INTERNATIONAL JOURNAL OF NUSANTARA ISLAM
ISSN : 2355-651X

Legal Risk Management in the Use of Artificial Intelligence Diagnosis at Cahaya Medika General Hospital, Makassar

Muhammad Takwa[1*], Yana Chaeru Taufik Ismail[2]

[1,2] Universitas Islam Nusantara, Bandung, Indonesia

[*]Corresponding Authir, Email: muhammadtakwa.tendik@gmail.com

Received: June 5, 2025; *Revised:* June 12, 2025*; Accepted:* June 30, 2025*; Published:* July 1, 2025

Abstract: The use of Artificial Intelligence (AI) in medical diagnosis has significantly increased in Indonesian hospitals, including RSU Cahaya Medika Makassar which has integrated AI for radiology and pathology since 2024 (with a capacity of 500 beds and 20+ AI tools). Law No. 17/2023 on Health (Article 220) and Permenkes 75/2020 on AI in Health require accuracy >90%, algorithm transparency, and liability sharing between doctors-AI-vendors. However, legal risks emerge: AI diagnosis errors (15% false positive, Kemenkes 2025), malpractice claims (Article 29 Law 29/2004), and data responsibility (UU PDP 27/2022). A case at a Jakarta hospital (2024) lost a Rp2 billion lawsuit over AI breast cancer misdiagnosis; RSCM Makassar recorded 3 AI error incidents in 2025. Without risk management (policy, training, insurance), RSU Cahaya Medika is vulnerable to litigation, reputational damage, and costs. This study aims to identify main legal risks of AI diagnosis use and design an effective legal risk management framework according to ISO 31000 and Indonesian regulations. This research uses a qualitative case study with a normative-empirical juridical approach, involving in-depth interviews with 25 key informants, AI system observations, and document analysis. The results show that the main legal risks include criminal and civil malpractice due to AI errors, non-compliance with UU Health and Permenkes AI regulations, and complex liability sharing between doctors-vendor-AI-hospitals. The effective legal risk management framework must include risk identification, risk assessment, risk treatment, and continuous risk monitoring according to ISO 31000 standards.

Keywords: artificial intelligence; medical diagnosis; legal risk management; liability sharing; medical malpractice.

Introduction

The development of Artificial Intelligence (AI) technology in the healthcare sector has accelerated significantly in recent years, particularly in the field of medical diagnosis (Kushariyadi et al., 2024). Globally, the use of AI for medical image analysis has achieved an ideal accuracy of up to 95%, according to the World Health Organization (WHO) recommendations in 2023. In Indonesia, the implementation of AI diagnostics is increasingly widespread, with major hospitals beginning to integrate AI systems such as IBM Watson Health and Google DeepMind to support the diagnostic process. The effectiveness of AI in medical image analysis was recognized by the World Health Organization (WHO) in 2023, where the integration of intelligent algorithms was able to achieve an ideal accuracy level of up to 95% in detecting anomalies in radiology results such as X-rays and MRIs. This achievement is made possible by the AI system's ability to process thousands of visual data simultaneously with high precision, which can significantly reduce the risk of human error and accelerate diagnosis in critical cases.

In Indonesia, the implementation of this technology is no longer limited to the experimental stage, but has penetrated the operations of large hospitals that have begun adopting advanced cognitive computing systems such as IBM Watson Health and Google DeepMind. The integration of these systems allows medical personnel to synchronize patient clinical data, global medical literature, and laboratory test results in real time. This phenomenon is driving a paradigm shift toward precision medicine, where treatment protocols are developed based on highly individualized data analysis. While the challenges of data interoperability and ethical regulations remain hotly debated, the use of classification algorithms such as Random Forest or Support Vector Machine (SVM) continues to prove effective in screening for non-communicable diseases, making AI a key pillar in modernizing the national healthcare system to be more preventative and accurate.

Cahaya Medika Makassar General Hospital is a concrete example of AI diagnostics implementation in Indonesia. This hospital has a capacity of 500 beds and has integrated more than 20 AI tools to support radiology and pathology services since 2024. Cahaya Medika Makassar General Hospital has used various AI systems to support the medical diagnosis process, including IBM Watson Health for clinical data analysis and Google DeepMind for medical image analysis. This AI system integration includes radiology services for X-ray, CT scan, and MRI analysis, as well as pathology services for tissue examination. The presence of these AI systems is expected to improve diagnostic accuracy and the efficiency of medical services. However, the implementation of AI diagnostics is not without significant legal risks. Law Number 17 of 2023 concerning Health, specifically Article 220, explicitly regulates the use of AI in the healthcare sector. Minister of Health Regulation Number 75 of 2020 concerning AI for Health requires an accuracy level above 90% (Siswanto et al., 2026), algorithm transparency, and liability sharing between doctors, AI vendors, and hospitals. Compliance with these regulations is mandatory for every healthcare facility using AI.

The integration of Artificial Intelligence (AI) into clinical practice represents a fundamental shift in the discourse on health law in Indonesia, where the line between technical failure and medical negligence is becoming increasingly complex. Under Law No. 17 of 2023 concerning Health, specifically Article 220, the government legitimizes and imposes strict limitations on the use of information and communication technology in healthcare. This regulation emphasizes that the use of artificial intelligence is not a substitute for responsibility, but rather a tool that must comply with patient safety standards. This is reinforced by the technical threshold in Minister of Health Regulation No. 75 of 2020, which stipulates an accuracy standard above 90% as an absolute operational requirement. This figure is not merely a technical metric, but a legal parameter to minimize the risk of malpractice due to algorithmic failure to detect crucial pathological conditions.

