Journal of Economics and Social Sciences (JESS)
Vol. 5, 1 (January-June, 2026), pp. 403-410
EISSN: 2830-5264, DOI: https://doi.org/10.59525/jess.1641

The Strategic Role of Hospital Management in Ensuring the Security of Health Information and Preventing Patient Data Leakage: A Case Study at Agung Mulia Hospital

Agung Suhirman[1], Muharyati[1], Latifah Indriasari Utami[1], Fajar Hadi Wijayanto[1], Marsudi Dedi Putra[1]

[1] Universitas Wisnuwhardana Malang, Indonesia

ARTICLE INFO

Keywords:

Hospital Management;
Information Security;
Data Breach

Article history:

Received 2025-03-25
Revised 2026-04-28
Accepted 2026-06-02

ABSTRACT

This study aims to analyze in depth the strategic role of hospital management at RSU Agung Mulia in formulating policies, implementing cyber protection systems, and overcoming operational constraints to ensure health information security and prevent patient data breaches. A qualitative approach with a descriptive research type was applied to uncover facts directly in the field through a natural setting. The primary data collection technique was conducted through in-depth interviews with three key informants, namely the Director, the Head of the Information Technology Unit, and the Head of the Medical Records Department, which was further strengthened by objective direct observation methods. The data analysis procedure followed an interactive model encompassing data reduction, data display, and conclusion drawing stages. The results of the study indicate that management policies are focused on formulating strict internal regulations, restricting medical data access rights based on job roles, and mandating the signing of staff integrity pacts. The main obstacles faced by the institution include operational budget constraints, outdated hardware conditions, and low digital literacy among administrative staff, which trigger human errors in the service area. Managerial efforts to circumvent these limitations are realized through a financial cluster strategy with hardware leasing options, optimizing operating systems using open-source software, and conducting periodic phishing attack simulations. The implementation of a reward and punishment system combined with the appointment of cyber pioneers has proven successful in altering staff behavior to become more disciplined and increasing operational compliance in safeguarding patient data confidentiality.

Corresponding Author:
Agung Suhirman
Universitas Wisnuwhardana Malang, Indonesia; spogagung@gmail.com

1. INTRODUCTION

The era of digitalization has changed the operational landscape in various fundamental sectors, including the healthcare industry globally. The integration of information technology in the hospital system is no longer just an innovative option, but an absolute necessity to improve efficiency and quality of services. The change from manual recording to a digital-based system is designed to speed up the administrative process, minimize medical errors, and facilitate coordination between health workers. This transformation requires a comprehensive readiness from all elements of the organization so that technology adoption can go hand in hand with the service quality standards expected by the community (Pujihastuti, 2021).

An integrated health information system plays a crucial role as the operational lifeblood of modern medical facilities. The existence of electronic medical records, online registration systems, and clinical databases allows healthcare providers to access patients' medical records in seconds. The speed of access has a significant impact on the accuracy of clinical decision-making, especially in emergency situations that require immediate treatment. The efficiency offered by digitalization ultimately contributes directly to improving patient safety and optimizing the work productivity of medical personnel (Ratnasari et al., 2024).

Patient health data is a type of information that is very sensitive and confidential because it includes personal identity, disease history, laboratory results, and financial information. This detailed and high-value data characteristic makes the healthcare sector a prime target for various cybercrime threats in cyberspace. Patient data leaks are not only materially harmful, but can also permanently damage the reputation of medical institutions and undermine public trust. The protection of the confidentiality of this information is a legal and moral mandate that must be strictly maintained by health service providers (Tampubolon et al., 2024).

The government has tightened regulations related to personal data protection through various legal instruments to respond to increasing digital security vulnerabilities. The regulation requires every public data management institution, especially hospitals, to implement a strict and accountable protection system. Compliance with the law is no longer just an administrative formality, but a benchmark for the professionalism and integrity of a medical institution in operating technology. Failure to comply with this regulation can have implications for severe legal sanctions, revocation of operational permits, and criminal charges for the management (Utami et al., 2024).

The hospital management holds the main control as the architect of the strategy in formulating policies, allocating budgets, and determining the direction of information technology governance. Visionary leadership is needed to build an information security-conscious culture across the organization, from the board of directors to the frontline administrative staff. Investment in sophisticated cybersecurity infrastructure will not function optimally without strict internal regulations and consistent supervision from managerial sides. Strategic steps of management are the main determinants of whether a digital health system can run safely or become a dangerous vulnerability loophole.

