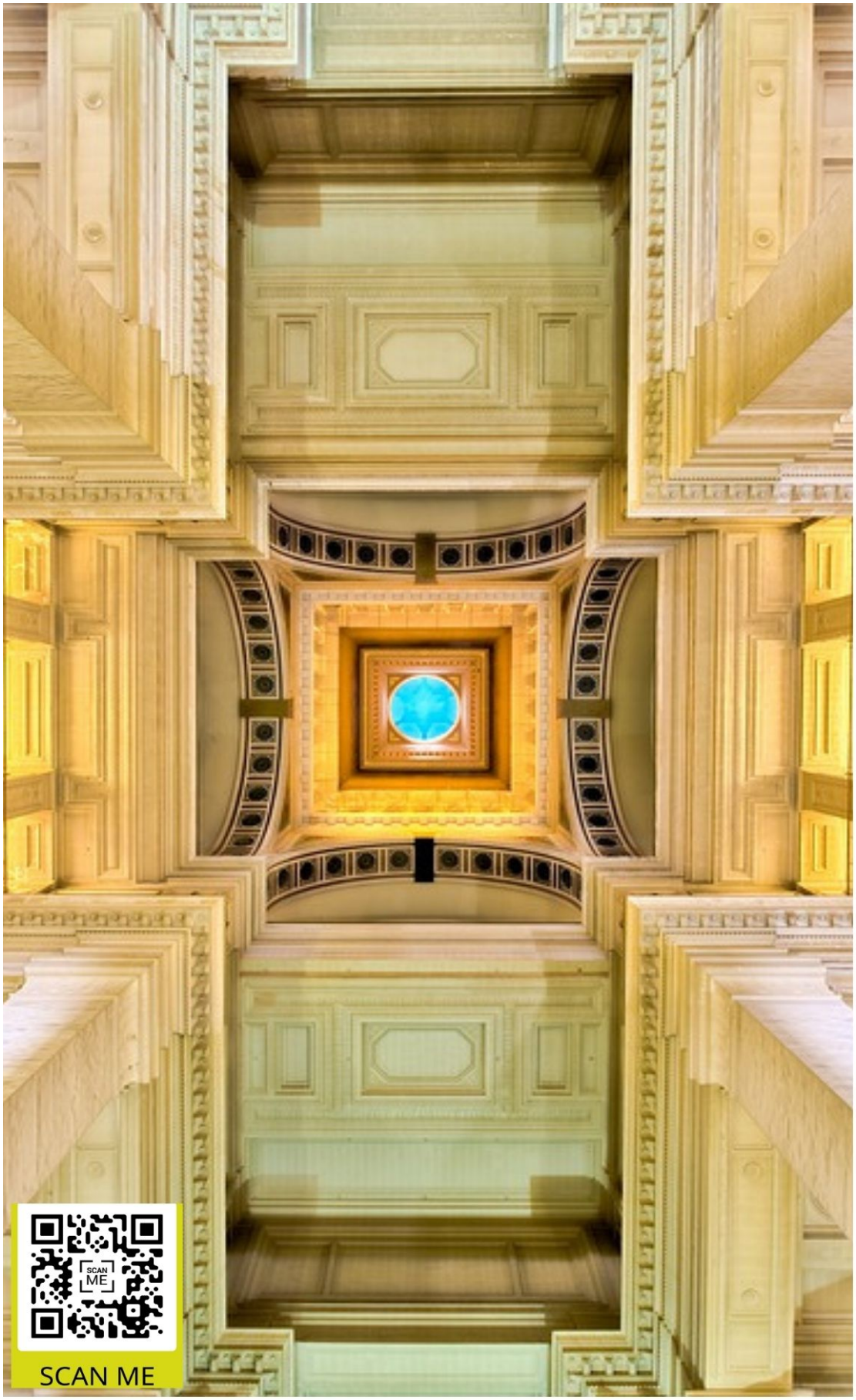
Rechtsidee

Vol. 14 No. 1 (2026): June



RECHTSIDEE

PUBLISHED BY
UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

ISSN 2443-3497
(online)

Rechtsidee

Vol. 14 No. 1 (2026): June

Table Of Contents

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Rechtsidee

Vol. 14 No. 1 (2026): June

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Rechtsidee

Vol. 14 No. 1 (2026): June

EDITORIAL TEAM

Editor in Chief

Mochammad Tanzil Multazam, Universitas Muhammadiyah Sidoarjo, Indonesia
Scopus ID: 57200559335
Researcher ID: A-2135-2016
ORCID: 0000-0002-6373-1199

