Widya Cipta : Jurnal Sekretari dan Manajemen
Volume 9 No. 2 September 2025
ISSN (Online) 2550-0791 | ISSN (Print) 2550-0805
DOI: https://doi.org/10.31294/widyacipta.v9i2.26065

Data Privacy Risk Governance in Hospital Management Information System: A Proposed Framework for Hospital in Padang

Muhammad Galing Ganesworo[1*], Raden Aswin Rahadi[2]

[1,2]Master of Business Administration Program, Institut Teknologi Bandung
Jalan Gelap Nyawang No. 1, Bandung, Indonesia

Corresponding e-mail: galing_ganesworo@sbm.itb.ac.id

Submission:	Revision:	Acceptance:	Available Online:
04-06-2025	17-06-2025	14-07-2025	01-09-2025

Abstract - The implementation of Hospital Management Information Systems (SIMRS) in Indonesia, mandated by the Ministry of Health, reflects the country's digital transformation in healthcare particularly in managing electronic medical records (EMRs), operational efficiency, and patient data security. This study aims to develop a privacy risk governance framework by integrating three key references: COSO Enterprise Risk Management (ERM) 2017, ISO/IEC 27701:2019, and Indonesia's Personal Data Protection (PDP) Law No. 27/2022. Employing a qualitative case study approach, data were collected through in-depth interviews with five key stakeholders and analyzed thematically. Five major themes emerged: (1) Governance and Leadership in Privacy Risk, (2) Privacy Risk Identification and Assessment, (3) Privacy Controls and Operational Safeguards, (4) Monitoring and Incident Management, and (5) Legal and Regulatory Compliance. The study identified fragmented privacy practices, weak governance structures, and limited awareness of privacy obligations. To address these gaps, a phased improvement plan is proposed—starting with the appointment of a Data Protection Officer (DPO), the development of privacy-related standard operating procedures (SOPs), and the implementation of privacy impact assessments. These steps are designed to improve digital maturity and regulatory alignment. The proposed governance model is adaptable and scalable for other hospitals in Indonesia facing similar challenges. Ultimately, this framework contributes to enhancing patient safety, ensuring data protection, and supporting a sustainable digital health transformation.

Keywords: Data privacy, Risk governance, Hospital management information

1. Introduction

In today's digital era, the phenomenon of globalization has encouraged massive improvements in data processes and transfers, which directly increases risks, especially related to the security and privacy of personal data (Organisation for Economic Co-operation and Development, 2015). Many incidents of digital security breaches have occurred, where consumers' personal data has been stolen by external parties such as hackers (Häuselmann & Custers, 2024). In addition, privacy risks also arise from unethical practices, such as the clandestine sale of consumer data to third parties or the misuse of personal data without additional consent.

This challenge is becoming increasingly urgent in the healthcare sector, where highly sensitive patient data is collected and processed every day (Ferdosi & Molavi, 2020; Sari et al., 2023; Wibowo et al., 2022). As digital threats increase, information security is now the main foundation in maintaining the confidentiality of patient data and organizational resilience (Cavoukian, et al., 2010). According to (Alder, 2025), the number of individuals affected by data breaches reached a record high in 2024, which is more than 250 million people since 2009, which indicates the urgency of a stronger data protection strategy.

In the healthcare sector, the hospitals face two main types of risks: clinical and non-clinical risks (Widyastuti et al., 2023). Clinical risks include events that directly impact patient safety such as surgical complications, misdiagnosis, medication misadministration, healthcare-related infections (HAIs), as well as delays in emergency handling (Jiménez-Rodríguez et al., 2018). In contrast, non-clinical risks arise from administrative, technological, legal, or operational aspects that have an indirect impact on patients (Bhati, et al., 2023). Examples are data breaches, system failures, regulatory non-compliance, weaknesses in vendor supervision, and errors in medical record management (Lawand et al., 2015; Etges et al., 2018). In this context, hospital information systems that are the backbone of clinical efficiency and data accuracy are the main targets of data privacy risks, especially those related to unauthorized access, misuse, and improper disclosure of patients' personal data (ISO/IEC, 2019; Organisation for Economic Co-operation and Development; Manongga et al., 2024).