RSU Agung Mulia is currently facing serious challenges in the form of increasing frequency of cyber hacking attempts and partial data leak incidents caused by staff lack of awareness of digital security and weak updates to the internal protection system. This phenomenon is exacerbated by the limited allocation of special budgets for cyber risk mitigation, so that the technological defense infrastructure owned by this hospital is still lagging behind compared to the increasingly sophisticated rate of digital crime threats. This vulnerability triggers major concerns among patients regarding the security of their medical histories and has the potential to have serious legal consequences for institutions if not addressed promptly through systematic managerial intervention.

This research was carried out to analyze the strategic role of the management of RSU Agung Mulia in formulating policies, implementing cyber protection systems, and overcoming operational constraints to ensure the security of health information and prevent the leakage of patient data.

2. METHODS

Qualitative research is a research procedure that produces descriptive data in the form of written or spoken words from people and behaviors that can be observed directly. A qualitative approach is used to understand the phenomenon of what the research subject experiences in depth and thoroughly in the natural environment. This type of descriptive research is chosen because it aims to provide a systematic, factual, and accurate picture of the facts and characteristics of a particular population or area. The use of this qualitative descriptive method is considered most appropriate to reveal and explain how the strategic role of the management of RSU Agung Mulia is in real life in the field.

The main data collection technique is carried out through in-depth interviews to explore structured information about hospital digital security governance. This interview process involved three key informants who have authority and a deep understanding of the research object, namely the Director of RSU Agung Mulia as the highest policy maker, the Head of the Information Technology Unit as the technical implementer of cybersecurity, and the Head of the Medical Records Section who directly manages patient data. The three informants were deliberately selected using *purposive sampling techniques* so that the data obtained had high credibility and were in accordance with the needs of analysis. The information from the results of this direct question and answer is expected to be able to provide a holistic understanding of the commitments and managerial obstacles faced by the institution.

The observation method is applied directly as a supporting technique to strengthen the validity of the data obtained from the interview results. This observation activity is focused on the daily activities of administrative staff when operating the health information system, the implementation of password protection procedures in the work area, and the physical condition of the server infrastructure owned by RSU Agung Mulia. Field recording was carried out carefully to see the compatibility between the written policies presented by the management and the real implementation in the public service area. This step is crucial to identify security gaps that may arise due to human negligence or objective limitations of technical devices.

Data analysis techniques refer to interactive models that include the stages of data reduction, data presentation, and conclusion drawn. Data reduction is carried out by summarizing, selecting main things, and focusing analysis on matters related to the role of management and data leak prevention. The presentation of data is realized through structured narrative texts so that the pattern of relationships between variables can be easily understood by readers. Drawing conclusions is the final stage which is carried out by verifying the meaning of each data collected in order to produce a valid answer to the formulation of the research problem.

3. FINDINGS AND DISCUSSION

Fingings

Policies Implemented by the Management of Agung Mulia Hospital in Building a Health Information Security System to Prevent Patient Data Leakage

The policy implemented by the management of RSU Agung Mulia in building a health information security system is focused on the preparation of strict internal regulations and restrictions on medical data access rights. This initial step was taken as a managerial commitment to create a strong legal umbrella for all staff in operating electronic medical records. The governance structure is designed by establishing a new standard operating procedure that requires data encryption on every patient information traffic on the hospital network. Periodic monitoring has also begun to be scheduled to ensure that each service line complies with written instructions regarding the restriction of the use of personal external storage devices in the work environment.

The formulation of strategic policies at the highest level of the organization focuses on the aspects of legality and accountability of data management as a whole. The top management has issued a special decree that regulates strict sanctions for any violation of patient information privacy. This is in line with the results of an interview by the Director of RSU Agung Mulia, who said that:

"We have issued internal regulations requiring all staff to sign an integrity pact regarding the confidentiality of patient data, as well as allocating a dedicated budget in stages to update cybersecurity software to minimize hacking loopholes."

Policy implementation at the technical level is then translated into a network architecture setup that is more secure and isolated from public access. Access restrictions are created in layers using unique authentication methods that are tailored to each user's functions and authorizations. This is in line with the results of an interview by the Head of the Information Technology Unit, who said that:

"We are tightening our current digital defense system by installing new firewalls and dividing database access by job role, so that ordinary administrative staff will not be able to access in-depth clinical histories that are the full authority of doctors or medical personnel."

The storage and circulation of digital medical files at the downstream part of the service is also regulated through systematic and fast incident reporting procedures. The socialization of information confidentiality regulations began to be integrated into orientation programs for new employees as well as refresher training for senior staff on a regular basis. This is in line with the results of an interview by the Head of the Medical Records Section, who said that:

"Every computer in the medical record room is now set to automatically lock if left for two minutes inactivity, and we are required to log daily access so that every patient data review activity can be clearly tracked by its account holders."