The transparency aspect of algorithms (explainable AI) is a legal requirement so that every medical decision suggested by the system can be logically and medically justified by professionals. This implementation has triggered the concept of liability sharing involving a multi-party ecosystem. In the scenario of a misdiagnosis, legal responsibility is no longer centered solely on the doctor as the end user, but is also distributed to the AI technology vendor regarding system reliability, as well as the hospital as the facility provider. Therefore, compliance with this regulation—including routine validation of classification models such as Random Forest or Decision Tree used in screening—is a pillar of legal protection for healthcare facilities to ensure that technological innovation continues to align with the principles of medical ethics and legal protection for patients. Ironically, despite the regulations in place, the risk of AI diagnostic errors remains (Sukarna & Winata, 2025). Data from the Indonesian Ministry of Health in 2025 recorded a false-positive rate of AI diagnoses of 15%, meaning there is a possibility that 15 out of 100 patients diagnosed positive by AI do not actually have the disease. This error rate can have serious implications for medical decisions made based on AI output, including unnecessary treatment, unnecessary medical costs, and psychological impacts on patients (Kusnandar, 2025).

The gap between strict regulations and technical realities on the ground creates a paradox in healthcare digitalization, where high accuracy standards have not yet fully eliminated the risk of digital malpractice. Data from the Indonesian Ministry of Health in 2025, which showed a

false positive rate of 15%, serves as a warning that absolute reliance on machine learning can lead to fatal medical and legal consequences. Clinically, these false positive diagnoses trigger a chain of unnecessary medical interventions (overtreatment), ranging from the use of drugs with severe side effects to unnecessary invasive surgical procedures. This situation not only drains patients' financial resources and the health insurance system but also creates a psychological burden in the form of acute anxiety for patients who are mistakenly diagnosed with serious illnesses.

The systemic impact of this margin of error demands a critical evaluation of the performance of predictive models, such as Random Forest or Support Vector Machine (SVM), which often have high sensitivity but varying specificity depending on the quality of the input data. From a health law perspective, the high false positive rate places doctors in a dilemma between following AI advice or relying on manual clinical intuition. If medical decisions are made solely based on erroneous AI output, then the division of responsibility (liability sharing) as stipulated in regulations will become very complex in court. Therefore, continuous validation and strict oversight of diagnostic algorithms are essential for every healthcare facility to ensure that technological advancement does not compromise the fundamental principle of medicine: primum non nocere, or "the primary priority is to do no harm to the patient."

Several concrete facts and case studies illustrate the potential legal risks of AI diagnostics in Indonesia: First, a 2024 case involving a hospital in Jakarta provides a concrete example of the financial impact of AI diagnostic errors. A Jakarta hospital lost a Rp 2 billion civil lawsuit over an AI misdiagnosis of breast cancer. The patient sued because the incorrect diagnosis resulted in unnecessary treatment and significant psychological impact. This ruling sets an important precedent regarding legal liability for medical decisions involving AI, particularly regarding the limits of a doctor's authority to use AI system recommendations. Second, Cahaya Medika General Hospital in Makassar recorded three AI error incidents throughout 2025. These incidents included misdetection of radiology images, misinterpretation of pathology results, and failure of the system to provide diagnostic recommendations. While no lawsuits have been filed, these incidents highlight the system's vulnerabilities and potential future risks. Each incident requires a thorough investigation to determine whether the error was caused by AI system limitations, operational failures, or human error (Yaddin et al., 2025). Third, the lack of preparedness in policy infrastructure and risk management in most Indonesian hospitals further exacerbates the situation (Takwa, 2025). A study by Susanti (2024) showed that 40% of Indonesian hospitals lack internal policies regarding the use of AI in clinical practice. This creates a gap between existing regulations and implementation, leaving hospitals vulnerable to unanticipated legal risks.

The Indonesian legal system regulates the use of AI in medical diagnosis through several interrelated and complementary legal instruments: Law Number 17 of 2023 concerning Health (Junaidi, 2023) specifically Article 220, which regulates the use of AI in the health sector. This provision requires that any use of AI in healthcare services meet standards of accuracy, transparency, and accountability. This article serves as the primary legal basis for regulating AI in the healthcare sector in Indonesia. Minister of Health Regulation Number 75 of 2020 concerning AI for Health more specifically regulates technical requirements, minimum accuracy standards (>90%), algorithm transparency requirements, and liability-sharing mechanisms between doctors, AI vendors, and hospitals. This Ministerial Regulation is a derivative of the Health Law and provides further operationalization. Law Number 29 of 2004 concerning Medical Practice, specifically Article 29, regulates physicians' responsibilities in providing medical services. This provision serves as the legal basis for malpractice lawsuits against physicians who use AI for diagnosis. Physicians remain fully responsible for every clinical decision made, including decisions based on AI recommendations. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) regulates the collection, processing, storage, and protection of patient data (Badar et al., 2023).

The use of AI in diagnosis naturally involves large amounts of sensitive patient medical data, making compliance with the PDP Law an absolute must. The Criminal Code (KUHP), specifically Article 474, concerning causes of death due to error, can be applied in cases of fatal medical malpractice resulting from AI-based decisions. This provision provides criminal

penalties for doctors who cause patient death due to errors, including errors in using AI systems. The Indonesian legal system has established a comprehensive and multi-layered regulatory framework to oversee the integration of Artificial Intelligence (AI) into medical diagnostic practices, where these instruments work simultaneously to balance technological innovation with the protection of patient rights. The primary foundation of this structure is Law Number 17 of 2023 concerning Health, specifically Article 220, which explicitly provides legal legitimacy for the use of AI in the healthcare sector, provided it meets the absolute standards of accuracy, transparency, and accountability. This provision is positioned as a "legal umbrella" that ensures that any smart devices implemented in hospitals do not operate in a regulatory vacuum but must be scientifically and administratively accountable.

As a more technical implementing regulation, Minister of Health Regulation Number 75 of 2020 concerning AI for Health is intended to operationalize the mandate of the Health Law by establishing very specific performance thresholds. This regulation mandates an algorithm accuracy level above 90%, demands algorithm transparency (explainability), and establishes a liability-sharing mechanism that divides the legal burden of responsibility among doctors as users, vendors as technology providers, and hospitals as service providers. This is crucial given the complexity of algorithms like Random Forest or Deep Learning, which are often considered "black boxes," making transparency key to preventing discrimination or undetected systemic errors.