Patient data is not just administrative information, but data that is clinically crucial, ethically sensitive, and legally protected. Information such as medical history, genetic data, diagnosis outcomes, and treatment plans are critical

components of providing quality and sustainable health care. Therefore, healthcare institutions that are able to protect patient data across the board will build patient trust and strengthen their credibility (Cheryl & Ng, 2022; Skagerström et al., 2022; Rahmadani et al., 2022).

Especially in Indonesia, the hospitals are required to digitalize their services and infrastructure comprehensively through Hospital Management Information System (SIMRS), which functions to improve service quality, operational efficiency, and patient data security (Dihartawan at al., 2023; Pratama & Setiawan, 2023). However, along with this increase in digitalization, data privacy risks are also increasing and are now a crucial part of non-clinical risk management. If not handled systematically, these risks can lead to violations of the law, loss of public trust, and leakage of patient confidentiality (OECD, 2015; ISACA, 2020). The need for information security and privacy governance is also increasingly emerging with the issuance of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which is the basis for national regulations for personal data protection.

Although global and national regulatory frameworks are in place, the reality is that many hospitals in Indonesia still face practical challenges in implementing effective data protection standards. The hospital is a real example of this situation. As a type C specialist surgical hospital that has been in operation for more than 37 years, Hospital has demonstrated a wide range of institutional achievements, including KARS Primary Level accreditation and strategic partnerships with BPJS. However, a review of the 2024 risk register documents shows that of the 131 documented risk items, none identified risks to privacy, information governance, SIMRS vulnerabilities, or legal compliance related to digital data processing. This shows that there is a serious gap between operational practices and regulatory obligations that are growing.

Further, the SIMRS infrastructure is operated in cooperation with third parties, but there are no contractual clauses that explicitly establish the vendor's responsibility as a data processor or the obligation to notify data breaches. The role of internal IT units is also limited to technical remediation, with no involvement in privacy governance or breach incident escalation flows (Baker, et al., 2016). On the other hand, medical records units still use physical forms to manage patient consents without digital integration into the SIMRS system, so there is no audit mechanism that ensures compliance or electronic tracking of consents. Although Hospitals already have written policies on patient rights, the right to privacy has not been operationally associated with SIMRS workflows, consent management, or data subject access requests (Di Martino et al., 2022; Kuner et al., 2020).

This condition shows institutional fragmentation, where privacy risks are still seen as administrative or legal issues, rather than as strategic organizational risks. The lack of integration between the medical records unit and the SIMRS IT unit, plus gaps in vendor contracts and approval tracking, creates a high-risk environment both regulatively and ethically. These business issues demonstrate the importance of implementing an integrated risk management framework as emphasized in COSO ERM, which demands stronger risk governance and internal controls, particularly in the face of the digital age and the protection of personal data.

2. Research Methods

2.1 Research Design

This study uses a qualitative case study approach to analyze governance and risk management in the context of compliance with the Personal Data Protection Law (PDP Law) at Hospital (Yin, 2028; Yan, 2023). The main focus is directed at how the hospital handles privacy risks through the hospital management information system (SIMRS) by referring to the COSO Enterprise Risk Management (ERM) FRAMEWORK, ISO/IEC 27701 as the privacy information management system (PIMS) standard, and PDP Law Number 27 of 2022 as the basis of national law.

The design of this study was compiled following the approach proposed by Creswell (2014), which allows an in-depth exploration of organizational dynamics through various data sources, in particular semi-structured interviews and document analysis. A qualitative approach is considered appropriate to understand the reasons and mechanisms for implementing privacy policies as well as the institutional challenges that arise in the context of the digitalization of health services (Braun & Clarke, 2006). The series of stages of this research include:

1. Problem Identification: The initial stage is carried out through a review of internal Hospital documents, including *risk registers* that do not include privacy risks, as well as cooperation contracts with third-party SIMRS providers that do not adequately contain data protection clauses.
2. Literature Review: An in-depth literature review is used to strengthen the theoretical foundation, including an understanding of the COSO ERM FRAMEWORK, ISO/IEC 27701, and the regulations of the PDP Law.
3. Theoretical Foundation: The three frameworks are used as a conceptual reference for research: COSO ERM in assessing risk governance, ISO 27701 for aspects of operational control and information security, and the PDP Law as a national legal framework.
4. Conceptual Framework: Based on the gaps found, a conceptual model is prepared that maps the

