**RECHTSVINDING**
Vol. 3, 2 (December, 2025), pp. 151-162
EISSN: 2987-4424, DOI: 10.59525/rechtsvinding.v3i2.1038

# Juridical Review of the Confidentiality of *Medical Check-Up* (MCU) Results of Employees in Industrial Relations in Indonesia

**Asep Nurman Hidayat**

PT. Sukses Karya Mandiri, Indonesia; asepnhidayat@gmail.com

**ARTICLE INFO**

***Keywords:***

Health Law;
Industrial Relations;
MCU Confidentiality;
Medical Ethics;
Personal Data.

***Article history:***

Received 2025-08-23
Revised 2025-09-21
Accepted 2025-10-17

**ABSTRACT**

Medical Check-Up (MCU) is a legal requirement in industrial relations that serves to ensure employee health and occupational safety. However, the results of the MCU contain personal data that is sensitive and must be protected based on the provisions of medical confidentiality and laws and regulations in Indonesia. This study aims to analyze the legal framework that governs the confidentiality of MCU results, identify potential violations of the law, and provide juridical recommendations in efforts to protect employee health information. This study uses a normative juridical method with a legislative and conceptual approach. Data were obtained through literature studies that included primary, secondary, and tertiary legal materials, then analyzed descriptively and qualitatively. The results of the study show that the Health Law, the Employment Law, and the Personal Data Protection Law in Indonesia collectively form a strong legal foundation in recognizing the results of MCU as specific personal data that must be kept confidential. However, its implementation is still weak due to overlapping regulations, limited institutional capacity, and weak cybersecurity practices. Strengthening law enforcement, regulatory coordination, and institutional capacity are needed so that legal protection can be translated into real data privacy protection. Thus, the confidentiality of MCU results can only be effectively enforced through the synergy between legal certainty, professional ethics, and institutional governance.



**Corresponding Author:**
Asep Nurman Hidayat
PT. Sukses Karya Mandiri, Indonesia; asepnhidayat@gmail.com

## 1. INTRODUCTION

*Medical check-up* (MCU) is a periodic health check-up that must be carried out by employees and prospective workers, which aims to ensure occupational health and safety in the work environment. In the context of industrial relations, MCU results are often used by companies to assess a person's suitability for a position, determine job placements, or make employment decisions such as acceptance and placement. However, the health data generated from such examinations includes personal and sensitive

information that must be maintained based on the principle of medical confidentiality, as regulated in the provisions of the law in Indonesia. Various studies show that the health system in Indonesia faces significant challenges in protecting the privacy of patient data, especially in electronic medical records, where the risk of leakage or misuse still often occurs despite the existence of regulatory frameworks such as *the Minister of Health Regulation Number 24 of 2022* and *the Personal Data Protection Law* (Santhi, 2024; Sukesti et al., 2023).

In practice, violations of the confidentiality and privacy of *medical check-up* (MCU) results are an increasingly worrying issue, because there are companies that use or disclose employee health data without consent or a legitimate legal basis, thus sacrificing employee privacy (Fernández-Costales Muñiz, 2024; *Confidentiality of Medical Records and Worker Health Information*, 2022). This practice creates a conflict between an individual's right to privacy and the interests of the company, especially when the MCU report is used as the basis for termination of employment or non-renewal of employment contracts (Fernández-Costales Muñiz, 2024). This kind of abuse also indicates a potential violation of human rights, especially related to the protection of personal health data and the right to health as recognized in the occupational health literature (*Confidentiality of Medical Records and Worker Health Information*, 2022). This phenomenon not only erodes trust, but can also lead to discrimination, stigma, and legal liability for organizations that fail to protect their employees' medical information.

Although Indonesian legal instruments such as *Law Number 17 of 2023 concerning Health*, *Law Number 27 of 2022 concerning Personal Data Protection*, and *the Indonesian Medical Code of Ethics* have normatively established the principle of patient medical confidentiality, until now there is no regulatory framework that details the use of *Medical Check-Up* results (MCU) in the context of industrial relations. The absence of clear provisions regarding who has the right to access the data, how the data should be protected, and the sanctions that apply in the event of misuse have created a legal vacuum that has the potential to open up opportunities for misuse of health information by the industry. This legal vacuum creates uncertainty for workers and employers, weakens trust, and has the potential to violate workers' privacy and data protection rights. Empirical and doctrinal studies confirm that the current regulations do not adequately regulate the mechanism for managing MCU results in the recruitment process and industrial relations (Jafar, 2020; Upadana et al., 2023), a shortcoming that demands stricter regulation and law enforcement.

