Journal of Indonesian Rural and Regional Government
Online ISSN: 2829-0798. Print ISSN: 2580-9342
Vol. 9 No. 1 (2025): Special Issue: Page no: 178-189

Implementation of Patient Data Protection Policy through the SMARTA-Based Electronic Medical Record System at Yogyakarta City Hospital

Ulfah Hidayati [1], Rumsari Hadi Sumarto [2]
[1,2] Sekolah Tinggi Pembangunan Masyarakat Desa APMD Yogyakarta, , Indonesia
Corresponding Author: kimulfahhidayati@gmail.com
DOI: https://doi.org/10.47431/jirreg.v9i1.719

Article Info
Article History;
Received:
2025-09-01
Revised:
2025-10-09
Accepted:
2025-10-28

Abstract: The protection of patient personal data is a crucial aspect of digital healthcare services. Yogyakarta City Hospital has implemented an SMARTA-based Electronic Medical Record (EMR) system as part of its policy to protect patient data in accordance with national regulations and internal hospital regulations. However, the success of policy implementation is not only determined by the existence of the system, but also by how the policy is implemented by those in the field. This study aims to analyze the implementation of patient personal data protection policies through the perspective of Edward III's Policy Implementation Theory, which covers four main variables, namely communication, resources, implementer disposition, and bureaucratic structure. This study used a qualitative descriptive approach with 20 informants selected through purposive sampling, involving medical record officers, information technology staff, health workers, legal staff, and management officials at the Yogyakarta City Hospital. Data were collected from August to October 2025 through in-depth interviews, observations, and documentation studies, then analyzed using the Miles and Huberman interactive model and validated through triangulation and member checking. The results of the study indicate that policy communication has been effective, but understanding of data access restrictions is not yet uniform, human resource competence in digital security is still limited, and coordination between units, especially between the information technology department and the polyclinic, is not yet optimal in handling patient data incidents. The results of the study show that based on interviews and observations, most informants stated that policy communication and the commitment of implementers to maintain the confidentiality of personal data had been carried out in accordance with procedures, although several technical obstacles were still found in the distribution of information and access monitoring, particularly in terms of clarity of communication and the commitment of implementers to maintain data confidentiality. However, there are still obstacles in the form of uneven distribution of information, limited human resource competencies related to digital security, the practice of using shared accounts, and monitoring mechanisms that tend to be reactive. This study is expected to provide practical recommendations for public hospitals in their efforts to improve patient data protection management in a sustainable and secure manner.

Keyword: *Patient data protection, electronic medical records, SMARTA, policy implementation, Edward III*

INTRODUCTION

The protection of patient personal data is an integral part of modern healthcare systems. In today's digital age, the use of information technology is the primary solution for improving the efficiency and security of medical records. One such innovation is the implementation of electronic

medical records (EMR), which enable healthcare providers to access patient personal data quickly and accurately while reducing the risk of data leaks.

Tifany Dwi Harant (2024), in her research, aims to analyze the forms of legal protection for patient data confidentiality in two systems, namely conventional hardfile-based (physical or paper) medical records and electronic medical records. In her research, Tifany divides legal protection into two main aspects: first, securing data confidentiality through storage regulations for both physical and digital archives; and second, establishing controlled procedures for accessing and distributing patient information.

Fita Rusdian Ikawati and Anis Ansyori (2023), in their research focusing on identifying various major obstacles in the implementation of Electronic Medical Records (EMR) related to the protection of patients' personal data. The results of the study show several obstacles, including a lack of strategic planning in the EMR data entry process, which has an impact on implementation that has not been carried out systematically and integrally.

In addition, Indra Indra, Trihoni Nalesti Dewi, and Daniel Budi Wibowo (2024) in their research journal examined how to assess the balance between the obligation to provide EMR data access to the government as stipulated in Permenkes No. 24 of 2022 and efforts to maintain patient data confidentiality. The results of this study show that although the regulation aims to strengthen national health data supervision and integration, its implementation in the field still faces ethical and technical dilemmas, particularly regarding potential violations of patient privacy due to a lack of control mechanisms and inadequate data security protection.