linkages between governance components, operational practices, and regulatory obligations.
5. Methodological Approach: This study took Hospital as the main unit of analysis. The focus is directed at institutional awareness, internal control systems, as well as stakeholder engagement in privacy risk management.
6. Research Design: The research questions are arranged in harmony with the indicators in the framework of COSO, ISO, and the PDP Law. The case studies were selected based on the hospital's specialty, digital maturity level, and risk visibility.
7. Data Collection: Data was collected through interviews with five key informants representing strategic, operational, technical, and regulatory aspects. Document analysis is also carried out as a form of data triangulation.
8. Data Analysis: Thematic analysis was carried out by following six stages according to Braun and Clarke (2006), with a deductive approach based on the framework of COSO ERM, ISO 27701, and the PDP Law (Nowell et al., 2017).
9. Interpretation: Results are comprehensively analyzed across roles and between frameworks, to identify institutional gaps and policy inconsistencies.
10. Conclusions and Recommendations: The research resulted in a number of recommendations for improvement, including the appointment of a data protection officer (DPO), the renewal of SOPs, the digitization of patient consent, and the strengthening of data protection clauses in third-party vendor contracts.

2.2 Data Collection Techniques

The main data collection was carried out through semi-structured interviews with five purposively selected informants based on direct involvement in data management and SIMRS. The interview lasted 40–60 minutes, was recorded with the respondent's consent, and transcribed verbatim. The informants consist of:

1. Hospital Director: Provides a strategic perspective in SIMRS decision-making and policy (Code 1).
2. Quality and Risk Management Committee: Conveys information related to the risk identification, evaluation, and compliance monitoring process (Code 2).
3. Chief Medical Recorder: Describes operational aspects, such as patient data management, approval mechanisms, and data retention (Code 3).
4. IT Department Representative: Provide technical insights related to the implementation of SIMRS and data access control (Code 4).
5. Ministry of Health Officials (DTO): Convey regulatory views and policy challenges in terms of supervision and compliance (Code 5).

In addition to the interviews, additional documents analyzed included internal hospital policies, SOPs, *risk registers*, vendor contracts, as well as relevant legal frameworks and standards.

2.3 Data Analysis Techniques

Data analysis was carried out through *the Thematic Analysis method* which refers to the six stages of Braun and Clarke (2006), namely:

1. Data Recognition: Interview transcripts and documents are thoroughly reviewed to understand the context and identify initial patterns.
2. Initial Code: Data is coded deductively based on the main categories of COSO ERM (e.g., *Governance & Culture*), ISO/IEC 27701 (e.g., *Consent Management*), and the PDP Act (e.g., *Breach Notification*).
3. Theme Search: The code is grouped based on contextual meanings related to privacy risk management, such as "Leadership's Commitment to Privacy" and "Data Lifecycle Weaknesses".
4. Theme Review: Themes formed versus cross-roles to ensure consistency and accuracy of meaning.
5. Theme Naming: Each theme is given a definition and name according to its relevance to the research question and theoretical framework.
6. Synthesis of Findings: The theme is prepared in an integrated manner with SOP document analysis, role comparison, and mapping of the COSO-ISO-PDP framework.

Describing the chronological research, including research design, research procedures (in the form of algorithms, Pseudocode or others), how to test and acquire data. The research program description should be supported by references; thus, the explanation can be accepted scientifically.

3. Results and Discussion

3.1 Thematic Analysis

This chapter presents the thematic findings from interviews and document review conducted at Hospital as the data. After familiarizing the data, initial codes were generated from the interview transcripts. Subsequently, key themes were identified by combining several related codes line-by-line using three key frameworks that aligned together as mentioned in this study:

1. COSO Enterprise Risk Management (ERM) 2017 Framework which determined the Enterprise Risk Management structure governance, strategy, performance, information, monitoring
2. ISO/IEC 27701:2019 Privacy Information Management System (PIMS) consists of Privacy Principles, Roles, Controls
3. Indonesia's Law No. 27 of 2022 on Personal Data Protection (PDP Law) consist of legal basis for Data Protection, Rights of Subjects, Security

Obligations.

3.2 Themes and Codes

The thematic analysis focused on identifying privacy-related risks and governance gaps in the implementation of the Hospital Management Information System (SIMRS) at Hospital. As the main system for processing and storing patient data, SIMRS presents as the critical points for data governance. In which the goal of this analysis was to synthesize insights that are presented with the thematic flowchart (Figure 1) below that guided this analysis, illustrating how conceptual constructs from each framework are translated into grounded, operational findings.