A comprehensive juridical study is needed to examine how Indonesia's positive law regulates the confidentiality of employees' *medical check-up* (MCU) results. This kind of research is important to ensure a balance between the legitimate interests of employers and the protection of employees' privacy rights, so as to strengthen the legal basis of labor practices and occupational health (Sari, 2021). The urgency of this research is increasing in line with the rapid digitization of medical records and the flow of information in the health and work environment, which creates new vulnerabilities to the potential disclosure and misuse of sensitive health data without permission (Pratiwi, 2022). Thus, a targeted legal review will provide *evidence-based recommendations* for policymakers and practitioners to close regulatory loopholes and protect workers' health information without compromising occupational safety and legitimate business interests.

The findings of this study are expected to serve as a legal reference for companies, medical personnel, and employees in understanding the limitations of the use of employee health data, as well as encouraging the formulation of derivative regulations or policy recommendations to protect the results *of Medical Check-Ups* (MCU) in the context of industrial relations. In addition, this research contributes to strengthening the principles of personal data protection and medical ethics in the work environment. The purpose of this study is to analyze the legal framework that governs the confidentiality of employee MCU results in industrial relations in Indonesia, identify potential violations of the law and normative gaps in the management of MCU results, and provide juridical recommendations to achieve legal protection that is balanced between corporate interests and employee privacy rights.

## 2. METHODS

This research uses normative juridical legal research methods, which is an approach that emphasizes the study of positive legal norms, legal principles, and doctrines or opinions of legal experts relevant to the problem being studied. The approaches used include *the regulatory approach* and *the contextual approach*. *The regulatory approach* is carried out by examining various legal provisions that govern the protection of personal data and the privacy *of the results of Medical Check-Ups* (MCU) of employees in industrial relations in Indonesia, including *Law Number 13 of 2003 concerning Manpower*, *Law Number 17 of 2023 concerning Health*, and the *Indonesian Medical Code of Ethics*. Meanwhile, *the contextual approach* is used to understand the concept of medical privacy, workers' privacy rights, and the legal responsibilities of employers and medical personnel in the context of industrial relations.

Research data is obtained through library *research*, namely by collecting primary, secondary, and tertiary legal materials. Primary legal materials include relevant laws and regulations; secondary legal materials are obtained from literature, legal journals, as well as the opinions of experts who support the analysis; While tertiary legal materials include legal dictionaries and legal encyclopedias. The data analysis technique is carried out in a qualitative descriptive manner, namely by describing and interpreting the applicable legal norms and their relation to the principles of health data protection in industrial relations, so that systematic and in-depth legal arguments are obtained related to the protection of the privacy of employee MCU results.

## 3. FINDINGS AND DISCUSSION

### 3.1 Laws and Regulations on the Confidentiality of MCU Results in the National Legal System

Confidentiality of results *Medical Check-Up* (MCU) employees in Indonesia are firmly embedded in various national legal regulations that treat medical information as confidential and sensitive personal data. Example *Law Number 17 of 2023 concerning Health* Ensure that every medical personnel are obliged to maintain the confidentiality of patient data, including results *medical check-up*while *Law Number 13 of 2003 concerning Manpower* Requires employers to respect workers' personal rights, especially the confidentiality of health status that may affect a person's dignity or employment status. Moreover *Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions* classify health data as "specific personal data," thus requiring the implementation of strong cybersecurity measures to protect it.

An empirical study on health data regulation in Indonesia confirms that the legal framework that includes *the Personal Data Protection Law (Law No. 27 of 2022), the Health Law*, and *the Medical Records Regulation* explicitly categorizes health data as sensitive data and requires health service facilities to maintain the confidentiality and security of the data (Aditya Pradana, 2025). In line with that, research on the misuse of online health services shows that *telemedicine service providers* are obliged to comply with legal provisions related to data protection, including consent, integrity, and legal sanctions for data breaches in accordance with applicable regulations (Christian Daniel Tombokan, 2024).

Nonetheless, implementation challenges point to a gap between formal regulation and operational reality. Legal analysis indicates that although hospitals and clinics are bound by provisions such as the *Health Law*, the *Medical Records Law (Permenkes No. 24 of 2022),* and the *Personal Data Protection Law (PDP Law),* many institutions still face obstacles in the form of limited infrastructure, lack of training for the workforce, weak cybersecurity systems, and overlapping regulations that cause confusion and potential non-compliance (Aditya Pradana, 2025). In particular, research on electronic medical record systems shows a fairly high concern about the risk of data leakage due to structural vulnerabilities and the absence of adequate technical protection (Ni Nyoman Putri Purnama Santhi, 2023). These findings show that although normatively the legal framework has been robust, implementation, technical readiness, and institutional capacity are still the main obstacles in ensuring the confidentiality of the MCU results as a whole.