Ahdiana Yuni Lestari, Misran Misran, Trisno Raharjo, Muhammad Annas, Dinda Riskanita, and Adya Paramita Prabandari (2024), found in their research that there is a significant gap in the implementation of Minister of Health Regulation No. 24 of 2022 and Law No. 27 of 2022 concerning Personal Data Protection. This study shows that small-scale health care facilities, such as independent clinics, still face infrastructure and resource limitations in implementing these regulations. Inconsistencies in the implementation of data protection contribute to an increase in data leakage cases in various health care institutions.

Research conducted by Wahyuli, K. T., and Budi, S. C. (2022) at the Yogyakarta Regional General Hospital using the PIECES method discussed the relationship between staff perceptions of six aspects within the PIECES framework, namely Performance, Information, Economic, Control, Efficiency, and Service. The results of this study indicate the level of effectiveness of the implementation of the SMARTA-based SIMRS. From a total of 642 hospital employees, 87 respondents were selected using stratified random sampling. The results of the study show that simultaneously, these six aspects can explain 78.6% of the variability in the effectiveness of the implementation of the SMARTA SIMRS.

Siregar, R. A., and Sinaga, H. S. R. (2025), in their research, highlight the legal framework governing patient data protection in the implementation of Electronic Medical Records (EMR) in Indonesia. This article emphasizes that although digitization in the health sector brings great benefits in improving service efficiency, it also increases the potential risk of patient data leaks. Therefore, the protection of medical record data in the EMR system is seen not only as an ethical responsibility, but also as a legal obligation that must be fulfilled by health care facilities.

Ibrahim, A. M., et al. (2024), in their study examining how public health institutions implement policies to maintain patient data confidentiality while ensuring smooth service coordination. This study identifies various challenges and policy strategies used, such as data access rights regulations, encryption system implementation, audit implementation, and the development of internal policies that support data protection and service efficiency in government health institutions.

Research by Asrofi, A. F. (2024) examined the extent to which regulations related to the Electronic Medical Record (EMR) system have been implemented in various health care facilities in Indonesia. The results of this study show that the implementation of the EMR system still faces a number of obstacles, namely limitations in digital infrastructure, low human resource competence, and a lack of understanding of the legal provisions contained in Minister of Health Regulation No. 24 of 2022 concerning Medical Records. This research emphasizes the importance of synchronization between government policies, the readiness of relevant institutions, and the improvement of digital literacy among health workers as implementers to ensure effective patient data protection in the EMR system.

Research by Hossain et al. (2025) explores the level of adoption of Electronic Medical Records (EMR) and medical recording culture in various hospitals in Indonesia. This study found that the implementation of EMR systems still faces various organizational cultural barriers, such as resistance from practitioners to change from manual to digital systems, lack of training for practitioners, and the perception that electronic recording can slow down clinical workflows. Leadership factors, management support, and consistent government policies have proven to play an important role in promoting the successful implementation of EMR. These findings are relevant to research related to the SMARTA system at the Yogyakarta City Regional General Hospital, as they highlight the importance of work culture and internal policy functions in ensuring the successful implementation of patient personal data protection policies.

Research by Tertulino (2024) conducted a systematic mapping study related to privacy issues in the implementation of Electronic Medical Record (EMR) systems in various countries. The results show that the main threats to patient privacy include unauthorized access, encryption weaknesses, and low compliance with data protection policies. This study emphasizes the importance of combining strong regulations, secure system design, and the importance of training healthcare workers on the ethics of protecting patients' personal data. Its relevance to research at the Yogyakarta City Hospital lies in strengthening SMARTA system policies and governance to be in line with global principles of patient data security and privacy.