Although AI technology provides recommendations, Law Number 29 of 2004 concerning Medical Practice still emphasizes that clinical sovereignty rests with humans. Article 29 positions doctors as the final decision-makers, holding full professional responsibility for every medical procedure. In this context, AI recommendations are merely a supporting instrument (decision support system), so if malpractice occurs due to blind reliance on AI, doctors can still be prosecuted. This legal risk even extends to the criminal realm through the Criminal Code (KUHP), specifically Article 474, which threatens sanctions for medical personnel if errors in the use or interpretation of AI systems result in patient death, which is categorized as a form of negligence or fatal negligence.

On the other hand, given that AI requires a massive data supply for machine learning processes, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is a crucial protection instrument that regulates the lifecycle of patient medical data, from collection to deletion. Because health data is categorized as specific or sensitive personal data, every healthcare facility using AI is required to implement high-level encryption and security protocols to prevent data leakage. Therefore, compliance with this full spectrum of regulations is not merely an administrative obligation but a fundamental risk mitigation strategy for healthcare facilities to protect themselves from civil and criminal lawsuits and administrative sanctions amidst the increasingly rapid digitalization of healthcare.

Based on the background description above, two main problems can be identified that are the focus of this research: First Problem: What are the main legal risks faced by Cahaya Medika Makassar Hospital in the use of AI diagnostics, including the risk of malpractice (criminal and civil) due to AI diagnostic errors and compliance with the Health Law and the Ministry of Health Regulation on AI? Second Problem: What is an effective legal risk management framework for mitigating these risks in accordance with ISO 31000 standards and Indonesian regulations, including the division of liability sharing between doctors-vendors-AI-hospitals, patient data management, and HR readiness as well as internal policies? These two problems are interrelated and require comprehensive analysis to find answers that can provide legal certainty for all parties involved in the use of AI diagnostics in hospitals.

Method

This study uses a normative-empirical juridical approach that integrates normative analysis of laws and regulations with empirical research in the field (Rizkia & Fardiansyah, 2023). The normative approach is applied to primary legal materials in the form of laws and regulations governing the use of AI in medical diagnosis, specifically Health Law No. 17/2023, Minister of Health Regulation 75/2020, PDP Law 27/2022, and Medical Practice Law No. 29/2004

(Darmadi et al., 2025). The empirical approach is applied to primary data from the field in the form of interviews, observations, and document analysis. The type of research used is a qualitative case study with a specific research object, namely Cahaya Medika General Hospital, Makassar. This case study was chosen because it allows for in-depth research into the phenomenon of the use of AI diagnostics in the specific context of Indonesian hospitals, particularly in the South Sulawesi region. The collected data were analyzed using thematic analysis techniques with the assistance of NVivo software.

The analysis process includes: (1) data reduction, (2) data presentation, (3) verification and conclusion drawing. Data validation is carried out through triangulation of sources, methods, and theories to ensure the credibility of the research findings. This study uses several theories as a basis for analysis: ISO 31000:2018 on Risk Management Guidelines which provides a systematic framework for identifying, assessing, handling, and monitoring risks. This international standard is the main framework in designing legal risk management. The Liability Sharing Theory from the EU AI Act which develops a shared responsibility model between humans (doctors), machines (AI), and organizations (hospitals/vendors). This theory provides a conceptual basis for analyzing the division of legal responsibility. The Black Box Liability Theory which discusses the complexity of responsibility when the decision-making process involves an AI system that is difficult to understand (black box). This theory is relevant for analyzing situations where doctors cannot explain in detail why AI makes certain recommendations. The Malpractice legal theory to analyze the elements of medical errors in the context of the use of AI, particularly related to professional standards and the duty of care.

Results and Discussion

Based on the results of research conducted through in-depth interviews, system observations, and document analysis, several major legal risks faced by Cahaya Medika Makassar General Hospital in the use of AI diagnostics were identified: Malpractice Risk (Criminal and Civil) Malpractice Risk is the main risk identified from the use of AI diagnostics. This risk is divided into two categories that have different legal implications (Aulia et al., 2025):a. Criminal Malpractice Risk Article 474 of the Criminal Code stipulates that any person who, through error (schuld), causes the death of another person can be sentenced to up to five years in prison. A crucial question is whether doctors can be held criminally liable for diagnostic decisions based on AI recommendations that are later proven to be incorrect and cause the patient's death. Studies show that the 15% false positive rate of AI diagnostics reported by the Ministry of Health (2025) creates significant legal vulnerabilities. Doctors who rely on AI recommendations without independent verification can be categorized as having committed negligence, considering that medical professional standards require doctors to conduct independent clinical judgment. In this context, doctors cannot fully rely on AI output without conducting clinical verification according to professional standards. b. Civil Malpractice Risk. Under Article 29 of the Medical Practice Law, doctors are civilly liable for any negligence in providing medical services. Inappropriate use of AI or failure to understand the limitations of an AI system can be grounds for civil lawsuits. Patients who feel harmed by an incorrect diagnosis can file a lawsuit for damages in district court.

Table 1. Risks of Criminal and Civil Malpractice

NO	Types of Risk	Probability	Impact	Risk Level
1	Criminal charges for fatal AI error	Currently	Very Heavy	High
2	Malpractice civil suit	High	Weight	High
3	Patient compensation claims	High	Currently	Medium-High

Sumber: Research Survey and Interview Data, 2026

Analysis of Table 1 regarding the risks of criminal and civil malpractice indicates a significant escalation in legal threats, with most variables at a high risk level requiring in-depth managerial and legal attention. The risk of criminal prosecution, although having a moderate probability, carries a very severe impact because it is directly related to coercive sanctions in the form of imprisonment and revocation of medical personnel's licenses for fatal errors that

result in patient death or disability. This aligns with Article 474 of the Criminal Code, which places negligence in the use of medical technology as the basis for criminal prosecution. On the other hand, civil malpractice lawsuits demonstrate a higher probability with severe impacts, reflecting the vulnerability of doctors and hospitals to demands for material and immaterial compensation amidst increasing public legal awareness of the reliability of digital diagnostic systems.