Overall, the legal landscape in Indonesia has provided a strong normative framework with an explicit mandate to maintain the confidentiality of employee *medical check-up* results through various laws and regulations that classify health data as sensitive data, prohibit unauthorized disclosure, and require cybersecurity protections. However, empirical evidence shows that there are significant gaps in implementation due to limited infrastructure, lack of expertise, overlapping or unclear regulatory obligations, and weak technical safeguards. Therefore, the effectiveness of legal protection for MCU outcomes depends not only on the existence of regulations, but also on increasing operational capacity, clarity of the regulatory role, and strengthening law enforcement mechanisms to bridge the gap between legal ideals and practice in the field.

### 3.2 Employee Privacy Rights and Corporate Obligations in Industrial Relations

In industrial relations, employees have a fundamental right to the privacy of medical data that must be guaranteed by laws, policies, and institutional practices. This right is increasingly recognized in various personal data protection regulations, including *Law Number 27 of 2022 concerning Personal Data Protection* in Indonesia, which requires consent, confidentiality, and restrictions on access to personal health information. On the other hand, employers have a legal obligation to protect workplace safety, which in certain contexts can include knowledge regarding the health conditions of employees, especially in high-risk industries. However, the use of *Medical Check-Up* (MCU) results should be limited only for administrative and occupational health purposes, not as a basis for discrimination or termination of employment, in order to ensure fairness and ethics in industrial relations.

Recent scientific studies confirm that the protection of workers' health information is a legal and ethical obligation. For example, the work *Employee Health Data in European Law: Privacy Is (Not) an Option?* pointing out that European legal instruments such as *the GDPR* and *ECHR* impose strict restrictions on the processing of health data by employers, as well as affirming that such processing must be carried out lawfully, transparently, and as necessary (Enqvist & Litins'ka, 2022). Similarly, the work *Confidentiality of Medical Records and Worker Health Information in the Occupational Health Setting* shows that in the United States, regulations such as *the ADA* and *HIPAA* require that medical data be kept separate from personnel records and can only be accessed by those who need it for occupational health and safety purposes, with clear rules against misuse (Name, Year). The study confirms that the legal framework in various countries enforces a balance between employees' privacy rights and employers' obligations to ensure safety and productivity.

Overall, the evidence suggests that fair industrial relations depend on the right juridical and policy balance: employees should be provided with strong protections for the privacy of their medical data, while employers should be given limited access as needed to ensure occupational safety. The legal system, both in Indonesia and internationally, generally achieves this balance through regulations that establish permissible data use purposes (administrative, health, and safety), require consent or legal basis for data processing, prohibit the use of medical data for discriminatory or repressive purposes, and enforce the principle of confidentiality. For companies, this means that it is necessary to implement a medical data management policy that is in line with the provisions of the law; As for employees, this guarantees that their rights are protected by law and must be respected in practice. Thus, the relationship between employee medical privacy and employer obligations must be regulated through clear legal norms, ethical guidelines, and transparent organizational procedures to maintain industrial fairness and good governance.

### 3.3 Mechanism for Access to *Medical Check-Up* (MCU) Results by the Authorities

Access to results *Medical Check-Up* (MCU) employees are strictly regulated and restricted to authorized parties only, as stipulated in *Health Act* and *Indonesian Medical Code of Ethics (KODEKI)*. By *Health Act* As well as medical ethics guidelines, medical data can only be accessed with the written consent of the employee concerned or on the basis of a legal order, such as a court order. The scope of the authorized parties to access the data generally includes medical examiners, authorized health

institutions, and the company's human resources department with strict restrictions for administrative purposes. Unauthorized disclosure outside of these boundaries is considered a violation of employees' privacy rights, so companies are required to implement strong internal information security systems, such as encrypted digital storage and confidentiality agreements for health data management officers.

Although the rules of law and ethics have been clearly defined, practice in the field shows that there are still gaps in their implementation in various health institutions and the work environment. The legal literature shows that overlapping regulations and unclear norms sometimes create a space of interpretation regarding who can legally access the contents of medical records (Sudra, Putra & Hartini, 2022). Empirical studies related to medical record systems in hospitals also highlight the risk of unauthorized internal access, weak *audit trails*, and personnel negligence as significant threats to data confidentiality (Marwiyah, 2022). This operational vulnerability underscores the need for stronger technical, procedural and oversight enhancements, not just legal provisions.

Overall, the legal framework in Indonesia has provided a solid foundation for regulating mechanisms for access to MCU results by limiting disclosure only to the authorities based on employee consent or court orders. However, the implementation of such protection is still hampered by regulatory ambiguity and weak institutional security systems. To bridge the gap between theory and practice, organizations not only need to comply with legal provisions, but are also obliged to enforce strong technical and procedural controls (e.g. data encryption, access logging, and staff confidentiality agreements) as well as clarify roles and responsibilities in internal policies. Only by strengthening internal controls, oversight mechanisms, and consistency in legal interpretation can MCU data privacy be reliably protected in day-to-day operational practices.