The study by Cobrado et al. (2024) is a systematic review that discusses various access control solutions in Electronic Medical Record (EMR) systems. The results of this study show that role-based access control (RBAC) and attribute-based access control (ABAC) approaches are considered the most effective methods for maintaining confidentiality and preventing misuse of patient personal data. This study also highlights the need for digital system audits and multi-layered system authentication to improve system security. The relevance to research at the Yogyakarta City Hospital lies in the implementation of strict access rights mechanisms in the SMARTA system to ensure the protection of patient personal data.

Research by Astuti and Fahyudi (2023) analyzed user satisfaction levels with the Electronic Medical Record Information System (EMR) at Tugurejo Regional General Hospital. The results of this study show that user satisfaction is influenced by factors such as ease of use, system reliability, and technical support from the IT team. Although the system is considered to help improve work efficiency, there are still obstacles related to access speed and user training. These findings are relevant to research at the Yogyakarta City Regional General Hospital, particularly in terms of user acceptance and adaptation to the SMARTA system, as well as the role of technical support in the successful implementation of patient data protection policies.

Yogyakarta City Hospital, as a government-owned hospital, has implemented an electronic medical record system based on SMARTA (Smart Medical Record and Administration). This policy is in line with Law No. 11 of 2008 concerning Electronic Information and Transactions, Minister of Health Regulation No. 24 of 2022 concerning Medical Records, and the principles of information

security in health services. This policy is regulated in detail in the Yogyakarta City Hospital Director Regulation No. 53 of 2022 concerning the Implementation of Medical Records at the Yogyakarta City Hospital.

The phenomenon observed in the field shows that there are still a number of obstacles, such as differences in perception regarding access rights among SMARTA users, limitations in the number of health workers who are competent in data security, and the discovery of data access practices that do not comply with procedures. It was found that some patients at the Regional General Hospital did not fully understand how their personal data was stored and protected in the digital system. This condition shows that the success rate of policy implementation is not only a matter of technological sophistication, but also concerns the readiness of resources and internal organizational governance.

Although the IT system has been implemented, the success of policy implementation cannot be assessed solely based on the existence of the existing system. The implementation of this policy system depends on how the policy is carried out by the implementing actors in the field. According to Edward III's policy implementation theory, there are four main variables that determine the success of policy implementation, namely internal communication within the organization, availability of resources, the disposition or attitude of the implementers, and a supportive organizational bureaucratic structure. In the context of the Yogyakarta City Hospital, these four variables are used as a reference to assess the extent to which the implementation of the patient personal data protection policy is consistently applied in the use of SMARTA.

Communication variables play an important role in ensuring that every implementing officer understands the policies, access procedures, and their responsibilities regarding patient data protection. Resource variables include the availability of competent health workers, adequate technological infrastructure, and various forms of technical support from the IT team. Disposition or attitude variables describe the level of commitment, compliance, and ethical awareness of officers in implementing data protection policies. Meanwhile, bureaucratic structure variables highlight the efficiency of organizational governance, division of authority, and oversight mechanisms implemented to ensure that policies are carried out in accordance with regulations. These four variables interact with each other and serve as the main benchmark variables in analyzing the success rate of implementing patient personal data protection policies at the Yogyakarta City Regional General Hospital.

Based on this background, this study aims to analyze the implementation of patient personal data protection policies through the SMARTA-based EMR System at Yogyakarta City Hospital using Edward III's Theory perspective. The focus of the research analysis is on four main implementation variables, namely communication variables, resource variables, implementer disposition variables, and bureaucratic structure variables, as well as identifying the obstacles or constraints encountered in its implementation. The results of this study are expected to not only contribute to the academic field, but also provide practical input for the hospital in improving its digital personal data protection management system to be secure, ethical, and sustainable.