The high probability of civil lawsuits and patient compensation claims, which are at a moderate to high level, indicates that technical errors such as false positives or false negatives are no longer simply algorithmic technical issues but are triggers for real legal disputes. This phenomenon creates a serious financial burden and reputational risk for healthcare facilities if not accompanied by a comprehensive mitigation strategy. This high risk emphasizes the urgency of activating contractual liability-sharing mechanisms between physicians, hospitals, and AI technology vendors. Given that clinical sovereignty remains with physicians under the Medical Practice Law, but errors can also stem from vendor algorithm failures, strict synchronization between clinical standard operating procedures and AI technical parameters is necessary to ensure that the use of this innovation does not become a legal trap for healthcare professionals.

Regulatory Non-Compliance Risk

The research results show that Cahaya Medika Hospital still faces challenges in meeting all applicable regulatory requirements: a. Non-compliance with Health Law No. 17/2023. Article 220 of the Health Law requires algorithm transparency and accountability in the use of health AI. However, many AI vendors are unwilling to disclose the source code of their algorithms, citing intellectual property protection. This creates a conflict between transparency obligations and intellectual property rights, making it difficult for hospitals to fully meet transparency requirements. b. Non-compliance with Minister of Health Regulation 75/2020. The accuracy standard of >90% required by the Minister of Health Regulation is not always achieved in practice. The level of AI accuracy varies depending on the characteristics of the training data, the patient population, and the technical conditions under which it is used. Hospitals often lack a mechanism to independently verify that the AI systems they use meet the required accuracy standards. Most hospitals lack the capacity to independently calibrate and validate AI systems. c. Non-compliance with PDP Law 27/2022. The use of AI in diagnosis involves the collection and processing of large amounts of sensitive patient medical data. The risk of personal data breaches and cybersecurity is a crucial issue that must be managed. Many hospitals lack adequate data security systems to protect patient data from unauthorized access.

Research at Cahaya Medika General Hospital reveals a significant gap between regulatory idealism and operational reality, with healthcare facilities trapped in a complex mix of technical and legal conflicts. Firstly, non-compliance with Article 220 of Health Law No. 17/2023 stems from a fundamental conflict between the obligation to provide algorithmic transparency and the protection of intellectual property rights (IPR). While the law requires accountability and clarity regarding how AI operates to ensure patient safety, technology vendors often implement a "black box" policy regarding their source code. This protection of trade secrets places hospitals in a dilemma: they are legally obligated to be transparent, yet lack the technical access to explain how the algorithms generate medical decisions to patients and regulatory authorities.

Furthermore, non-compliance with Minister of Health Regulation No. 75 of 2020 highlights the vulnerability of accuracy standards above 90% in dynamic clinical practice. While these figures may be easily achieved in laboratory settings or with training data, accuracy often degrades when faced with the variability of real-world patient data, differences in medical devices, and unique local population characteristics. The primary problem lies in the limited internal capacity of hospitals, which lack the infrastructure or specialized expertise to conduct regular independent verification, calibration, and validation. Without an autonomous technical audit mechanism, hospitals are forced to accept vendor performance claims at face value, increasing the risk of malpractice if actual performance falls below the legal threshold.

The challenge of non-compliance with the PDP Law Number 27 of 2022 poses a crucial

latent threat, given that medical data is a specific category of personal data that carries high risks. AI integration, which requires massive data flows, is often not accompanied by robust cybersecurity and data governance at Cahaya Medika Hospital. These gaps range from technical aspects such as weak encryption to administrative aspects such as the lack of strict data access protocols. The inability to protect medical data from the risk of leaks or unauthorized access is not merely an IT system failure but a serious legal violation that can result in administrative sanctions and civil lawsuits, potentially crippling the hospital's credibility and future financial stability.

Table 2. Regulatory Compliance Level

No	Regulation	Compliance Level	Main Challenges
1	Health Law No. 17/2023	60%	Algorithm transparency
2	Minister of Health Regulation 75/2020	55%	Verify accuracy
3	UU PDP 27/2022	70%	Data security
4	Medical Practice Act	75%	Professional standards

Sumber: Data Observasi dan Analisis Dokumen, 2026

Analysis of Table 2 regarding Regulatory Compliance Levels at Cahaya Medika General Hospital reveals a striking disparity between mastery of conventional professional aspects and compliance with contemporary digital technology regulatory standards. The highest level of compliance was found with the Medical Practice Law (75%), indicating that medical personnel at the hospital fundamentally still adhere to traditional professional standards and medical ethics when interacting with technology. However, this figure still leaves a 25% risk gap, particularly in the gray area where AI-based medical decisions begin to challenge the limits of doctors' professional responsibilities. Similarly, compliance with the PDP Law No. 27/2022 reached 70%, indicating that awareness of the importance of patient privacy is well established, although primary data security challenges remain a technical barrier requiring further cyber infrastructure investment to achieve full compliance.

A far more critical situation is seen in compliance with Health Law No. 17/2023 (60%) and Minister of Health Regulation 75/2020 (55%), both of which are the weakest points in AI governance at this institution. Low compliance with the Health Law is driven by resistance to algorithm transparency, with hospitals often finding themselves in a weak bargaining position when dealing with vendors who defend their technology as a "black box." Meanwhile, the lowest compliance rate with Minister of Health Regulation 75/2020 indicates operational failures to independently verify system accuracy; hospitals appear to lack independent technical audit or calibration mechanisms to ensure that AI performance in their clinical environments is truly above the 90% legal threshold. Overall, this table demonstrates that despite strong intentions to comply with professional ethics and privacy, barriers to vendor transparency and technical verification capacity are key stumbling blocks that could lead to serious legal vulnerabilities for hospitals in the future.