Managing Editor

Dr. Rifqi Ridlo Phahlevy, Universitas Muhammadiyah Sidoarjo, Indonesia
Scopus ID: 57205880567
ORCID: 0000-0002-6684-1190

Editorial Board

Regional Editor for Central Asia

Saydaxmedov Umid Murodovich, Associate Professor of Economic Law, Higher School of Judges under the Supreme Council of Judges of the Republic of Uzbekistan [Google Scholar]

Esanov Azamat Esirgapovich, Tashkent State University of Law, Uzbekistan [Scopus]

Dametken Medikhanovna Turekulova, Esil University, Kazakhstan [Scopus]

Regional Editor for Asia Pacific

Faizal Kurniawan, Universitas Airlangga, Indonesia [Google Scholar] [Scopus]

M. Zulfa Aulia, Universitas Jambi, Indonesia [Google Scholar] [Scopus]

Fradhana Putra Disantara, Institut Teknologi Bisnis Yadika, Indonesia [Google Scholar] [Scopus]

Dr. Noor Fatimah Mediawati, Universitas Muhammadiyah Sidoarjo, Indonesia [Google Scholar] [Scopus]

Regional Editor for America

Dinara F. Abdunayimova, University of Illinois College of Law, USA [Google Scholar]

Regional Editor for Middle East

(No data provided)

Complete list of editorial team (link)

Complete list of indexing services for this journal (link)

How to submit to this journal (link)

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Rechtsidee

Vol. 14 No. 1 (2026): June

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Rechtsidee

Vol. 14 No. 1 (2026): June

Health Data Protection Gaps in Indonesia and Romania

Ruth Maria Angelina Hutapea, ruthmariaangelina@gmail.com (*)

Universitas Brawijaya, Malang., Indonesia

Reka Dewantara , rainerfh@ub.ac.id

Fakultas Hukum, Universitas Brawijaya, Malang, Indonesia, Indonesia

Patricia Audrey Ruslijanto, patricia@ub.ac.id

Fakultas Hukum, Universitas Brawijaya, Malang, Indonesia, Indonesia

(*) Corresponding author

Abstract

General Background: The rapid digitalization of healthcare services after COVID-19 has expanded health data processing and increased privacy breach risks. **Specific Background:** Indonesia and Romania have developed comprehensive legal frameworks through the Indonesian Personal Data Protection Law, Health Law, GDPR, and Lege nr. 190/2018, yet both jurisdictions still face difficulties in protecting sensitive health information. **Knowledge Gap:** Existing studies have not sufficiently compared post-pandemic health data protection in Indonesia and Romania by examining supervisory institutions, law enforcement mechanisms, and the gap between legal norms and empirical implementation. **Aims:** This study analyzes and compares the regulation, enforcement mechanisms, supervisory capacity, and institutional governance of health data protection in Indonesia and Romania. **Results:** The findings show that both countries possess adequate normative frameworks but experience enforcement gaps caused by institutional weaknesses, inconsistent supervision, fragmented sectoral coordination, limited technical readiness, and weak compliance culture in healthcare institutions. Indonesia faces a critical institutional void because the independent data protection authority is not yet fully operational, while Romania faces selective and passive enforcement by ANSPDCP toward public healthcare institutions. **Novelty:** This study offers a comparative model that links regulatory design, health data governance, supervisory capacity, and institutional compliance in two distinct legal regimes: Indonesia's national data sovereignty model and Romania's GDPR-based free data flow model. **Implications:** Effective health data protection requires independent supervisory authorities, privacy by design, accessible dispute resolution, harmonized sectoral regulation, and sustainable institutional compliance culture.

Published date: 2026-06-08

I. Introduction

The global digitization of healthcare services has fundamentally transformed medical governance, with electronic health records, telemedicine, and app-based health platforms becoming critical infrastructure that is inseparable from modern healthcare systems[1] . The unique characteristics of health data lie in its irreversible nature—it is sensitive, permanent, and lifelong—meaning that a breach exposes long-term, irreparable identity vulnerabilities[2] . Unlike financial data, which can be altered or reversed following a breach, health data requires a qualitatively stricter protection regime. Article 9(1) of the General Data Protection Regulation (GDPR) (EU) 2016/679 explicitly prohibits the processing of health data unless limited exceptions are met, reflecting supranational recognition of the high risk to the fundamental rights of data subjects. The GDPR establishes a risk-based approach to health data protection, under which processing is permitted only if grounded in one of the legitimate grounds listed in Article 9(2), such as explicit consent or the necessity of healthcare services[3] .