RESEARCH METHOD

This study uses a qualitative descriptive approach that aims to explore and gain a deep understanding of how patient personal data protection policies are implemented through the SMARTA-based electronic medical record (EMR) system at the Yogyakarta City Hospital. This approach was chosen because it is considered appropriate for describing the processes, dynamics, and experiences of policy implementers in a real-world context. The focus of the research is not only on formal policies, but also on how these policies are applied, understood, and responded to by various related parties.

This study was conducted at Yogyakarta City Hospital, a government-owned general hospital that has implemented a SMARTA-based electronic medical record (EMR) system in an effort to improve service efficiency and patient data security. This location was chosen because Yogyakarta City Hospital is one of the pioneers in the implementation of digital medical record systems at the regional level in the Special Region of Yogyakarta. The research covered the preparation stage, data collection process, analysis, and reporting.

The research data was collected through three main techniques, namely in-depth interviews, observation, and documentation study. In-depth interviews were conducted face-to-face using semi-structured interview guidelines, so that informants could easily explain their experiences and views openly. Observations were carried out using passive participatory methods, namely directly observing how the SMARTA system was used in the Medical Records Department and health service units that were in direct contact with patients. Meanwhile, the documentation study was carried out by reviewing the hospital's internal policies, the standard operating procedures that were implemented, the guidelines for using the SMARTA system, and external regulations that were likely to be related to the protection of patients' personal medical records.

Data analysis in this study was conducted qualitatively using Miles and Huberman's interactive analysis model. The data analysis process began at the initial stage of data collection, through data reduction to sort relevant information, presentation of data findings in narrative form, tables, or charts to clarify the findings, and concluded with the drawing of conclusions that were verified repeatedly. Data validity was maintained through triangulation of data sources and methods, namely by comparing the results of interviews, observations, and documentation in order to ensure consistency of information. In addition, member checks were also carried out by asking informants to confirm the interpretation of the data obtained.

With this descriptive qualitative research approach, researchers are expected to be able to provide a comprehensive overview of how patient personal data protection policies are translated into practice through the SMARTA EMR system, including supporting factors, obstacles, and their implications for health information security at Yogyakarta City Hospital.

RESULT AND DICUSSION

Communication Variable

In Edward III's policy implementation theory, communication is one of the important factors that determine the level of success of policy implementation. Good communication includes clarity of policy content, consistency of message content, and smooth distribution of information to policy implementers. Based on the results of research at the Yogyakarta City Hospital, good communication has a strategic role in supporting the implementation of patient personal data protection policies through the SMARTA-based electronic medical record system.

In general, communication between the internal management of the hospital and policy implementers in the field has been running quite well. Management is able to routinely disseminate policies on patient data protection through various activities, such as coordination meetings, technical training on the use of the SMARTA system, dissemination during new employee orientation or student internship orientation, and dissemination of information through circular letters via the JSS (Jogja Smart Service) application and the hospital's internal communication platform. Informants or sources from medical record officers and IT staff revealed that they received clear explanations regarding data confidentiality rules, SMARTA system access rights, and their respective responsibilities in maintaining the security of patients' personal data.

Clarity of policy content is one of the factors that supports the implementation process. Information about the procedures for using the SMARTA system, the reporting mechanism in the

event of a data security incident, and data access rights rules have been outlined in Standard Operating Procedures (SOPs) and written guidelines in the Medical Records Department. Most employees understand the substance of the policy, especially those directly involved in patient data management. However, not all health workers have the same understanding of the policy. Several informants from among nurses and doctors admitted that the dissemination of the policy was sometimes brief and one-sided, so they did not have enough opportunity to discuss it and ask in-depth questions.

In addition to the clarity of the policy content, the mechanism for conveying information also has an impact on the success of communication. Yogyakarta City Hospital has utilized various types of communication channels, ranging from print media such as circulars and bulletin boards, to digital media through the hospital's internal messaging group and the SMARTA system itself. The use of these various channels aims to ensure that information reaches all service units quickly and evenly. However, in daily practice, the process of delivering information is not yet fully uniform. On several occasions, IT system updates or changes in technical procedures were only communicated to unit representatives, so that information was not always fully conveyed to all officers working directly in the field.

