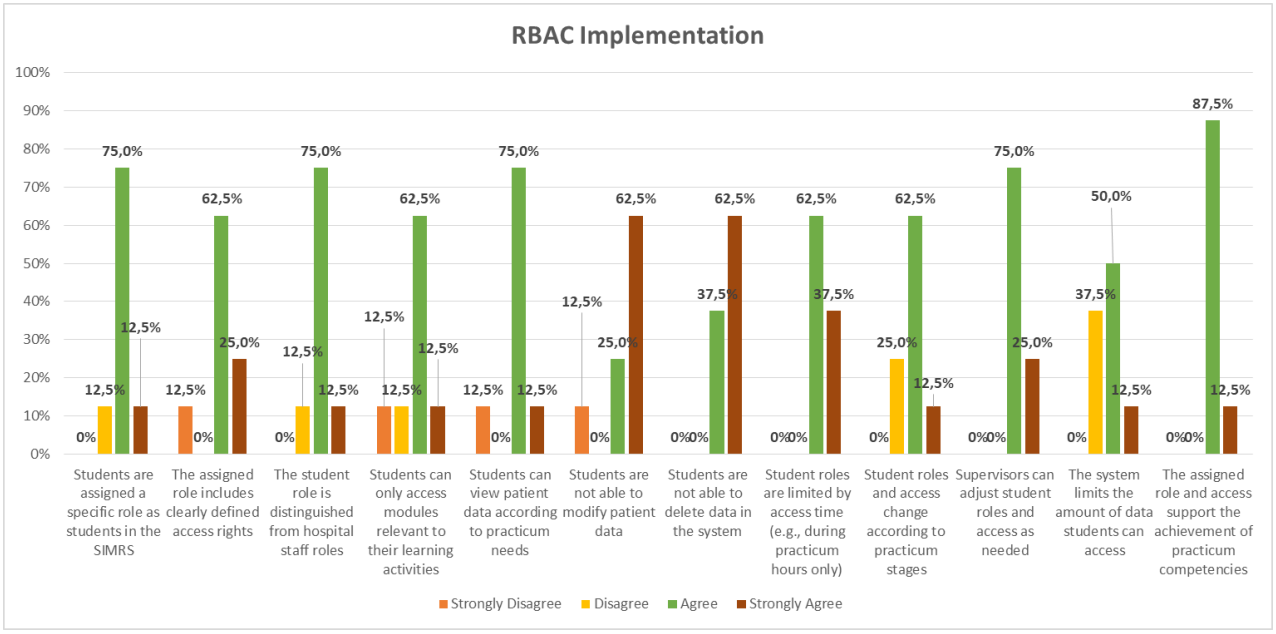

Figure 6. RBAC Implementation Variable Based on CI Perceptions

In the assessment of the RBAC implementation variable, CI perceptions indicated that the most positive aspect was the indicator stating that the roles and access granted supported the achievement of practicum competencies, with 87.5% of respondents agreeing and 12.5% strongly agreeing. Conversely, the weakest aspect was the indicator regarding the system's limitation on the amount of data that students could access, where 37.5% of respondents disagreed, 50% agreed, and only 12.5% strongly agreed. This indicates that although the student role in SIMRS has supported learning competencies, the policy on limiting data quantity has not been optimally implemented.

Figure 7. Data Security Variable Based on CI Perceptions

The assessment results of the data security variable showed that the most positive aspect was the indicator of CI's understanding of their responsibility to maintain patient data confidentiality, with 75% agreeing and 12.5% strongly agreeing. Conversely, the weakest aspect appeared in the indicator of having a personal username and password, where 37.5% of respondents disagreed and only 50% agreed, indicating that account-sharing practices among users still occur.