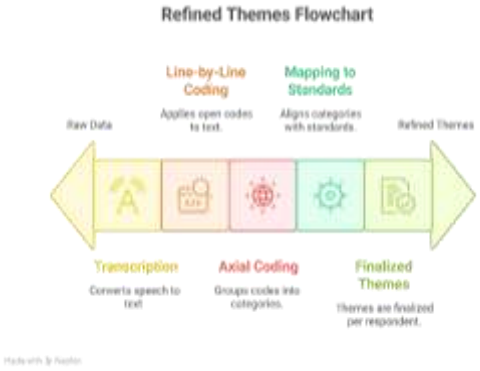

Figure 1. Refined Thematic Flowchart

By combining deductive coding from the three frameworks and inductive coding from the five respondent transcripts. This method is suited for applied research where predefined conceptual frameworks guide inquiries, but where flexibility is required to accommodate contextual insights from the stakeholders which is beneficial when researchers aim to validate theoretical constructs while also allowing novel themes to emerge directly from participant narratives (Fereday & Muir-Cochrane, 2006; Tamene, 2016).

The method ensures both theoretical relevance and empirical authenticity, which is essential in institutional settings like hospitals where privacy governance is both regulated and variably implemented. This thematic coding uses four levels as explained below: raw interview data (Level 1: direct respondents quotes), initial codes (Level 2: condensed meaning units), sub-themes (Level 3: categorized group), and final themes (Level 4: themed concepts aligned with frameworks) as explained in table 1 below.

Table 1. Coding Structure

Level 1: Raw Data	Level 2: Initial Codes	Level 3: Sub-Themes	Level 4: Final Themes
"We haven't included data privacy in our risk register."	Absence of privacy in risk register	Lack of privacy risk identification	Governance and Leadership in Privacy Risk
"There's no dedicated Data Privacy Officer (DPO) "	No formal data protection governance	Unassigned roles and leadership	Governance and Leadership in Privacy Risk
"Basically, we assess risks only after the incidents happen."	Reactive risk management	Absence of proactive risk identification	Privacy Risk Assessment and Identification
"We've started moving to digital towards electronic medical records but no IT audit trail in the system yet."	No IT audit trail in place	Weak monitoring infrastructure and no traceability mechanism	Monitoring and Incident Management
"Consent is still manual, patient's consent is written then we uploaded to the system"	Manual consent documentation	Gaps in consent management	Privacy Controls and Operational Safeguards
"Vendors still hold the data, we supervise only."	Vendor holds full access	Lack of internal data ownership control	Privacy Controls and Operational Safeguards
"There's no SOP if there's a data incident or breach happens.	No formal incident response	Lack of structured response procedures	Monitoring and Incident Management
"We're not fully familiar with the PDP Law yet."	Limited legal compliance understanding	Partial awareness of legal obligations	Compliance with Legal and Regulatory Requirements

Level 1: Raw Data	Level 2: Initial Codes	Level 3: Sub-Themes	Level 4: Final Themes
"Our contract doesn't clearly define data controller or data processor roles."	Weak clause contracts	Incomplete third-party compliance framework	Compliance with Legal and Regulatory Requirements

Next, the five themes determined certain aspects of the frameworks and are followed by statements from selected stakeholders in Hospital as explained below in thematic analysis by theme:

Table 2. Aligned Coded Theme 1

Respondent Code	Observed Gap	Evidence (Quote/Summary)	What to Do (Follow-up Question)
Code 1	No DPO assigned; no formal policy	"There's no policy yet for appointing a DPO."	What resources would be needed to formally designate a DPO?
Code 2	Privacy roles not formalized in SOPs	"SOPs only list general information management roles, not privacy risk ownership."	How could Komite Mutu contribute to establishing privacy SOPs?
Code 4	SIMRS team has no governance linkage	"We just run the system... the policy part is with the management."	What structure would help IT work with compliance roles?

Based on this theme on strategic level, hospital director and risk committee members acknowledged that privacy is not yet embedded into formal risk governance structures. The statement mentioned: *"We haven't included data privacy as a non-clinical risk, in our risk register because our risk management strategy focused on clinical risks"*. (Code 1) This confirms the lack of strategic alignment at the intuitional level. Table 3 shows Aligned Coded Theme 2.