In terms of consistency, the messages conveyed by hospital management regarding policy are relatively stable and do not overlap. The instructions and provisions listed in the SOP are in line with the explanations provided during the socialization. However, when there are updates to features in the SMARTA system, the process of delivering information data often experiences delays. This causes several service units to have difficulty adapting quickly, especially in the login procedure and use of new security features.

Coordination between service units is also an important aspect of communication. The interviews revealed that coordination between the Medical Records Department, the Information Technology Department, and other health workers is not yet optimal. Communication channels for reporting technical problems or data security breaches tend to be bureaucratic, so the response to incidents is often not as quick as expected. Several informants suggested the need for more direct and responsive communication channels so that technical problems can be resolved immediately without having to go through a long bureaucratic reporting chain.

Overall, the findings of this study indicate that communication in the implementation of patient personal data protection policies through the SMARTA system at Yogyakarta City Hospital is sufficiently clear and structured, particularly in terms of the clarity of policy content and consistency of information messages. However, aspects of the data transmission process and coordination between service units still need to be strengthened so that policy implementation can run more optimally. This communication reinforcement is not only needed during the policy socialization process, but also in the rapid response mechanism to technical disruptions and data security incidents.

Resource Variable

Based on the results of the study, the implementation of patient personal data protection policies through the SMARTA-based Electronic Medical Record (EMR) System at the Yogyakarta City Regional General Hospital is influenced by the availability, capacity, and utilization of resources, including human resources, budget, information technology infrastructure, and support in the form of internal regulations.

1. Human Resources (HR)

   Yogyakarta City Hospital itself already has personnel from various elements such as medical record officers, IT staff, and health workers who are directly involved in the use of the SMARTA system. In terms of quantity, the number of human resources is considered

sufficient to support the system's operations. Internal personnel data shows that as of October 2025, there were 704 HR personnel at the Yogyakarta City Hospital, including medical staff and hospital management staff. Although the Yogyakarta City Hospital has implemented various periodic human resource competency development programs through training, the focus of the training is still dominated by material related to improving service and medical support skills. Training programs such as clinical skills, medical equipment operation, and health service quality standards are the top priorities in the annual agenda. On the one hand, this shows the hospital's commitment to maintaining service quality. On the other hand, training related to patient data protection and digital information security has not been given equal attention. Therefore, in terms of digital quality and competence, there is still a slight gap in capabilities among service officers, especially those who are not yet familiar with changes in information technology. This condition has resulted in the implementation of personal data protection not being uniform across service units.

2. Technological facilities and infrastructure
   The hospital has provided various hardware such as computers, servers, internet networks, and digital security systems (password protection and access authorization) to support the implementation of the EMR program. However, several informants have reported technical obstacles in the field, such as slow system access, server overload during peak hours, and limited hardware in some rooms, which hinder the consistent implementation of data protection.
3. Budget and funding support
   Funding for human resource competency development and the SMARTA system maintenance budget is provided through the BLUD RSUD cash budget or assistance from the City Government's APBD. The use of the human resource training budget is still limited to strengthening the implementation of patient personal data protection policies and training for IT and Medical Records Department personnel, as the training budget only focuses on developing the competencies of medical support staff. The budget for IT infrastructure support is used, among other things, for the purchase of computer and information technology materials (purchase of HDMI cables, HDMI splitters, micro HDMI, USB Type C adapters, LAN barrels, laptop power cables). Lini Shop. K25-0076, maintenance of computer equipment and supplies (purchase of holders, LED brackets, pointers, label ties), StarComp. K25-0079, maintenance of computer network equipment (purchase of Belden Cat6 Iron RJ45 connectors, Belden Cat 5 RJ45 Connectors for Switch Installation, LAN Installation, Wallmount Installation, FO Termination, UTP Cable Installation), Computindo, K25-0080, as well as computer network equipment maintenance with third parties (purchase of 19" Wallmount Racks) in collaboration with PT Sarana Insan Muda Selaras. The average IT infrastructure budget spends millions to tens of millions of rupiah per transaction. However, the allocation of funds specifically for strengthening data security and human resource training is still considered limited, so that security technology updates are not yet fully optimal.
4. Regulatory resources and SOPs
   The hospital has SOPs related to the use and management of patient data in the EMR system. All of these are regulated in the Yogyakarta City Hospital Director Regulation No. 53 of 2022 concerning the Implementation of Medical Records. Director Regulation No. 03 of 2018 concerning the Management of Internal Human Resources at the Regional General Hospital, Director Regulation No. 24 of 2021 concerning Internal Regulations for Medical Staff at the Regional General Hospital, several SOP guidelines for medical record services, medical record organization, and SOPs in the event of planned or unplanned downtime or failure to access