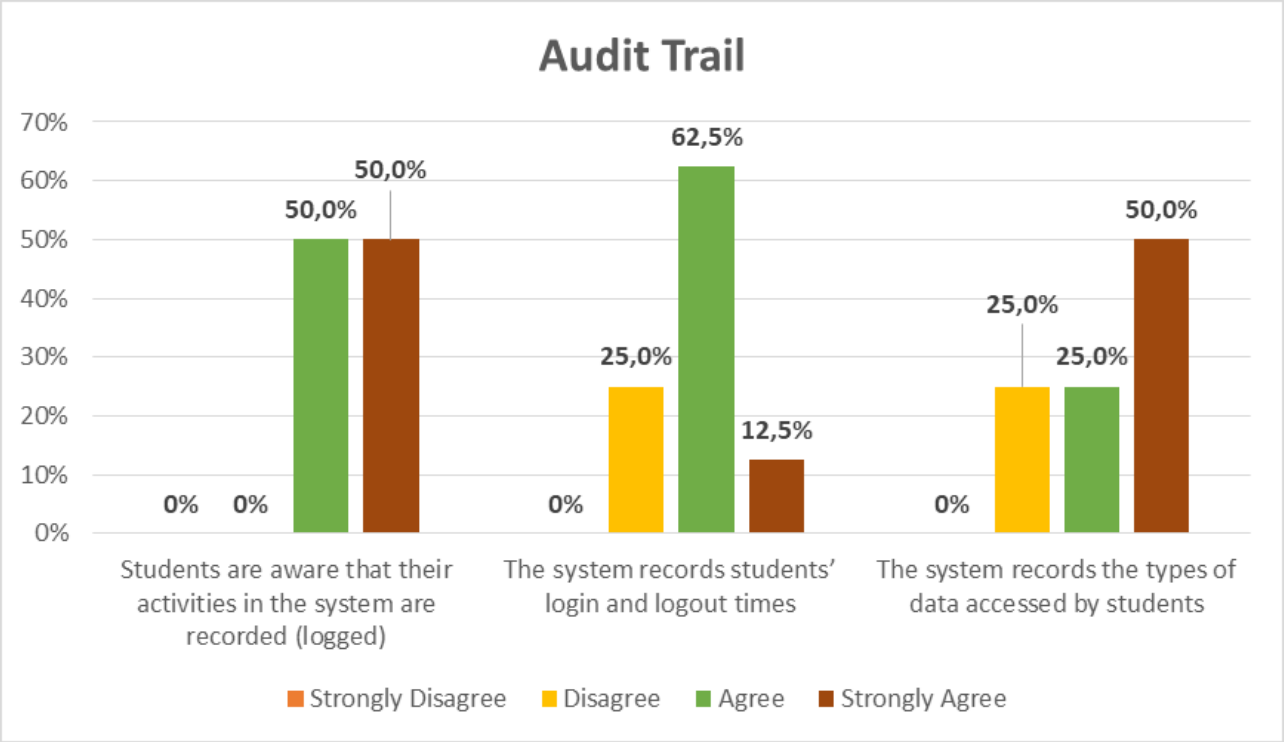

Figure 8 Audit Trail Variable Based on CI Perceptions

The audit trail variable was measured using 3 statement items. All CIs (50% agreed, 50% strongly agreed) acknowledged that their activities in the system were recorded. Most respondents also stated that the system recorded login and logout times (62.5% agreed, 12.5% strongly agreed), although 25% disagreed. In addition, 50% strongly agreed and 25% agreed that the system tracked the data accessed by users. These findings indicate that the user activity monitoring mechanism is functioning well, although a small proportion of respondents did not fully agree regarding the recording of detailed activities.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

SIMRS authorisation policies in the Poltekkes Kemenkes Tasikmalaya practicum network generally align with students' learning requirements by defining access roles and restricting data modification. Nevertheless, gaps in data-security practices—particularly account sharing and lax confidentiality agreements—undermine both patient privacy and professional development. Because this study relies on self-report and cross-sectional data, it cannot establish causal links between authorisation practices and competency achievement. We recommend strengthening data-security training, enforcing unique credentials and confidentiality agreements, and coordinating curriculum and practicum policies. Future studies should adopt larger samples, objective competency measures and inferential analyses to better understand how information-system authorisation shapes healthcare education.

Recommendations

Based on the study findings and analysis, several key insights have emerged regarding the implementation of the SIMRS authorization system in supporting student competencies. While the system demonstrates strengths in policy structure and role-based access control, persistent weaknesses in data security and confidentiality practices remain evident. To address these gaps and enhance both system performance and educational outcomes, the following recommendations are proposed for academic institutions and clinical practicum facilities.

REFERENCES

Addepally, A., Purkayastha, S., & Gichoya, J. W. (2017). Implementation of a single sign-on system between practice, research and learning systems. https://doi.org/10.4338/ACI-2016-10-CR-0171

Aritonang, I. J. (2018). Audit keamanan sistem informasi menggunakan framework COBIT 5 (APO13). ITEJ: Jurnal Ilmiah Teknik Elektro dan Komputer, 1(1). http://journal.syekhnurjati.ac.id/index.php/itej/article/view/27/27

Istiqlal, H. (2022). SIMRS GOS.

Jethwa, S., Bryant, P., Singh, S., Jones, M., Berlin, A., & Rosenthal, J. (2009). Your life in their pocket: Students' behaviors regarding confidential patient information. Family Medicine, 41(5), 327–331.

Kementerian Kesehatan Republik Indonesia. (2013). Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit.

Kementerian Kesehatan Republik Indonesia. (2023). Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 tentang Kesehatan.

Kusumaningtyas, T., Utarini, A., & Pinzon, R. T. (2017). Dampak pemberlakuan clinical pathway terhadap kualitas pelayanan stroke di RS Bethesda Yogyakarta. Berkala Ilmiah Kedokteran Duta Wacana, 2(2), 349–360. https://bikdw.ukdw.ac.id/index.php/bikdw/article/view/60

Perekam Medis dan Informasi Kesehatan, & Rumah Sakit Kota Yogyakarta. (2018). Evaluasi pencapaian kompetensi perekam medis dan informasi kesehatan di rumah sakit kota Yogyakarta berdasarkan metode self-assessment. Jurnal Kesehatan Vokasional, 3(1), 7–16. https://jurnal.ugm.ac.id/jkesvo/article/view/29594

Prihatiningsih, T. S. (n.d.). Kurikulum berbasis kompetensi (Capaian Pembelajaran) untuk pendidikan... [Google Books]. Retrieved April 10, 2025, from https://books.google.co.id/books?hl=en&lr=&id=gbGpEAAAQBAJ

Purkayastha, S., Gichoya, J. W., & Addepally, S. A. (2017). Implementation of a single sign-on system between practice, research and learning systems. Applied Clinical Informatics, 8(1), 306–312.

Sianturi, E., Soemitro, D., & dkk. (2016). Sistem informasi kesehatan [Google Books]. https://books.google.co.id/books?hl=id&lr=&id=hec_EAAAQBAJ

Tunggal, A. T. (2023). What is role-based access control (RBAC)? Examples, benefits, and more. UpGuard. https://www.upguard.com/blog/rbac

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157–178.

Wibowo, H. S. (2023). Pengembangan teknologi media pembelajaran: Merancang pengalaman langsung dengan sistem informasi kesehatan... [Google Books]. https://books.google.co.id/books?hl=en&lr=&id=OhTJEAAAQBAJ