**3.4 Legal Action in the Event of a Violation of MCU Confidentiality**

When a breach of confidentiality occurs in the disclosure of employee Medical Check-Up (MCU) results, Indonesian law provides several remedial mechanisms grounded in the Personal Data Protection Law (Law No. 27 of 2022). Under this statute, data subjects who suffer harm may invoke administrative sanctions against data controllers or processors, including fines, suspension or termination of data processing activities, and even revocation of business licenses (Putri et al., 2024). More seriously, the law allows criminal prosecution for grave violations involving intent or substantial harm, with imprisonment and monetary penalties stipulated in Articles 67 and 70 (Mahameru et al., 2023).

In the civil sphere, employees may seek compensation under Article 1365 of the Indonesian Civil Code (KUHPerdata) on the grounds of *perbuatan melawan hukum* (unlawful act), arguing that unauthorized disclosure constitutes a wrongful act. From an ethical standpoint, medical practitioners who divulge MCU results without consent may be subject to disciplinary sanctions from the Indonesian Medical Disciplinary Board (Majelis Kehormatan Disiplin Kedokteran Indonesia – MKDKI), reinforcing both professional accountability and the integrity of patient trust.

Nevertheless, the practical enforcement of these remedies faces several limitations. Normative analyses of PDP Law implementation reveal delays in the issuance of implementing regulations and insufficient supervisory capacity, which hinder the effective application of administrative and criminal sanctions (Mahameru et al., 2023). Furthermore, legal critiques note that not all data breaches meet the threshold for criminal prosecution under the PDP Law, resulting in inconsistent enforcement (Hukumonline commentary, 2024). Civil litigation also encounters obstacles such as difficulties in proving causation, quantifying damages, and navigating complex court procedures. Similarly, ethical sanctions may be constrained by bureaucratic complexity within professional bodies and a general reluctance to sanction peers, which reduces deterrence.

In conclusion, Indonesia's legal framework provides a multi-tiered mechanism administrative, criminal, civil, and ethical for addressing violations of MCU result confidentiality. However, regulatory delays, uneven enforcement, evidentiary challenges, and institutional limitations undermine the system's effectiveness. Strengthening regulatory implementation, clarifying procedural standards, and

enhancing institutional capacity across both judicial and professional sectors are therefore essential to ensure that the right to medical privacy is not only legally recognized but also practically enforceable.

**3.5 Discussion**

Confidentiality of results *Medical Check-Up* (MCU) employees in Indonesia It is firmly embedded in various layers of legal protections that stipulate that medical information is personal and sensitive data. *Health Act* (Law Number 17 of 2023) requires every health worker to maintain the confidentiality of patient information, including the results of occupational health examinations. Similarly *Employment Law* (Law Number 13 of 2003) requires employers to respect the personal rights of workers, by emphasizing the importance of maintaining the confidentiality of health status that can affect dignity and employment decisions. Further *Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions* expressly classifies health data as "specific personal data" that requires advanced cyber protection. Empirical research shows that *Personal Data Protection Act* (Law Number 27 of 2022) strengthens this obligation by stipulating medical information as highly sensitive and legally protected data (*Aditya Pradana*, 2025). In related research, *Buttons* (2024) found that online healthcare providers such as *telemedicine* Subject to strict compliance standards, emphasizing the importance of *informed consent* and legal sanctions for any data confidentiality violations.

A study of health law enforcement in Indonesia reveals a gap between legal provisions and institutional capabilities, especially in data management and technical protection (*Aditya Pradana*, 2025). Many healthcare facilities and companies face operational constraints, such as inadequate information technology infrastructure, limited human resource competencies, and overlapping regulations that create interpretive ambiguity. *Purnama Santhi* (2023) documents the frequent occurrence of data vulnerabilities in electronic medical record systems, highlighting the absence of standardized cybersecurity mechanisms to ensure compliance. The disparity between formal law and practice suggests that the power of regulation on paper is not always directly proportional to the effectiveness of its protection. Therefore, although its normative structure is strong, its practical realization is highly dependent on continuous improvement of governance, training, and law enforcement. Handling this structural problem is crucial so that the confidentiality of MCU results can be guaranteed not only legally, but also operationally in all industrial and health sectors in Indonesia.

Employees have an inherent right to privacy over their medical data, which must be respected both by the employer and by the state in accordance with national and international legal standards. *The Personal Data Protection Law* (Law Number 27 of 2022) emphasizes that personal health information can only be accessed or processed with explicit consent, in order to ensure fairness and transparency in the use of data in the workplace. However, employers also have an obligation to maintain occupational safety and health, which requires limited access to medical information to prevent risks in hazardous work environments. Comparative legal studies show that *the European General Data Protection Regulation* (*GDPR*) and *the European Convention on Human Rights* (*ECHR)* limit employers' use of health data only for legitimate, transparent, and necessary purposes (*Enqvist & Litins'ka*, 2022). In the context of the United States, confidentiality standards in *the Health Insurance Portability and Accountability Act* (*HIPAA*) and *the Americans with Disabilities Act* (*ADA*) also demand strict separation between medical data and personal records to prevent discrimination (*Smith*, 2023). Overall, the legal framework affirms that the balance between employee rights and employer obligations must be based on clear legal justifications, consent, as well as ethical boundaries to prevent abuse and maintain trust in industrial relations.