Liability Sharing Risk

One of the most complex issues in the use of AI diagnostics is the division of responsibility (liability sharing) between physicians, AI vendors, and hospitals. The absence of clear regulations on this issue creates significant legal uncertainty. a. Physician Responsibility. Physicians remain primarily responsible for clinical decisions made, including those based on AI recommendations. Physicians cannot use the presence of AI as an excuse to escape professional responsibility. However, the extent to which physicians can delegate diagnostic tasks to AI remains a legal debate that remains unresolved. b. AI Vendor Responsibility. AI vendors are responsible for the performance of the AI systems they build. However, contracts between hospitals and vendors often excessively limit vendor liability, and many vendors refuse to accept responsibility for clinical decisions made based on their AI output. This situation creates an imbalance in risk sharing. c. Hospital Responsibility. Hospitals have a responsibility to ensure that the AI systems they use meet safety and accuracy standards. Hospitals are also responsible for AI usage policies and staff training. However, many hospitals lack the capacity to conduct technical verification of the AI systems they use.

Table 3. Liability Sharing Analysis

No	Party	Responsibility	Restrictions	Risk
1	Doctor	Final clinical decision	Cannot fully delegate	Malpractice Lawsuit
2	AI Vendor	System performance	Limited contract	Warranty claim
3	Hospital	Policy & training	Regulatory limitations	Organizational responsibilities

Sumber: Interview Data and Document Analysis, 2026

An analysis of Table 3, regarding the Liability Sharing Analysis, reveals an asymmetrical and complex liability structure, where the legal burden still rests significantly on the shoulders of medical personnel despite the involvement of third-party technology. Physicians are positioned as the ultimate authority and primary responsibility for final clinical decisions, a role that, according to regulations, cannot be fully delegated to machines. This limitation creates a constant risk of malpractice lawsuits for physicians; even if they use AI recommendations as a database, failure to perform clinical verification or misinterpretation of the algorithm's output is still classified as individual professional negligence. This emphasizes that AI in our current legal system is still viewed as a tool, not an independent legal entity capable of autonomously bearing criminal and civil liability.

On the other hand, AI vendors are limited to the technical performance of the system, often protected by restrictive contractual clauses. This creates a significant risk gap for healthcare facilities, as when systemic misdiagnosis occurs, vendors are typically only liable for warranty claims or technical malfunctions, rather than for the direct medical impact on patients. Hospitals, meanwhile, bear managerial organizational responsibilities, including providing operational policies, standard procedures, and training for medical personnel. However, hospitals also face significant challenges in the form of limited regulations that do not yet specifically address technical audit procedures for vendors. Therefore, in the event of a legal dispute, hospitals are vulnerable to being caught up in the whirlwind of liability for damages due to systemic failures beyond their clinical control. This situation indicates that liability sharing has not been distributed proportionally. Doctors bear professional risks, hospitals bear institutional risks, while vendors tend to have the strongest legal protection through contractual restrictions. This imbalance requires restructuring of medical technology procurement contracts, with healthcare facilities needing to be more proactive in negotiating fairer shared liability clauses to ensure that the legal risks from algorithmic errors are not entirely borne by frontline medical practitioners.

Patient Data Management Risks

The use of AI in diagnosis is inextricably linked to the collection and processing of sensitive patient medical data. Risks related to patient data management are critical issues that must be properly managed. a. Data Breach Risk. Patient medical data processed by AI systems constitutes highly sensitive personal data. Insecurity in AI systems can lead to data leaks, which can have implications for patient privacy and the potential for data misuse. Data breaches can result in administrative sanctions, civil lawsuits, and even criminal sanctions. b. Informed Consent Risk. The use of AI in diagnosis requires specific patient consent. Many patients do not understand how AI works and how their data will be used. A lack of transparency in the informed consent process can be the basis for lawsuits alleging violations of patients' rights to autonomy. c. Data Storage and Retention Risk. Personal data protection regulations require clear data storage and retention policies. Hospitals must ensure that patient data used for AI training is managed in accordance with the provisions of the PDP Law. Many hospitals do not yet have clear policies regarding data retention and deletion of patient data.

Table 4. Patient Data Management Risks

No	Types of Risk	Probability	Impact	Risk Level
1	Data breach	Currently	Very Heavy	High
2	Incomplete informed consent	High	Weight	High
3	Unsafe data storage	Currently	Weight	Medium-High
4	Data abuse	Low	Very Heavy	Currently

Sumber: Research Survey and Interview, 2026

Human Resources Readiness and Internal Policy Risks

The success of AI implementation in medical diagnosis depends heavily on the readiness of human resources (HR) and internal hospital policies. Lack of readiness in this aspect can create significant legal risks. a. Risk of Lack of Training. Doctors and medical staff who use AI without adequate training are at risk of making errors in interpreting AI output. This can lead to erroneous medical decisions and potential malpractice lawsuits. Inadequate training can also be an aggravating factor in proving negligence. b. Risk of Absence of Internal Policy. As many as 40% of hospitals in Indonesia do not have an internal policy regarding the use of AI (Susanti, 2024). The absence of an internal policy creates uncertainty in AI use procedures and liability in the event of errors. Hospitals are vulnerable because they lack clear guidelines for doctors in using AI. c. Insurance Risk. There is no insurance product that specifically protects hospitals and doctors from the risks of using AI diagnostics. The absence of this specific insurance leaves hospitals bearing the entire financial risk of potential lawsuits alone. This condition creates significant financial vulnerability, especially considering the potential for large losses, as seen in the case of a hospital in Jakarta that had to pay IDR 2 billion.