Table 3. Aligned Coded Theme 2

Respondent Code	Observed Gap	Evidence (Quote/Summary)	What to Do (Follow-up Question)
Code 2	Privacy not in Risk Register	"We haven't identified data privacy in our risk register."	What steps could be taken to incorporate privacy risks?
Code 1	Risk identification is reactive	"We review incidents after they happen."	What process could enable early warning systems?
Code 5	No structured hospital PIA	"We haven't required PIAs, just general data mapping."	Could the Ministry support standardized PIA tools or training?

On this theme, risk assessment also involved hospital director and quality committee conducting risk assessments thoroughly and proactively, but the Hospital lacks both institutional processes and awareness for forecasting or modeling data risks before they occur.

The statement is mentioned below: "*We assess risk after something has happened, not before*," (Code 2). This confirms the lack of strategic alignment at the intuitional level in terms of privacy and lacks proactive risk assessment that align with the COSO ERM's framework.

Additional insight, *"We have no SOP if data breaches happen. We just follow general practice, but there's no fixed procedure yet."* (Code 3). This also violates COSO's "Monitoring Activities" and ISO 27701 Clause 10.1. PDP Law Article 21 mandates reporting of breaches within 72 hours. Table 4 shows Aligned Coded Theme 3.

Table 4. Aligned Coded Theme 3

Respondent Code	Observed Gap	Evidence (Quote/Summary)	What to Do (Follow-up Question)
Code 3	Consent is manual; not digital	"Consent is still partly manual, we use written signatures although we will upload it again "	What would be required to digitize and integrate consent in SIMRS?
Code 4	No audit trail in SIMRS	"We've started moving to digital, but no audit trail yet."	Can SIMRS log user access? If not, what's missing?
Code 1	Vendor controls infrastructure	"We supervise, but the vendor handles everything technical."	How can hospital build internal ownership of SIMRS data?

By this theme, Code 3 risk assessment also involved hospital director and quality committee conducting risk assessments thoroughly to doing mandates, "*the process is still partly manual and inconsistent across departments and there's limited understanding*" (Code 4) of PDP Law obligations and no specific clauses in vendor contracts that define roles like data controller or processor. Table 5 shows Aligned Coded Theme 4.

Table 5. Aligned Coded Theme 4

Respondent Code	Observed Gap	Evidence (Quote/Summary)	What to Do (Follow-up Question)
Code 4	No SOP for breach response	"There's no SOP if a breach happens."	What are the barriers to writing a formal SOP?

Respondent Code	Observed Gap	Evidence (Quote/Summary)	What to Do (Follow-up Question)
Code 2	No breach simulation/test	"We just correct and report after the issue."	What kind of testing could help staff prepare?
Code 3	Poor integration between records & IT	"We only know if IT tells us something's wrong."	How can breach handover be improved between units?

As mentioned in this theme *"there are no SOP if data breaches happened"*. This made in violates COSO's "*Monitoring Activities*" and other ISO also with the PDP Law for data breach handling. This directly affects COSO's "Monitoring Activities" and ISO 27701's clauses on audit controls and incident response (Clause 10.1). According to PDP Law Article 21, breach notifications must occur within 72 hours currently, Hospital lacks any formal mechanism to meet this requirement. Table 6 shows Aligned Coding Theme 5.

Table 6. Aligned Coding Theme 5

Respondent Code	Observed Gap	Evidence (Quote/Summary)	What to Do (Follow-up Question)
Code 5	Vendor contracts lack PDP clauses	"Our contract doesn't clearly define processor roles."	What clauses should be added to vendor agreements?
Code 1	PDP Law not reflected in policies	"We haven't translated PDP Law into our SOPs yet."	What training is needed to support PDP implementation?
Code 2	Compliance only triggered by surveyors	"Usually we prepare for surveyors, not proactively."	How can audits be aligned with ongoing PDP compliance?

3.3 Findings and Implications for Privacy Risk Governance

Thematic analysis of the internal conditions of Hospital shows that data privacy governance is still not fully integrated into institutional strategies. While there have been several efforts such as restricting account access in SIMRS and increasing awareness of data privacy, five key themes weak governance leadership, reactive risk identification approaches, absence of incident management systems, weak operational controls, and non-compliance with legal regulations point to fundamental gaps strategically, operationally, and regulatory (Sari et al., 2023).