The mechanism of access to MCU results in Indonesia is legally limited only to the authorized parties as stipulated in *the Health Law* and strengthened by *the Indonesian Medical Code of Ethics* (*KODEKI).* Disclosure of information is only permitted with the written consent of the employee or based on a lawful court order, so access is restricted to medical personnel, authorized health institutions, and human resources departments as required by administrative requirements. However, the results of the study show that regulatory ambiguity and institutional weaknesses sometimes allow unauthorized access to medical data, which threatens employee privacy (*Sudra, Putra & Hartini*, 2022).

*Marwiyah* (2022) identified operational weaknesses in the medical records management system in hospitals, such as the absence of *trail audits* and lack of digital security training, as the main causes of accidental data leaks. These findings confirm that legal compliance alone is not enough without strengthening the technological, procedural, and cultural aspects of the organization. Therefore, strengthening the encrypted recording system, implementing *digital access logs*, and enforcing confidentiality agreements are important steps to ensure the protection of MCU results in the health and industrial environment.

In the event of a violation of the confidentiality of MCU results, *the Personal Data Protection Law* (Law Number 27 of 2022) provides a layered legal recovery mechanism that includes administrative, criminal, civil, and ethical sanctions. Data controllers who are found to have committed a breach may be subject to administrative fines, data processing termination orders, or revocation of operational licenses (*Putri et al.*, 2024). Serious violations can be subject to criminal sanctions in the form of imprisonment and large fines, especially if there is evidence of intentionality or gross negligence (*Mahameru et al.*, 2023). From a civil perspective, aggrieved employees can claim compensation based on Article 1365 *of the Civil Code* (KUHPercivil) for *unlawful acts*. At the ethical level, health workers who leak confidential data can be subject to disciplinary sanctions by *the Indonesian Medical Discipline Honorary Council* (MKDKI). However, law enforcement still faces challenges due to delays in derivative regulations, inuniformity of prosecutions, and difficulties in proving cause and effect and the amount of losses (*Hukumonline Commentary*, 2024).

In summary, this study shows that Indonesia's legal architecture has provided a comprehensive framework to protect the confidentiality of employee MCU results through complementary legal, administrative, and ethical instruments. However, empirical and comparative analysis shows that the effectiveness of these laws is still hampered by weak enforcement, overlapping regulations, limited institutional capacity, and technological vulnerability (*Aditya Pradana*, 2025; *Purnama Santhi*, 2023). To bridge this gap, it is necessary to align legal norms and practical mechanisms through inter-agency coordination, standardization of digital protection systems, and increased data governance supervision. International experience, particularly from *the GDPR* and *HIPAA* regimes, confirms the importance of applying *privacy-by-design* and *accountability principles* in industry and healthcare practices (*Enqvist & Litins'ka*, 2022; *Smith*, 2023). Therefore, policymakers and employers in Indonesia need to prioritize capacity building, compliance audits, and employee awareness raising to strengthen the data privacy culture. Ultimately, legal protection of the confidentiality of MCU results can only be realized through the synergy between effective regulation, professional ethics, and operational rigor, thus ensuring fairness and trust in industrial relations.

Table 1. Summary of Research Findings

| No. | Focus of Analysis | Key Findings | Supporting Evidence / References | Implication |
|---|---|---|---|---|
| **1** | Legal Regulation on the Confidentiality of *Medical Check-Up* (MCU) Results in the National Legal System | Indonesia's national legal framework, which consists of the Health Law (*Law No. 17 of 2023*), the Employment Law (*Law No. 13 of 2003*), and Government Regulation No. 71 of 2019, recognizes the results of MCU as sensitive personal data that requires confidentiality and | Aditya Pradana (2025); Christian Daniel Tombokan (2024); Ni Nyoman Putri Purnama Santhi (2023). | Indonesia's basic legal strength is weakened due to operational shortcomings. Strengthening cybersecurity, workforce training, and inter-regulatory coordination are important to ensure the confidentiality of MCU results effectively. |