SMARTA, so that services can continue to run. However, there is still a discrepancy between the written rules and their implementation in the field, particularly in monitoring the use of access rights by unauthorized users.

Disposition or Implementers' Attitude Variable

Based on the results of the study, the implementation of patient data protection policies through the Electronic Medical Record System (SMARTA) at the Yogyakarta City Hospital is greatly influenced by the disposition or attitude of policy implementers. This disposition includes the commitment, compliance, and responsibility of implementers in maintaining the security and confidentiality of patient data. Among them are the following:

1. Implementers' commitment to data protection

   Most of the staff in the Medical Records Department, health workers, and IT Department staff showed a positive commitment to maintaining the confidentiality of patient data. They realized that medical information is sensitive and should not be accessed carelessly. This cautious attitude was demonstrated by not sharing login accounts and refusing access requests from unauthorized parties. One medical records officer during a new employee orientation session in the Teratai Room of the Regional General Hospital said, "We in the medical records department, healthcare personnel, and IT are all committed to maintaining the confidentiality of patient data. We understand that medical information is sensitive and should not be accessed carelessly. Therefore, we never share login accounts, and if anyone requests access without a clear reason, we immediately refuse."
2. Ethical awareness and responsibility

   Informants stated that data protection is not only an administrative obligation, but also a moral responsibility and a form of respect for patient rights. This is reflected in the practice of staff not disclosing patient data without clear medical or administrative reasons. Quoted in a direct explanation by the Medical Records Department team during an orientation activity for interns in the Main Hall of the Regional General Hospital, which was attended by various interns from universities in the Yogyakarta area, "Data protection is not only an administrative obligation, but also our moral responsibility as health workers. It is a form of respect for patient rights. We will not disclose patient data if there is no clear medical or administrative reason."
3. Variations in compliance levels among implementers

   Although most implementers have a good attitude, differences in compliance levels were found among units. Some officers still consider the use of shared accounts to be a normal practice to speed up service. This permissive attitude has the potential to lead to misuse of access, which can weaken data protection. In high-workload service situations, especially in service units that handle large numbers of patients, sharing login accounts is considered a practical solution to avoid access queues or technical obstacles due to periodic account changes. However, although efficient from an operational perspective, this practice poses a major risk to the security of patients' personal data. With accounts used by more than one person, the system cannot identify who actually accessed or changed the data, thus obscuring individual responsibility. Furthermore, shared accounts open up opportunities for illegal access or misuse of patients' personal data without accurate traceability. Therefore, while the use of shared accounts is practical in speeding up service, it also carries serious risks in terms of accountability and patient data protection.
4. Response to monitoring and evaluation

Service employees who receive warnings or evaluations related to access rights violations generally accept them well and are willing to correct their mistakes. However, not all implementers have the proactive initiative to report potential data security risks.