One of the crucial issues is the low understanding of the PDP Law and the absence of a vendor contract clause that clearly establishes the role of data controller and processor (González, 2020). This is not only contrary to the important articles of the PDP Law (Articles 5–7 and 35–46), but also inconsistent with COSO principles regarding the communication of the role and requirements of ISO 27701 in third-party control. This vacancy shows the need for thorough legal education and revision of third-party contracts.

Furthermore, Hospital also faces structural challenges such as limited resources, high dependence on SIMRS vendors, fragmentation of responsibilities between work units, and technical ambiguities in access control and audit mechanisms (Sari & Amelia, 2022). Coupled with the lack of clarity on the practical implementation of the PDP Law, this condition poses serious institutional risks ranging from administrative sanctions, reputational loss, to operational disruptions (Putra & Kurniawan, 2023; Yusuf et al., 2021). To address these challenges, a gradual and contextual strategy with a three-level approach is needed:

1. Strategic Level – Leaders need to place privacy governance as the core value of the institution, in accordance with COSO's principles of culture and governance.
2. Operational Level – A standard SOP, digital tools for approval and auditing, and role documentation aligned with ISO/IEC 27701 are required.
3. Regulatory Level – The legal obligations of the PDP Act should be integrated into day-to-day activities, including role designations, incident reporting flows, and contractual adjustments with third parties.

These findings form the basis for the strategy and roadmap for strengthening privacy risk management in SIMRS which will be described in the next chapter. The five major themes illustrate the governance, technical, and legal gaps that must be addressed immediately so that hospitals can transform towards sustainable and regulatory compliance (Kuner et al., 2015).

3.4 Leadership and Governance at Risk Privacy

Preliminary findings show that there is no formal structure related to privacy governance at the managerial level. The absence of an official *Data Protection Officer* (DPO) and the absence of privacy issues in the *risk register* indicate a weak integration between risk strategies and personal data protection. A statement from one of the informants, "We have not entered privacy data in the risk register because our strategy focuses on clinical risk," confirms that privacy is still not treated as a strategic non-clinical risk. This is contrary to the principles of "Governance & Culture" within the framework of COSO ERM and demonstrates the urgent need to explicitly define roles and responsibilities in the management of privacy risks.

3.5 Reactive Risk Identification Approach

Furthermore, it was found that the risk identification process is reactive. Hospitals tend to conduct risk assessments only after an incident occurs, as quoted: "We assess risk after something

has happened, not before." This indicates the absence of a predictive mechanism or *privacy impact assessment* (PIA) model that can help map potential risks before the implementation of new policies or systems. This lack of a proactive approach undermines prevention efforts and hampers the institution's ability to systematically respond to risks in accordance with the "Strategy and Objective Setting" principles in COSO and ISO 27701 best practices.

3.6 Absence of Incident Management and Monitoring System

Regarding the aspect of incident supervision and response, the analysis shows the absence of *a standard operating procedure* (SOP) that specifically handles data breach incidents. In addition, SIMRS is not equipped with adequate *trail audits* to trace user activity, thus weakening incident monitoring and tracing capacity. One of the informants stated: "There is no SOP in case of a data breach, we just follow common practices." This condition is contrary to the principle of "Monitoring Activities" in COSO and clause 10.1 of ISO 27701, and violates Article 21 of the PDP Law which requires incident reporting within 72 hours. The absence of simulations or incident response training also shows that there is no institutional readiness to deal with potential data breaches.

3.7 Weaknesses in Operational Control an Technical Safety

The analysis also revealed weaknesses in the technical-operational control aspect. For example, the process of granting patient consent is still done manually, which is then uploaded to the system without full digital integration. In addition, control over data is still dominated by third parties or vendors, while hospitals only conduct surveillance without full ownership of the data. Statements like, "The vendor manages everything, we just keep an eye on," reflects the weak internal controls over the systems that are the backbone of patient data management (Janssen et al., 2020). This shows that *operational safeguards* and privacy controls have not been implemented comprehensively.

3.8 Non-compliance with Legal Regulations and Standards

The last theme is related to the aspect of legal compliance. The results of the interviews show that the understanding of the PDP Law is still limited among hospital managers, and there has been no integration of these legal norms into internal policies or vendor contracts. The cooperation contract has not explicitly distinguished the roles of *data controller* and data *processor*, which are fundamental in personal data protection. Compliance is more *event-driven*, that is, triggered by an external audit or survey, rather than as part of an ongoing process. This shows that regulatory awareness is still low and has not become part of the organizational culture, so hospitals have not fully complied with the provisions of Articles 5–7 and 35–46 in the PDP Law.