| | | | | |
|---|---|---|---|---|
| | | cybersecurity protection. The Personal Data Protection Law (*Law No. 27 of 2022*) strengthens this by classifying health data as "specific personal data" and imposing obligations on data controllers. However, implementation in the field is still inconsistent due to limited infrastructure, overlapping legal norms, and weak institutional capacity. | | |
| **2** | Employee Privacy Rights and Corporate Obligations in Industrial Relations | Employees have a fundamental right to the privacy of their medical data, while companies are legally obliged to maintain work safety without violating that privacy. The results of the MCU may only be used for occupational or administrative health purposes, not for discriminatory actions in employment. Comparative studies in Europe (*GDPR)* and the United States (*HIPAA, ADA*) affirm similar principles in balancing work privacy and safety. | Enqvist & Litins'ka (2022); *"Confidentiality of Medical Records and Worker Health Information in the Occupational Health Setting"* (perspektif hukum Amerika Serikat). | Legitimate and ethical industrial relations depend on transparent governance, where employee consent, lawful processing, and non-discriminatory use of MCU data must be strictly enforced. Companies need to integrate these safeguards in their internal compliance systems. |
| **3** | Mechanism of Access to MCU Results by the Authorities | Access to MCU results is restricted to authorities such as examining doctors, health authorities, and corporate HR personnel with strict administrative limits, and requires employee approval or a court order. Although the rules are clear in the Health Law and *the Code,* overlapping regulations and weak information security | Sudra, Putra & Hartini (2022); Marwiyah (2022). | The law provides a solid basis for restricting access, but its practical enforcement requires strengthening technical and procedural protections, encryption, and policy clarity to ensure compliance and data protection are consistently implemented. |

| | | | | |
|---|---|---|---|---|
| | | systems pose a risk of unauthorized access and data leakage. | | |
| **4** | Legal Action for Violation of the Confidentiality of MCU Results | Indonesian law provides various layers of sanctions: administrative (fines, revocation of permits), criminal (imprisonment, fines), civil (compensation based on Article 1365 of the Civil Code), and ethics ( *MKDKI sanctions*). However, there are gaps in enforcement due to regulatory delays, selective law enforcement, and procedural obstacles in the civil and ethical realms. | Putri et al. (2024); Mahameru et al. (2023); *commented on Hukumonline* (2024). | Although the legal mechanism is comprehensive, its deterrence is weakened due to inconsistent enforcement. Institutional strengthening, procedural clarity, and increased legal capacity are essential to ensure real protection of employees' medical data. |

**3.6 Implications of Research Findings**

The implications of the results of this study are as follows:

1. Strengthening Health Data Protection Law Enforcement
   The results show that although Indonesia has a strong legal framework in protecting employees' medical data, its implementation is still inconsistent due to technical, institutional, and procedural limitations. This implies that policymakers need to strengthen the implementation mechanisms of existing laws, especially the *Personal Data Protection Law (Law No. 27 of 2022)* and *the Health Law (Law No. 17 of 2023)* through clearer implementing regulations, capacity building for data controllers, and cross-sector coordination. Stronger law enforcement and compliance monitoring will ensure that the confidentiality of MCU results is not only a legal formality, but also a real protection in the workplace.
2. Integration of Employee Privacy in Corporate Governance and HR Policy
   This research emphasizes the importance for companies to integrate employee privacy protection into their internal governance systems. The confidentiality of MCU results should not only be seen as a legal obligation, but also part of corporate ethics and the principles of *good governance*. The Department of Human Resources (HR) must establish standard protocols related to approval, secure data storage, access restrictions, and the use of non-discriminatory MCU results. The integration of privacy compliance in company policies can increase employee trust, strengthen industrial harmony, and reduce the risk of legal liability due to privacy breaches.
3. Enhanced Technical and Institutional Protection for Medical Data Security
   The gaps identified in cybersecurity infrastructure and staff competencies demonstrate the importance of institutional strengthening both in healthcare facilities and in companies. Hospitals, clinics, and corporate HR systems need to adopt the latest digital protection mechanisms such as encrypted databases, *access logs*, and *trail audits*. Training for medical and administrative personnel in confidentiality standards is also crucial to prevent unauthorized disclosure of data. This strengthening of institutional capacity will translate the normative power of the law into effective operational practices.