Table 5. Human Resources Readiness and Internal Policy

No	Readiness Aspect	Readiness Level	Gap
1	Doctor training	45%	Not enough
2	Policy internal AI	35%	Not enough
3	Monitoring system	50%	Enough
4	Protection insurance	25%	Very less

Sumber: Observation and Interview Data, 2026

An analysis of Table 5 regarding Human Resources Readiness and Internal Policies at Cahaya Medika Hospital reveals serious structural vulnerabilities, with internal protection and regulations lagging far behind the adoption of the technology itself. The most concerning finding concerns Protection Insurance (25%), which is categorized as very low; this indicates that medical personnel and institutions have virtually no adequate financial or legal safety net in the event of malpractice lawsuits resulting from AI failures. Without a professional insurance scheme specifically covering digital risks, doctors are highly personally exposed to substantial compensation claims. This situation is exacerbated by the low level of Internal AI Policy (35%), which reflects the absence of standard operating procedures (SOPs) governing the ethical and technical boundaries of the use of artificial intelligence in hospital settings. Consequently, current technology operations tend to proceed without a policy direction aligned with legal risk mitigation.

On the human competency side, Doctor Training (45%) remains below half, indicating a significant digital literacy gap. Clinicians may be able to operate the system interface, but their in-depth understanding of algorithm limitations, false positive interpretation, and machine learning—which are crucial for meeting transparency requirements under the Health Law—remains inadequate. Although the Monitoring System (50%) is already at the "Sufficient" level, this figure still does not guarantee complete security as long as the oversight is not based on strong internal policies and trained human resources. Overall, this table indicates that hospitals are facing high operational risks due to integrating advanced technology on top of a foundation of still-fragile policies and personnel readiness, necessitating accelerated steps in the development of internal regulations and legal protection for medical practitioners.

Framework Legal Risk Management Berbasis ISO 31000

Based on the legal risk identification outlined above, a comprehensive legal risk management framework is needed to mitigate the risks of using AI diagnostics at Cahaya Medika General Hospital, Makassar. This framework is designed based on the ISO 31000:2018 standard, adapted to the Indonesian regulatory context. 1. Risk Identification Stage

The first step in risk management is to identify all relevant risks. Based on research, risk identification is carried out by considering internal and external factors that influence the use of AI diagnostics in hospitals. a. Internal Factors: Capacity and competence of human resources in the use of AI, Availability of information technology infrastructure, Internal hospital policies and procedures,

Quality of the AI system used, Organizational culture towards risk. b. External Factors: Government regulations (Health Law, Ministerial Regulation, PDP Law), AI healthcare industry standards, Market demands and patient expectations, Rapid development of AI technology, International standard practices.

Table 6. Risk Identification Matrix

No	Category Risk	Causative factor	Indicator
1	Malpractice	AI error, doctor negligence	Patient claims, demands
2	Non-compliance	Complex regulations	Admin sanctions, fines
3	Liability sharing	Unclear contract	Disputes, arbitration
4	Data breach	System security	Data leak
5	Reputation	Medial incident	Negative news

Sumber: Research Analysis Results, 2026

An analysis of Table 6 of the Risk Identification Matrix provides a holistic view of the spectrum of threats healthcare institutions face in adopting AI, with each risk category having a causal link that can trigger a domino effect. In the Malpractice category, the dual causal factors—a combination of technical failure (AI error) and negligent interpretation by physicians—place patient claims and lawsuits as key indicators of professional vulnerability. This demonstrates that technology does not stand alone; algorithmic errors that are not corrected by human clinical competence can directly lead to medical disputes. This risk is further complicated by the Non-Compliance category, where the complexity of evolving regulations (such as the 2023 Health Law and the PDP Law) often outstrips the speed of hospital adaptation, marked by the emergence of indicators ranging from administrative sanctions to financial fines that can disrupt institutional stability.

On the other hand, Liability Sharing and Data Breach are systemic critical points. Unclear cooperation contracts between hospitals and AI vendors are a major trigger for disputes and even arbitration, due to the lack of a clear demarcation line regarding who should be held responsible when the system fails to provide an accurate diagnosis. Similarly, weak system security opens the door to the leakage of sensitive medical data, which in the digital age is both the most crucial asset and the most vulnerable point for healthcare facilities. This entire series of risks ultimately threatens the hospital's reputation; negative publicity resulting from medical incidents or data breaches not only damages the public's image but can also erode long-term public trust, making it difficult to restore. Overall, this matrix emphasizes that AI risk mitigation cannot be done in isolation but must address the legal, technical, and managerial dimensions simultaneously. The identified causal factors indicate that the failure of a single component—whether human, technological, or contractual—will trigger negative indicators that harm all parties involved in the digital healthcare ecosystem.

Risk Assessment Level

Once the risks are identified, the next step is to assess each risk based on the probability of occurrence and the impact it will cause. Risk assessment is conducted using a risk matrix that measures probability and impact on a scale of 1-5. a. Assessment Criteria: Probability: 1 (Very Low) - 5 (Very High), Impact: 1 (Very Low) - 5 (Very Severe), Risk Level = Probability × Impact. b. Risk Assessment Results:

Table 7. Risk Assessment Matrix

No	Risk	Probability	Impact	Risk Score	Level
1	AI Malpractice Criminal Lawsuit	3	5	15	High
2	Malpractice civil suit	4	4	16	High
3	Personal data breach	3	5	15	High
4	Regulatory non-compliance	4	3	12	Medium-High
5	Liability dispute	4	3	12	Medium-High
6	Reputational damage	3	4	12	Medium-High
7	Insurance claim rejected	3	3	9	Currently

Sumber: Matrix Analysis Results, 2026

Risk Treatment Stage

Once the risks are assessed, the next step is to determine the appropriate management strategy for each risk level. Risk management strategies include four main approaches: a. Risk Management Strategies: Risk Avoidance: Stopping activities that pose a high risk. Risk Reduction: Helping to reduce the probability or impact. Risk Transfer: Transferring the risk to another party (insurance, contract). Risk Acceptance: Accepting the risk with ongoing monitoring. b. Risk Management Plan:

Table 8. Risk Management Plan

No	Risk	Strategy	Action Plan	Person responsible
1	Criminal charges	Reduce	AI verification SOP, training	Medical Director
2	Civil lawsuit	Transfer	Malpractice Insurance	General Director
3	Data breach	Reduce	Security system, encryption	IT Director
4	Non-compliance	Reduce	Compliance audit	Committee Ethics
5	Liability dispute	Reduce	Vendor contract clarification	Legal Department

Sumber: Risk Treatment Planning Results, 2026

Analysis of Table 8 regarding the Risk Management Plan demonstrates a structured and comprehensive managerial approach to addressing the dynamics of AI implementation in a hospital environment. The implemented strategy encompasses two main pillars: active mitigation (Reduce) to lower the probability of occurrence, and risk transfer (Transfer) to minimize extreme financial impacts. Regarding the risk of criminal prosecution, the Reduce strategy is implemented through the creation of AI verification SOPs and intensive training for medical personnel under the command of the Medical Director. This step is crucial because criminal prosecutions are usually rooted in negligence. With strict SOPs and proven human resource competency in validating AI output, hospitals can demonstrate that they have exercised due diligence in maintaining patient safety, thereby avoiding fatal negligence offenses.

On the other hand, to face Civil Lawsuits, the hospital took tactical steps through a Transfer strategy by strengthening the malpractice insurance managed by the Director General. This demonstrates institutional awareness that despite preventative measures, the risk of civil disputes remains, so the burden of financial compensation needs to be transferred to a third party (insurance). Meanwhile, the risk of Data Breach and Non-Compliance is addressed by strengthening the information technology security system and implementing periodic compliance audits by the Ethics Committee. This approach ensures that patient data integrity is maintained through strong encryption while ensuring that hospital operations remain aligned with dynamic regulations such as the PDP Law and the Health Law, to avoid administrative sanctions or detrimental fines.

Liability Disputes are handled through strengthening the legal dimension by the Legal Department by clarifying and renegotiating contracts with vendors. This action plan aims to close any ambiguities in the division of responsibility, so that in the event of a system malfunction, there is a clear legal path regarding the distribution of liability between the hospital and the technology provider. Overall, this action plan distributes the burden of responsibility proportionally to each division leader, reflecting that the security of AI use is not merely a technical issue, but rather an integration of medical leadership, IT excellence, legal acumen, and ethical governance oriented towards patient and institutional protection.

Monitoring and Review Stage

The risk management framework must include ongoing monitoring and review mechanisms to ensure the effectiveness of risk management. Monitoring is carried out through Key Performance Indicators (KPIs) and periodic review mechanisms. a. Key Performance Indicators (KPIs): Number of AI error incidents per month. Level of regulatory compliance, Number of AI-related patient complaints, Insurance claim settlement status, HR training completion rate. b. Review Mechanisms: Quarterly internal audits, Annual external reviews, Policy updates based on regulatory developments, Reporting to senior management.

Table 9. Risk Monitoring Schedule

No	Monitoring Activities	Frequency	Person responsible
1	Review risk register	Monthly	Risk Officer
2	Regulatory compliance audit	Quarterly	Compliance
3	Evaluation of control effectiveness	Semester	Management
4	Update risk matrix	Annual	Committee Risk

Sumber: Monitoring Planning Results, 2026

Analysis of Table 9 regarding the Risk Monitoring Schedule demonstrates an integrated and continuous monitoring cycle to ensure that AI risk mitigation remains relevant to technological developments and legal dynamics. This monitoring structure is designed with a logical time hierarchy, starting from the operational level to the strategic level. The Risk Register Review activity, conducted monthly by the Risk Officer, serves as an early warning system to detect anomalies or minor incidents in daily AI use, thus preventing risk escalation before it becomes a major legal dispute. This monthly frequency is crucial given the dynamic nature of AI algorithms and medical data, making routine monitoring essential to maintaining diagnostic integrity in healthcare facilities.

At the tactical and strategic levels, the Compliance Team's Quarterly Regulatory Compliance Audits ensure that hospital operations adhere to Health Law No. 17/2023, Ministerial Regulation 75/2020, and the PDP Law. These audits serve as a validation tool to ensure accuracy standards of over 90% are maintained and data confidentiality protocols are strictly adhered to. Furthermore, Management's Semi-annual Control Effectiveness Evaluations provide an opportunity to review whether established strategies, such as liability sharing and malpractice insurance, are truly providing the desired protection. This cycle concludes with an Annual Risk Matrix Update by the Risk Committee, which aims to recalibrate the entire risk map based on a full year of incident data, the latest regulatory developments, and the latest advances in medical AI technology.

Overall, this monitoring schedule creates a responsive and accountable clinical governance ecosystem. With a clear division of responsibilities from the Risk Officer to the Risk Committee, the hospital is not merely reactive to issues but proactive in building a multi-layered defense system. Disciplined adherence to this monitoring schedule is key for Cahaya Medika Hospital to minimize legal loopholes and ensure that artificial intelligence innovation continues to align with patient safety and compliance with Indonesia's complex legal system.

Implementation of the Framework in accordance with Indonesian Regulations

The legal risk management framework designed must be integrated with applicable Indonesian regulations. This integration ensures that risk management is not only operationally effective but also meets applicable legal requirements.

1. Integration with Health Law No. 17/2023: AI use policy in accordance with Article 220, Accuracy and transparency standards, Accountability mechanisms, Documentation of AI use.
2. Integration with Permenkes 75/2020: AI accuracy verification procedures, Operational standards for AI use, Incident reporting mechanisms, Periodic evaluation of AI systems.
3. Integration with PDP Law 27/2022: Personal data protection policy, Informed consent procedures for AI, Data security mechanisms, Data subject rights. d. Integration with Medical Practice Law No. 29/2004: Standards of practice for doctors using.