The series of written policies and managerial commitments showed real alignment with the factual conditions in the field based on direct observations. Observations in the work area show that the computer screens on the registration desk and the medical record room are no longer left open when the officer is leaving the premises. The main data storage hardware or server has also been placed in a special room that is locked with login access using a fingerprint biometric scanner. Visual instructions in the form of warning posters regarding the prohibition of sharing passwords for SIMRS (Hospital Management Information System) accounts are clearly installed in every corner of the service room as a form of daily reminder for all employees.

Obstacles and Challenges Faced by RSU Agung Mulia in Implementing Electronic Medical Data Protection Procedures

The obstacles and challenges faced by RSU Agung Mulia in implementing electronic medical data protection procedures are rooted in financial limitations and resistance to digital work culture. These structural barriers slow down the process of modernizing security systems because the procurement of high-level protective devices requires enormous investment costs. The human factor is also a complicated challenge when most employees are still used to manual work patterns that are considered more practical and hassle-free. The unpreparedness of supporting infrastructure such as the stability of the local network often forces officers to take shortcuts that ignore basic security protocols in order to maintain a smooth queue of patient services.

The problem of limited operational budgets is the main stumbling block that limits the institution's room to move in updating the cyber defense system as a whole. The current allocation of funds must still be prioritized for the fulfillment of emergency medical facilities and the procurement of essential medicines. This is in line with the results of an interview by the Director of RSU Agung Mulia, who said that:

"We face a big dilemma in budget allocation because the cost of anti-hacking software licenses is very high, so we have had to upgrade the protection system gradually and not be able to cover the entire service installation."

Technical hurdles in the field are exacerbated by outdated hardware and the inability of legacy systems to be fitted with modern encryption protection. Update attempts often trigger technical glitches (*crashes*) in the hospital's main application programs because the specifications of the computers available in the workspace are outdated. This is in line with the results of an interview by the Head of the Information Technology Unit, who said that:

"Many of the computers in the service unit are still using older operating systems that have not received security updates, and our internal server capacity is so limited that it is often overwhelmed when running virus scans or bulk data encryption."

The low level of digital literacy of administrative staff creates new security gaps caused by human *error*. The habit of sharing login accounts and passwords between officers in order to speed up the data input process is still often found during busy service hours. This is in line with the results of an interview by the Head of the Medical Records Section, who said that:

"Officers often feel that double authentication procedures or having to change passwords on a regular basis greatly slow down their work, especially when dealing with a surge in outpatients who require fast-paced administrative handling."

The phenomenon of internal obstacles presented by the informants was proven to be in line with the results of observations carried out directly in various service units of RSU Agung Mulia. Observations in the registration area showed that some computers were still left on with the officer's account still active despite being left to rest. Small pieces of paper containing usernames and passwords were even found pasted under computer keyboards or behind file folders for the purpose of being easily remembered by colleagues. Some computer devices in inpatient units also saw significant performance slowdowns when network-based security systems were tried to run simultaneously.

Efforts of the Management of RSU Agung Mulia in Overcoming Infrastructure Limitations and Increasing Human Resources Awareness related to Cyber Protection

The efforts of the management of RSU Agung Mulia in overcoming infrastructure limitations and increasing human resource awareness related to cyber protection are realized through a priority-scale fund allocation strategy and continuous education programs. Management took a tactical step by dividing hardware updates into annual phases so as not to put a sudden strain on the institution's cash flow. A persuasive approach is also applied to change the mindset of employees through interactively designed cyber threat simulation training. This combined step between improving physical facilities and fostering a work mentality is taken to create a safe, resilient, and compliant healthcare ecosystem with national data protection standards.

Financial policy is geared towards budget efficiency by diverting some of non-priority expenditure to fund improvements to key database protection systems first. Top management is working with external service providers to provide a more budget-friendly hardware rental option than buying a new unit. This is in line with the results of an interview by the Director of RSU Agung Mulia, who said that:

"We are circumventing funding constraints by implementing a cluster system, where the main server and computers in crucial units such as medical records are prioritized for replacement this year, while other units will follow as we regularly hold weekly reminder forums about the danger of data leaks for all installation heads."

Technical solutions to overcome the limitations of computer devices are optimized through the use of open source-based software that does not require expensive licensing fees but still has a solid security system. System maintenance scheduling is carried out during service hours, such as midnight, to avoid system slowdowns during peak hours. This is in line with the results of an interview by the Head of the Information Technology Unit, who said that:

"Our team outsmarted this by optimizing the old operating system to keep it running a lightweight encryption protocol, as well as creating periodic phishing simulation programs to staff emails to test the extent of their prudence in opening incoming foreign links."