Bureaucratic Structure Variable

The internal bureaucratic structure of Yogyakarta City Hospital plays an important role in supporting the implementation of patient personal data protection policies through the SMARTA system. Based on the results of the study, the bureaucratic structure in the implementation of this policy was analyzed through the existence of SOPs, coordination patterns, and the division of authority between implementing units.

1. Availability of Standard Operating Procedures (SOPs) as guidelines for implementation
   Yogyakarta City Hospital has SOPs related to patient data management and the use of the SMARTA-based EMR system. These SOPs cover mechanisms for granting access rights, data entry procedures, and handling information leaks. However, the implementation of SOPs has not been consistent, especially in service units with high workloads, so that some service officers sometimes ignore or skip formal procedures in order to speed up service.
2. Cross-unit coordination that is functional but not yet optimal
   There is a coordination structure between the Medical Records Department, IT Department, Medical Services Department, and internal hospital management. Formally, coordination takes place through regular coordination meetings and communication via internal systems. However, in practice, responses to system disruptions or access violations are sometimes delayed, as there is still excessive dependence on the IT Department team as the sole technical controller.
3. Division of authority and fragmentation of tasks
   System management authority is divided between the Medical Records Department as data administrator, the IT Department as SMARTA system manager, and the leadership as policy decision-makers. Although this division is clear structurally, the fragmentation of tasks causes some cases to be handled slowly, especially when access violations occur that require cross-unit coordination.
4. Internal supervision that is not yet fully strict and measurable
   Internal oversight of the implementation of patient data protection is carried out through internal audits and login system monitoring. However, this oversight mechanism is more reactive than preventive, so that violations are only dealt with after an incident has been reported. There is no early warning system or automatic reporting related to access rights that are considered suspicious.

CONCLUSION

Based on the results of the analysis of the implementation of patient personal data protection policies through the Electronic Medical Record System (SMARTA) at the Yogyakarta City Hospital, it can be concluded that the implementation of the policy has been running quite well, but still faces a number of challenges in operational practice.

In terms of communication, the policy has been routinely disseminated through various formal channels such as meetings, socialization, training, and internal media. The clarity of the policy content and consistency of the message have been reflected in the SOP and written guidelines. However, the distribution of information has not been entirely uniform because some IT system updates or procedural changes have only been received by a handful of people, namely unit representatives, so that understanding or perception at the direct implementer level still varies. Coordination across units

is also still bureaucratic, so that the response to technical incidents or access rights violations has not been optimal.

In terms of resources, the availability of technological infrastructure and human resources is considered sufficient to support SMARTA's operations. However, in terms of competence and training allocation, human resource development is focused more on clinical and medical support training, while specialized training related to digital data security and personal data protection is still limited. This has led to a gap in understanding data access governance and information security risk management. Similarly, IT budget allocation is directed more towards hardware maintenance than strengthening data security systems.

In terms of the disposition or attitude of implementers, in general, policy implementers show a positive commitment to maintaining patient data confidentiality. This is demonstrated by their cautious attitude in using login accounts and their refusal to grant unauthorized access. However, the practice of using shared accounts is still considered acceptable to speed up service, even though it is recognized as posing a high risk to data security. This means that implementers support the policy, but are still influenced by considerations of service efficiency, so that not all procedures are carried out in a disciplined manner.

Finally, in terms of bureaucratic structure, Yogyakarta City Hospital has clear SOPs and division of authority between the Medical Records, IT, and service units. However, implementation has not been consistent in the field, especially in units with high workloads. The monitoring mechanism is still reactive, with follow-up actions taken after violations occur. The reporting and technical coordination system also lacks a fast track, resulting in delayed responses to incidents.

ACKNOWLEDGEMENT

The author would like to express special thanks to the management and all employees of Yogyakarta City Hospital for granting permission, providing support, and cooperating throughout the research process. Thanks are also extended to the medical records officers, Information Technology staff, and health workers who were willing to serve as informants and provide valuable information that greatly contributed to the success of this research.