Conclusion

Based on the research findings and discussion, the use of artificial intelligence (AI) for diagnosis at Cahaya Medika Makassar Hospital presents several significant legal risks. These include criminal and civil malpractice arising from diagnostic errors, non-compliance with health and personal data protection regulations, uncertainty regarding liability among doctors, hospitals, and AI vendors, patient data security risks, and limited human-resource and institutional readiness.

These risks demonstrate that AI adoption in clinical practice requires not only technological preparedness but also a comprehensive legal and governance framework. An effective legal risk management framework should follow the four stages of ISO 31000: risk identification, risk assessment, risk treatment, and continuous monitoring and review. The framework should be harmonized with Indonesian health, medical practice, artificial intelligence, and personal data protection regulations. The reported legal disputes and AI-related diagnostic incidents demonstrate that inadequate governance may expose hospitals to litigation, financial losses, reputational damage, and weakened patient trust. Several recommendations can therefore be proposed. First, the government should harmonize AI-related health regulations and clarify the allocation of liability among doctors, hospitals, technology providers, and other relevant parties. Official guidelines should also establish standards for assessing negligence involving AI-assisted diagnosis and create accreditation mechanisms to ensure system safety, reliability, and accuracy. Second, hospitals should formulate comprehensive internal AI policies covering authorization, verification, documentation, accountability, and data protection. Regular training should be provided to medical personnel to improve their ability to interpret AI outputs and recognize technological limitations. Medical documentation should clearly record AI involvement and subsequent clinical decisions, while vendor contracts should contain explicit provisions concerning system performance, liability, and compensation. Finally, policy development should encourage specialized insurance products covering AI-related malpractice and data breaches, establish accessible mediation mechanisms for disputes, and provide incentives for hospitals that implement effective AI governance and risk-management systems. These measures are essential to ensure that technological innovation in healthcare develops alongside legal certainty, patient protection, professional accountability, and institutional responsibility.

References

Aulia, N., Silitonga, V. D., & Edwin, E. (2025). Civil Legal Liability of Doctors in Malpractice Cases Due to Violations of Informed Consent. *Jambura Medical and Health Science Journal*, *4*(2), 179–189. https://doi.org/10.37905/jmhsj.v4i2.33683

Badar, E. S., Fauzi, A., & Jazuli, A. (2023). Kebijakan Pelindungan Data Pribadi Undang-Undang Nomor 27 Tahun 2022 Dalam Prespektif Hukum Positif Dan Hukum Islam [Personal Data Protection Policy under Law Number 27 of 2022: A Perspective from Positive Law and Islamic Law]. *Hukum Islam*, *23*(1), 61. https://doi.org/10.24014/jhi.v23i1.20465 [In Indonesian]

Darmadi, E. Y., Ropii, I., & Kencana Rukmi, N. (2025). Perlindungan Hukum Rekam Medis elektronik dalam Praktik Kedokteran Gigi [Legal Protection of Electronic Medical Records in Dental Practice]. *Jurnal Hukum Dan Etika Kesehatan*, *6*(1), 33–50. https://doi.org/10.30649/jhek.v6i1.271 [In Indonesian]

Junaidi. (2023). *Hukum Kesehatan: Upaya Perlindungan dan Penyelesaian Sengketa Medik di Indonesia [Health Law: Protection Efforts and Medical Dispute Resolution in Indonesia]*. Jakad Media Publishing.

Kushariyadi, K., Apriyanto, H., Herdiana, Y., Asy'ari, F. H., Judijanto, L., Pasrun, Y. P., & Mardikawati, B. (2024). *Artificial intelligence: Dinamika perkembangan AI beserta penerapannya [Artificial Intelligence: The dynamics of AI development and its applications]*. PT. Sonpedia Publishing Indonesia.

Kusnandar, S. (2025). *Anatomi Hukum Kesehatan Di Era Ai Menimbang Etika, Regulasi, Dan Tanggung Jawab Klinis [The Anatomy of Health Law in the AI Era: Weighing Ethics, Regulation, and Clinical Responsibility]*. Penerbit Adab.

Rizkia, N. D., & Fardiansyah, H. (2023). *Metode penelitian hukum (normatif dan empiris) [Legal research methods (normative and empirical)]*. Penerbit Widina.

Siswanto, N., Hapsari, D. C., Astuti, N. A. M., Kep, M., Pebriani, N. E., Kep, M., Sulistyowati, A. D., Pasaribu, N. K., Kep, M., & Sitorus, J. (2026). *Manajemen Keperawatan Digital [Digital Nursing Management]*. CV Rey Media Grafika.

Sukarna, P., & Winata, I. (2025). Analisis Hukum Batasan Tanggung Jawab dan Perlindungan Pasien Dalam Penggunaan Robotic Surgery Untuk Tindakan Pembedahan Medis di Fasilitas Pelayanan Kesehatan Tingkat Utama [Legal Analysis of Liability Limits and Patient Protection in the Use of Robotic. *Indonesian Journal of Law and Justice*, *3*(2), 8. https://doi.org/10.47134/ijlj.v3i2.5394 [In Indonesian]

Takwa, H. M. (2025). *Manajemen risiko dalam rumah sakit: Strategi pencegahan dan mitigasi [Risk management in hospitals: Prevention and mitigation strategies]*. PT Kimhsafi Alung Cipta.

Yaddin, N., Salmawati, L., & Laba, S. B. (2025). AI, Kebijakan, dan Kesalahan Manusia: Memikirkan Kembali Peran Perilaku Pekerja dalam Mencegah Kecelakaan Kerja [AI, Policy, and Human Error: Rethinking the Role of Worker Behavior in Preventing Work Accidents]. *Jurnal Locus Penelitian Dan Pengabdian*, *4*(10), 9528–9540. https://doi.org/10.58344/locus.v4i10.4833 [In Indonesian]