Increasing cyber literacy for administrative and medical personnel is strengthened by the preparation of a digital pocket book on practical cybersecurity guidelines that are easy to understand for all age groups. The reward *and punishment system* has begun to be strictly enforced to motivate employees to be more disciplined in maintaining the confidentiality of their personal accounts. This is in line with the results of an interview by the Head of the Medical Records Section, who said that:

"Management now holds a prize quiz around data security at monthly meetings, and we also appoint several senior staff in each unit to be cyber pioneers who are tasked with reminding their colleagues if anyone neglects to revoke their electronic medical record accounts after completing their duties."

The various managerial breakthroughs that have been presented by the leadership are proven to be in line with the results of observations carried out directly in the operational area of RSU Agung Mulia. Observations in the server room show that there is a new *Uninterruptible Power Supply* that has been installed to anticipate data damage due to sudden power outages. Staff at the registration counter now seem to be more agile in rejecting requests from outsiders who want to see monitors without valid identity verification procedures. A quick guide sheet on tips for creating strong and secure passwords also appears neatly pasted on each officer's desk area as an effective daily visual reference.

Discussion

The information security governance policy formulated by the management of RSU Agung Mulia shows a high strategic awareness of patient privacy protection in the digital era. The drafting of strict internal regulations and the creation of new Standard Operating Procedures (POS) regarding data encryption are crucial foundational steps to mitigate the risk of data leaks. The restriction of access rights that are tailored to the functions and authorities of each user proves the application of *the principle of least privilege*, where staff are only given the minimum level of access necessary to complete their tasks. This managerial step has succeeded in minimizing the chance of abuse of authority or unauthorized access by internal parties who are not interested in sensitive medical data (Azizah & Setiawan, 2017).

The formulation of strict sanctions through the director's decision and the obligation to sign an integrity pact for all staff strengthens the aspect of legal accountability in the hospital environment. This formal approach provides a strong moral foundation, so that every employee understands the legal consequences inherent in any electronic medical record management activity. The gradual allocation of the budget for protection software updates shows a realistic financial commitment in the midst of limited operational funds. This managerial intervention from the highest level is the main driving force in transforming written regulations into real work instructions that must be complied with without exception by all service lines (Budiman et al., 2025).

The implementation of technical security at the network level in the form of the installation of *new firewalls* has succeeded in isolating clinical databases from potential exposure of public networks that are vulnerable to cyberattacks. The existence of authentication unique to each user ensures that every digital trace and log of patient data examination activity can be accurately monitored and tracked. The automatic locking setting on the medical record computer that the officer left behind for two minutes acts as a highly effective technical safety net. This passive protection system is very useful for anticipating human negligence, especially when officers have to suddenly leave the work desk to serve the urgent needs of patients in the service area (Dewi & Haksama, 2025).

Financial obstacles in the form of high costs for cyber anti-hatching software licenses are the biggest structural challenges that limit the space for digitization of RSU Agung Mulia. The dilemma of budget sharing between the fulfillment of emergency medical facilities and information technology investment forces hospitals to operate with a security system that is not yet comprehensive. The condition of outdated hardware further exacerbates system vulnerabilities, as older computer specifications are not capable of running modern encryption programs optimally. System failures or *crashes* that often occur during mass virus scans indicate a misalignment between the demands of cutting-edge security software and the readiness of the physical infrastructure of internal servers (Firdaus, 2025).

The resistance factor of digital work culture and low cyber literacy among administrative staff triggers the emergence of the phenomenon of *human error* that endangers the integrity of databases. The habit of sharing login accounts and passwords during service rush hour reflects sectoral egos, where administrative speed comes at the expense of the principle of prudence. Officers tend to view dual authentication procedures as an operational burden that hinders their work rhythm when faced

with a surge in outpatient queues. The discovery of password note paper stuck around the computer keyboard area proves that staff's tactical awareness of data protection is still at an alarming level (Marbun, 2020).

The financial cluster strategy implemented by the board of directors through external hardware leasing options and priority upgrades to crucial units is a very smart managerial solution. Cost-saving steps through optimizing legacy operating systems using open-source-based lightweight encryption protocols are able to bridge the technology gap without draining cash flow (Pramesti et al., 2024). The implementation of periodic phishing attack simulations by information technology units acts as an effective evaluation instrument to test the mental readiness of staff directly. This practical approach not only improves the technical structure, but also slowly forces employees to always be wary of foreign links coming into work emails (Permatasari, 2024).