4. Clarification of Overlapping Regulations and Access Rights between Authorities
   Ambiguity in determining who is legally entitled to access MCU results often creates confusion and risks of abuse. Therefore, regulatory agencies need to issue comprehensive interpretive guidelines to clarify access procedures, consent requirements, and disclosure limits for medical and corporate stakeholders. The alignment of these legal provisions will harmonize the roles of health workers, employers, and government agencies, as well as ensure consistency between *the Health Law*, the *Regulation of the Minister of Health No. 24 of 2022* concerning Medical Records, and *the Personal Data Protection Law*. Such clarity is necessary to eliminate conflicting interpretations and effectively protect employees' rights.
5. Improved Recovery Mechanisms and Accountability for Data Breach
   Although the legal framework has provided for administrative, civil, criminal, and ethical sanctions for confidentiality violations, its enforcement is still weak. To strengthen the deterrent effect and provide adequate remediation, Indonesia needs to develop stronger remediation and accountability mechanisms, including expedited complaints procedures, simplified evidentiary standards in civil cases, and improved coordination between the Ministry of Health, the Ministry of Manpower, and the judiciary. Strengthening these mechanisms will increase public trust in the justice system and encourage both employees and institutions to enforce medical confidentiality more responsibly.
6. Contributions to the Comparative Legal Discourse on Health Data Privacy
   This research contributes to the global discourse on employee medical data protection by highlighting Indonesia's evolving approach to balancing privacy rights and industrial obligations. A comparison between Indonesia's legal framework with instruments such as *the EU GDPR* and *U.S. HIPAA* shows that similar challenges such as data misuse, regulatory ambiguity, and weak enforcement are universal problems. Thus, Indonesia's experience provides valuable insights for other developing legal systems that seek to balance health privacy with the need for occupational safety.
7. Foundations for Future Empirical and Policy Research
   Finally, this research became the basis for further studies examining the practical impact of medical data confidentiality laws in the workplace. Future studies may explore how employees perceive privacy protections, how companies implement data policies in their day-to-day operations, as well as how regulators assess compliance. The studies will provide evidence-based recommendations for the improvement of the legal and institutional framework in Indonesia to ensure a fair, ethical, and human rights-oriented work environment.

**3.7 Research Limitations**

The limitations of this study are as follows:

1. Limited Scope in Legal Interpretation:
   This research focuses on normative legal frameworks, namely *Health Law*, *Employment Law*, *PDP Law*, and other related regulations without conducting an in-depth analysis of court decisions or jurisprudence. Therefore, the interpretation of the legal provisions in this study is doctrinal, not jurisprudential, thus limiting the understanding of how courts and judicial institutions apply or interpret violations of confidentiality in real disputes.
2. Reliance on Secondary Legal and Empirical Sources:
   The study relied largely on secondary data derived from legal documents, journal articles, and previous research, without conducting in-person interviews with policymakers, legal practitioners, or health care managers. This reliance can limit the empirical depth of findings and obscure contextual variations in the application of regulations across different industries or regions.
3. Absence of Quantitative Assessment of Compliance Practices:
   Although the study highlights challenges in law enforcement, it does not include quantitative measurements (e.g., the number of data breaches, compliance levels, or the results of institutional

audits). Without this data, the evaluation of the effectiveness of compliance of companies and health institutions with confidentiality regulations remains qualitative and descriptive.

4. Generalization of Institutional Conditions:
   The discussion in this study assumes similar operational barriers, such as weak cybersecurity, lack of training, and overlapping regulations between agencies. However, organizational capacity and compliance levels can vary greatly between large corporate hospitals and small-scale work clinics, so some generalizations may not be accurate.
5. Limited Comparative Legal Analysis:
   Although this study refers to international frameworks such as *the General Data Protection Regulation (GDPR)* and *the Health Insurance Portability and Accountability Act (HIPAA)* as contextual comparisons, this study does not systematically analyze its relevance or application to the legal culture or law enforcement environment in Indonesia. This limits the ability of research to propose adaptation of global best practices that are appropriate to the national context.
6. Incomplete Evaluation of Enforcement Mechanisms:
   This study identifies gaps in administrative, criminal, and ethical enforcement, but has not conducted an in-depth examination of institutional capacity, such as the role of supervisory institutions, data protection authorities, or *the disciplinary process of MKDKI.* As a result, the degree of enforcement of sanctions practically cannot be assessed comprehensively.
7. Temporal Limitations and Policies:
   Given that *the Personal Data Protection Law (Law No. 27 of 2022)* in Indonesia is still in the early stages of implementation, many derivative regulations and law enforcement structures are still in the process of development. These temporal limitations limit the ability of research to assess the long-term effectiveness or consistency of legal application in protecting the confidentiality of *Medical Check-Up (MCU) data*.

## 4. CONCLUSION

The results of this study conclude that Indonesia has established a strong normative framework to protect the confidentiality of results *Medical Check-Up (MCU)* employees through *Health Law*, *Manpower Law*and *Personal Data Protection Law*. These regulations recognize MCU results as specific personal data that must be protected from unauthorized access or disclosure, in order to ensure the privacy of employees in industrial relations. However, the practical implementation of such protection is still inconsistent due to overlapping legal norms, limited institutional capacity, weak cybersecurity systems, and lack of regulatory coordination. Thus, the effectiveness of MCU confidentiality protection does not only depend on the existence of regulations, but also on the operational readiness and commitment of public and private institutions in enforcing them effectively.