The author also expresses his deep appreciation to his academic advisor for the guidance, direction, and motivation provided during the preparation of this research. Last but not least, the author would like to thank his family and colleagues who have always provided moral support, encouragement, and prayers so that this research could be completed successfully.

REFERENCE

1. Asrofi, A. F. (2024). *Review of the implementation of the electronic medical record regulation in Indonesia. International Journal of Scientific Research (IJSR) / National Review, 13*(2), 45–52.

2. Astuti, N. D., & Fahyudi, A. (2023). *User satisfaction of Electronic Medical Record Information Systems (case: RSUD Tugurejo). Jurnal Manajemen Kesehatan Indonesia.*

3. Bungin, B. (2017). *Metodologi penelitian kualitatif.* Jakarta: Kencana.

4. Cobrado, U. N., Silva, M. R., & Fernandes, P. T. (2024). *Access control solutions in electronic health record systems: A systematic review. Computers in Biology and Medicine.*

5. Edward III, G. C. (1980). *Implementing public policy.* Washington, DC: Congressional Quarterly Press.

6. Harant, T. D. (2024). *Perlindungan hukum terhadap kerahasiaan data pasien antara rekam medis konvensional dan elektronik. Jurnal Hukum Kesehatan Indonesia, 9*(1), 45–57.

7. Hossain, M. K., Rahmawati, D., Nugraha, A., & Setiawan, E. (2025). *An exploratory study of electronic medical record adoption and recordkeeping culture in Indonesian hospitals. BMC Health Services Research.*

8. Ibrahim, A. M., et al. (2024). *Balancing confidentiality and care coordination: Challenges in the digital age. BMC Health Services Research, 24*(1), 117–129. https://doi.org/10.1186/s12913-024-XXXXX

9. Ikawati, F. R. (2024). *Challenges in implementing digital medical records in Indonesian hospitals: Perspectives on technology, regulation, and data security. ICISTech Journal.*

10. Indra, I., Dewi, T. N., & Wibowo, D. B. (2024). *Perlindungan kerahasiaan data pasien vs kewajiban membuka akses rekam medis elektronik. Jurnal Hukum dan Kesehatan, 8*(1), 33–48.

11. Lestari, A. Y., Misran, M., Raharjo, T., Annas, M., Riskanita, D., & Prabandari, A. P. (2024). *Improving healthcare patient data security: An integrated framework model for electronic health records from a legal perspective. Jurnal Keamanan Informasi Kesehatan Indonesia, 3*(1), 1–15.

12. Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Thousand Oaks, CA: Sage.

13. Siregar, R. A., & Sinaga, H. S. R. (2025). *Aspek hukum perlindungan data pasien dalam penyelenggaraan rekam medis elektronik di Indonesia. Jurnal Hukum To-ra, 11*(1), 106–116.

14. Tertulino, R. (2024). *Privacy in electronic health records: A systematic mapping study. International Journal of Public Health.*

15. Wahyuli, K. T., & Budi, S. C. (2022). *Analisis efektivitas implementasi sistem informasi manajemen rumah sakit (SIMRS) di RSUD Kota Yogyakarta dengan metode PIECES. Jurnal Sistem Informasi Kesehatan, 4*(3), 201–215.

16. Instruksi Presiden Republik Indonesia Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government.

17. Peraturan Direktur RSUD Kota Yogyakarta No. 53 Tahun 2022 tentang Penyelenggaraan Rekam Medis di RSUD Kota Yogyakarta.

18. Permenkes RI No. 24 Tahun 2022 tentang Rekam Medis.

19. Peraturan Direktur RSUD Kota Yogyakarta No. 03 Tahun 2018 tentang Pengelolaan SDM Internal RSUD.

20. Peraturan Direktur RSUD Kota Yogyakarta No. 24 Tahun 2021 tentang Peraturan Internal Staff Medis RSUD.

21. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

22. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.