The implementation of the *reward and punishment system* combined with monthly interactive quizzes has succeeded in stimulating the active involvement of employees in maintaining data confidentiality. The appointment of senior staff as cyber pioneers in each unit creates persuasive and ongoing inherent oversight in the operational space. The installation of new power protection devices in the server space as well as the attachment of a quick guide sheet to generate passwords on the workbench showed positive results (Pratama & Purwanto, 2023). The change in the behavior of officers who are now more agile in closing monitor screens and denying access to outside parties without legal verification indicates that the investment of time and energy in management has succeeded in improving information security standards at RSU Agung Mulia.

4. CONCLUSION

The management of RSU Agung Mulia plays a very crucial strategic role in ensuring the security of health information through the issuance of strict internal regulations, role-based access rights restrictions, and periodic budget allocations for system updates. Tactical measures such as the implementation of financial cluster strategies, the use of optimized open-source software, and the procurement of interactive educational programs in the form of phishing simulations and monthly quizzes have proven effective in mitigating the constraints of infrastructure limitations and the resistance of the digital work culture of staff. The integration of managerial commitment at the top level and the inherent oversight by cyber pioneers in the field has significantly changed officer behavior to be more disciplined, improved operational compliance, and strengthened institutional defenses in preventing incidents of patient medical data leakage.

REFERENCES

Azizah, N. L. N., & Setiawan, M. V. (2017). Pengelolaan Informasi Kesehatan secara Terintegrasi untuk Memaksimalkan Layanan Kesehatan kepada Pasien di Rumah Sakit. *Indonesian Journal of Pharmaceutical Science and Technology*, *4*(3).

Budiman, A., Isa, M., & Soekiswati, S. (2025). Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta. *Ranah Research : Journal of Multidisciplinary Research and Development*, *7*(3).

Dewi, M. P., & Haksama, S. (2025). Pengaruh Manajemen Strategis terhadap Kualitas Pelayanan Pasien di Rumah Sakit. *PREPOTIF : Jurnal Kesehatan Masyarakat*, *9*(3).

Firdaus, D. A. (2025). Analisis Keamanan Informasi Rumah Sakit Menggunakan COBIT 2019 dengan Fokus Domain APO13: Systematic Literature Review. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(4).

Marbun, N. C. P. (2020). Strategi Pencegahan dan Pengendalian Dalam Upaya Pemutusan Rantai Infeksi di Rumah Sakit. *Jurnal Sain*. https://doi.org/10.31219/osf.io/a248z

Permatasari, P. (2024). Optimalisasi Upaya Pengelolaan Sistem Informasi Layanan Kesehatan di Rumah Sakit. *JIK JURNAL ILMU KESEHATAN*, *8*(2).

Pramesti, D. P. A., Ayuningtyas, D., & Verdi, R. (2024). Keamanan dan Kerahasiaan Data Medis Pasien dalam Implementasi Rekam Medis Elektronik: Tinjauan Sistematis. *PREPOTIF : JURNAL KESEHATAN MASYARAKAT*, *8*(3).

Pratama, I. F., & Purwanto, E. (2023). Sistem Informasi Manajemen Rumah Sakit Dalam Meningkatkan Efisiensi. *COMSERVA : Jurnal Penelitian dan Pengabdian Masyarakat*, *3*(07).

Pujihastuti, A. (2021). Penerapan Sistem Informasi Manajemen Dalam Mendukung Pengambilan Keputusan Manajemen Rumah Sakit. *Jurnal Manajemen Informasi Kesehatan Indonesia*, *9*(2).

Ratnasari, N. D., Ardanti, R. I., Purwadhi, P., & Widjaja, Y. R. (2024). Keamanan dan Kerahasiaan Data Medis Pasien dalam Implementasi Rekam Medis Elektronik: Tinjauan Sistematis. *Jurnal Kesehatan Tambusai*, *5*(4).

Tampubolon, E. T. F., Putera, A. P., & Huda, M. K. (2024). Pertanggungjawaban Hukum Rumah Sakit Terkait Kebocoran Data Pribadi Pasien Berdasarkan Peraturan Perundang-Undangan. *Syntax Idea*, *6*(3).

Utami, D. T., Muskitta, F. M., Fardiyani, F., Widjaja, Y. R., & Sanjaya, U. A. R. (2024). Analisis Hukum Manajemen Strategik Keselamatan Pasien di Rumah Sakit: Analysis of Legal Strategies for Patient Safety Management in Hospitals. *Jurnal Kesehatan Indra Husada*, *12*(2).