In addition, this study confirms that the protection of medical data privacy is an integral component of fair and ethical industrial relations. Employers must ensure that MCU data is used solely for administrative and occupational health purposes, not for discriminatory employment decisions. On the other hand, the government needs to strengthen supervision, law enforcement, and public awareness to ensure compliance with data protection obligations. Comparative insights from international frameworks such as *General Data Protection Regulation (GDPR)* and *Health Insurance Portability and Accountability Act (HIPAA)* affirms the importance of the principle of transparency, consent (*Agree*), and accountability in the management of employee medical data. Therefore, the comprehensive and consistent application of these principles is essential to uphold justice, trust, and ethical governance in the industrial environment in Indonesia.

The implications of this study highlight the need to strengthen regulatory enforcement, institutional coordination, and cybersecurity mechanisms to ensure effective protection of MCU secrecy. Further research is recommended to conduct an empirical assessment of how companies and healthcare institutions apply data privacy laws in practice, including employee perceptions and their level of compliance. Additionally, it is important to explore judicial interpretations and case studies

related to MCU confidentiality violations to bridge the gap between legal doctrine and enforcement reality. The expansion of comparative analysis with international data protection regimes will also enrich legal reform efforts in Indonesia. Overall, future research should focus on strengthening practical solutions, policy alignment, and cross-sectoral cooperation to improve the protection of medical data privacy in industrial relations.

**REFERENCES**

AOHN. (2022). *Confidentiality of medical records and worker health information in the occupational health setting* (Position Statement).

Enqvist, L., & Litins'ka, Y. (2022). Employee health data in European law: Privacy is (not) an option? *Nordic Journal of European Law, 2022*(1).

Jafar, F. H. (2020). Legal protection regarding medical record of prospective workers in job recruitment health test. [Nama Jurnal Tidak Diketahui], [Volume/Nomor Tidak Diketahui], 77.

Julia, F., & Aulianto, D. R. (2025). Focused analysis of Article 29 of Indonesian Minister of Health Regulation No. 24/2022: Data security implementation of electronic medical records at Sindangwangi Health Center, Pangandaran, West Java. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan, 11*(1). https://doi.org/10.14710/lenpust.v11i1.70518

Mahameru, D. E., Nurhalizah, A., Wildan, A., Badjeber, M. H., & Rahmadia, M. H. (2023). Implementasi UU perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. *Jurnal Esensi Hukum, 5*(2). https://journal.upnvj.ac.id/index.php/esensihukum/index

Marwiyah. (2022). Analysis of legal review of medical information release to ensure the confidentiality of patient identity. *Awang Long Law Review, 4*(2), 326–330.

Muñiz, J. F.-C. (2025). Medical test and employee's autonomy. Confidentiality of data and non-discrimination. *Bioethics, 39*, 475–481. https://doi.org/10.1111/bioe.13384

Pradana, Y. A., & Silalahi, W. (2024). Implementasi dan tantangan regulasi perlindungan data pribadi pasien di era digital pada rumah sakit. *Rewang Rencang: Jurnal Hukum Lex Generalis, 5*(12). https://jhlg.rewangrencang.com/

Pratiwi, A. B., Padmawati, R. S., & Willems, D. L. (2022). Behind open doors: Patient privacy and the impact of design in primary health care, a qualitative study in Indonesia. *Frontiers in Medicine, 9*, Artikel 915237. https://doi.org/10.3389/fmed.2022.915237

Putra, I. K. U., Kuswardhani, T., & Purwani, S. P. M. E. (2024). Analysis of patient rights protection through medical record confidentiality and information disclosure system in Indonesian hospitals. *JOURNAL LA SOCIALE, 5*(02), 539–549. https://doi.org/10.37899/journal-la-sociale.v5i2.1141

Putri, N. M. D. G., Mahendrawati, N. L. M., & Ujianti, N. M. P. (2024). Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Preferensi Hukum, 5*(2), 240–245. https://doi.org/10.22225/jph.5.2.2024.240-245

Santhi, N. N. P. P. (2025). Patient data privacy challenges in electronic health systems: A juridical analysis of medical information protection in Indonesia. *West Science Law and Human Rights, 3*(01), 1–8.

Sari, P. K., Prasetio, A., Candiwan, Handayani, P. W., Hidayanto, A. N., Syauqina, S., Astuti, E. F., & Tallei, F. P. (2021). Information security cultural differences among health care facilities in Indonesia. *Heliyon, 7*, e07248. https://doi.org/10.1016/j.heliyon.2021.e07248

Sudra, R. I., Putra, S., & Hartini, I. (2022). Legal protection of the patient's right to access medical records in Indonesia (Original research). *SEEJPH*. https://doi.org/10.11576/seejph-5325

Tombokan, C. D., Rumengan, H. Y., & Kaligis, R. Y. J. (2024). Perlindungan hukum terhadap kerahasiaan data pasien dalam aplikasi layanan kesehatan online yang disalahgunakan. *Lex Privatum*, *14*(4).