3.9 Implications of the Findings

The five themes identified indicate fundamental gaps in institutional strategies, operational risk management, and legal compliance in data privacy governance at Hospital. Strategically, privacy has not been positioned as an essential element in institutional risk governance. From an operational perspective, weak integration between units, absence of incident reporting systems, and limited technical controls indicate the need for significant internal capacity building. Meanwhile, from a regulatory perspective, the implementation of the basic principles of the PDP Law in internal policies and external contracts reflects the need for more systematic education, training, and reformulation of privacy policies.

To improve institutional readiness, concrete steps are needed such as the appointment of DPOs, digitization of the patient approval process, the creation of incident SOPs, and the integration of PDP principles into vendor contracts and internal policies. This approach will not only strengthen legal compliance, but also increase public trust in the management of personal data in healthcare settings.

4. Conclusion

The study uncovered five key issues in the protection of personal data at Hospital . First, the absence of the appointment of a Data Protection Officer (DPO) and the non-inclusion of privacy risks in the risk register indicate weak governance and leadership aspects. Second, risk management, which is still reactive, shows that there is no anticipatory approach to data threats. Third, the absence of monitoring mechanisms and standard operating procedures (SOPs) in handling data breaches is a weakness in incident management. Fourth, gaps in privacy control were found, especially in consent procedures and lack of control over third parties. Fifth, a low level of understanding of regulations such as the Personal Data Protection Law (PDP Law) is a challenge in ensuring legal compliance (Martin, 2023). These findings reflect the gap between hospital-run practices and national and international standards, and show that Hospitals' digital maturity index is still low.

References

Alder, S. (2025). *Individuals affected by healthcare security breaches (2009–2024)* [Graph]. HIPAA Journal. https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/

Baker, D., Kaye, J., & Terry, S. F. (2016). *Governance Through Privacy, Fairness, and*

Respect for Individuals. *4*(2), 1207. https://doi.org/10.13063/2327-9214.1207

Bhati, D., Deogade, M., & Kanyal, D. (2023). Improving patient outcomes through effective hospital administration: A comprehensive review. Cureus. https://doi.org/10.7759/cureus.47731

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by Design: Essential for organizational accountability and strong business practices. Identity in the Information Society, 3(2), 405–413. https://doi.org/10.1007/s12394-010-0053-z

Cheryl, B., & Ng, B. (2022). Protecting the unprotected consumer data in Internet of Things: Current scenario of data governance in Malaysia. Sustainability, 14(16), 9893. https://doi.org/10.3390/su14169893

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

Di Martino, M., Meers, I., Quax, P., Andries, K., & Lamotte, W. (2022). Revisiting identification issues in GDPR 'Right Of Access' policies: A technical and longitudinal analysis. *Proceedings on Privacy Enhancing Technologies*, *2022*(2), 95–113. https://doi.org/10.2478/popets-2022-0037

Dihartawan, D., Fatma, L., Baiduri, W., et al. (2024). Analysis of factors affecting hospital risk management in Indonesia: The SEM-PLS approach. Kesmas, 19(2), 135–143. https://doi.org/10.21109/kesmas.v19i2.1106

Etges, A. P. B. da S., Grenon, V., Lu, M., Cardoso, R. B., Souza, J. S. de, Kliemann Neto, F. J., & Felix, E. A. (2018). Development of an enterprise risk inventory for healthcare. *BMC Health Services Research*, *18*(1), 1–16. https://doi.org/10.1186/S12913-018-3400-7

Ferdosi, M., Rezayatmand, R., & Molavi Taleghani, Y. (2020). Risk management in executive levels of healthcare organizations: A comprehensive framework and tools for effective risk assessment. Risk Management and Healthcare Policy, 13, 1–10. https://doi.org/10.2147/RMHP.S229879

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80–92. https://doi.org/10.1177/160940690600500107

González Fuster, G. (2020). The right to erasure in EU data protection law: The challenges of implementation. *International Data Privacy Law*, *10*(1), 1–12. https://doi.org/10.1093/idpl/ipz024

Häuselmann, A., & Custers, B. (2024). The right to rectification and inferred personal data. *European Journal of Law and Technology*, *15*(3). https://ejlt.org/index.php/ejlt/article/view/1004

ISACA. (2020). Aligning COSO and privacy frameworks. ISACA.

Janssen, H., Janssen, H., Cobbe, J., & Singh, J. (2020). Personal Information Management Systems: A User-Centric Privacy Utopia? *Social Science Research Network*. https://doi.org/10.2139/SSRN.3779655

Jiménez-Rodríguez, E., Feria-Domínguez, J. M., & Sebastian-Lacave, A. (2018). Assessing the Health-Care Risk: The Clinical-VaR, a Key Indicator for Sound Management. *International Journal of Environmental Research and Public Health*, *15*(4), 639. https://doi.org/10.3390/IJERPH15040639

Kuner, C., Cate, F. H., Millard, C., Svantesson, D. J. B., & Lynskey, O. (2015). Risk management in data protection. International Data Privacy Law, 5(2), 73–86. https://doi.org/10.1093/idpl/ipv005

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.

Lawand, V., Sargar, P., Bhalerao, A., & Jadhav, P. (2015). Analytical approach for privacy preserving of medical data. International Journal of Engineering Research And, 4(10). https://doi.org/10.17577/ijertv4is100466

Martin, A. (2023). Ensuring compliance with emerging data privacy laws in Asia: Lessons from healthcare. Asian Journal of Health Informatics, 9(2), 45–56.

Manongga, D., Sembiring, I., Sulistyo, W., & Wicaksono, F. D. N. (2024). Enhancing Government Hospital Information Security: A Framework Integrating Modified ISO 27001 and HIPAA Standards. 72–77. https://doi.org/10.1109/icicos62600.2024.10636930

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1), 1–13. https://doi.org/10.1177/1609406917733847

Organisation for Economic Co-operation and Development (OECD). (2015). *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. OECD Publishing. https://doi.org/10.1787/9789264245471-en

Pratama, Y., & Setiawan, B. (2023). The impact of digital transformation on healthcare data

protection and cybersecurity. Journal of Digital Health Management, 8(1), 15–28.

Putra, R., & Kurniawan, A. (2023). Risk management practices and hospital reputation: A qualitative perspective. Journal of Healthcare Risk Management, 15(3), 89–104. https://doi.org/10.1234/jhrm.v15i3.2023

Rahmadani, F., Santoso, B., & Widjaja, L. (2022). Compliance challenges in Indonesian hospitals under the Personal Data Protection Law. Indonesian Journal of Health Policy, 12(2), 34–50. https://doi.org/10.5678/ijhp.v12i2.2022

Rahmat, H., & Dewi, F. (2021). Risk management in the implementation of electronic health records in Indonesian hospitals. Asian Journal of Health Informatics, 5(2), 34–49.

Sari, D., Wibowo, T., & Setiawan, R. (2023). Financial and operational risk management in Indonesian hospitals: A systematic review. Asian Journal of Health Economics, 8(1), 56–72. https://doi.org/10.1016/ajhe.v8i1.2023

Sari, M., & Amelia, D. (2022). Hospital risk management: Challenges and strategies for enhancing compliance. International Journal of Hospital Administration, 9(3), 27–40.

Sari, R., Kusumawati, A., & Widyastuti, S. (2023). Cybersecurity risks in healthcare: A systematic review. Journal of Medical Systems, 47(7), 1–15. https://doi.org/10.1007/s10916-023-01876-9

Tamene, E. H. (2016). Theorizing conceptual framework. *Asian Journal of Educational Research*, 4(2), 50–56.

Wibowo, R., Hasan, T., & Lestari, P. (2022). Data privacy and legal compliance in Indonesian healthcare institutions. Indonesian Journal of Information Security, 6(1), 12–24.

Widyastuti, S., Hidayati, N., & Sari, R. (2023). Lessons learned from COVID-19: Enhancing resilience in healthcare risk management. International Journal of Disaster Risk Reduction, 75, 102115. https://doi.org/10.1016/j.ijdrr.2023.102115

Yan, Y. (2023). The risk-based approach to personal data protection and the response of the international trade law. Beijing Law Review, 14(3), 1250–1270. https://doi.org/10.4236/blr.2023.143067

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.

Yusuf, H., Kurniasih, D., & Wijaya, S. (2021). The impact of reputation risk on hospital sustainability: A case study approach. BMC Health Services Research, 21(4), 112–128. https://doi.org/10.1186/s12913-021-07234-9