The acceleration of digital transformation during the COVID-19 pandemic triggered a surge in cyber data breaches in the global healthcare sector[4] . This situation was exacerbated by a shortage of cybersecurity personnel and the adoption of remote work in medical institutions that were not yet infrastructure-ready[5] . This phenomenon occurred in parallel with the rushed, massive implementation of contact tracing apps and digital vaccination certificates, resulting in technological innovation outpacing legal readiness and technical mitigation measures[6] . In Indonesia, a fragmented legal framework has proven ineffective in protecting health data. This is evident in the data breach involving 1.3 million users of the older version of the *electronic Health Alert Card* (eHAC) system due to a failure in open-server security protocols[7] . A similar incident occurred in Romania in February 2024 when a massive *ransomware* attack paralyzed the Integrated Hospital Information System (*Hipocrate*) in over 20 hospitals[8] . The Romanian case demonstrates that the maturity of supranational regulations does not automatically guarantee empirical security. Both events highlight *an enforcement gap* between normative regulations and the reality of governance on the ground, serving as a critical starting point for evaluating the effectiveness of post-pandemic laws.

Indonesia has ushered in a new era of personal data protection through the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). Article 4(2) of the PDP Law explicitly classifies health data as a specific category of personal data, alongside biometric and genetic data, requiring a high level of protection. Through a categorical protection approach, the lawmakers placed health data in a special classification requiring stricter supervision than general personal data[9] . However, cyber mitigation failures during the pandemic—including the exposure of the President of the Republic of Indonesia's vaccination certificate data on the public search feature of the PeduliLindungi app—indicate that legal instruments do not automatically close systemic vulnerabilities[10] . Moreover, the Personal Data Protection Enforcement Agency, as an independent supervisory authority, is still in the transitional phase of establishment by the President. The existence of technical implementing regulations that have begun to be enacted has not yet been able to eliminate this critical institutional void. These normative and factual gaps demonstrate that the "ideal state" (das Sollen) has not yet fully materialized into the "actual state" (das Sein) due to the supervisory agency not yet being operational on the ground.

As a member state of the European Union, Romania is directly subject to the GDPR, which has been harmonized domestically through Law No. 190 of 2018 (*Lege nr. 190/2018*). Article 32 of the GDPR requires data controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including periodic security assessments. Based on the principle of accountability, compliance with the GDPR must not be merely a formality but must be demonstrated through ongoing documentation and technical procedures. The 2024 *ransomware* attack on the *Hipocrate* system, which paralyzed services at dozens of hospitals in Romania, clearly violated Article 32(1)(b) of the GDPR due to a failure to maintain the confidentiality, integrity, availability, and resilience of the system. On the other hand, the Romanian National Supervisory Authority for Personal Data Processing (*Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* – ANSPDCP) tends to be passive in enforcing compliance in the public sector, although it remains aggressive in imposing fines on private service providers[11] . This reality is exacerbated by a gap in clinical competence, where healthcare professionals in Romania tend to understand the theoretical aspects of patient *consent* but fail to apply GDPR technical protocols in their daily clinical practice[12] .

A comparison between Indonesia and Romania is relevant for assessing the effectiveness of post-COVID-19 health data protection enforcement. The two countries represent two distinct regulatory models: a national legislative model through the Personal Data Protection Act (PDP) and the Health Act in Indonesia, and a supranational harmonization model through the GDPR in Romania. These differences are also reflected in data flow policies, where Indonesia adopts a health data localization approach through Article 137 of Law No. 17 of 2023 on Health in conjunction with Government Regulation No. 28 of 2024, while Romania follows the principle of free flow of data within the framework of the European Union's Single Digital Market. Nevertheless, both countries face relatively similar challenges regarding the limited effectiveness of supervisory agencies in ensuring public sector compliance with data protection obligations. Therefore, this study aims to analyze the effectiveness of health data protection enforcement through a comparative study of Indonesia and Romania to identify the relationship between regulatory design, data governance models, and the institutional capacity of supervisory agencies in ensuring the protection of patients' privacy rights.

Research on health data protection has been conducted by several researchers with diverse focuses. Eka N.A.M. Sihombing et al., in *the *Veteran Law Review**, analyzed the legal protection of COVID-19 patient data in Indonesia and found that the regulations in effect during the pandemic remain sector-specific and do not yet provide adequate legal certainty for data subjects[13] . Dona Budi Kharisma and Alvalerie Diakanza, in *the International Journal of Human Rights in Healthcare*, compared patient data protection regimes in Indonesia, Singapore, and the European Union, concluding that the EU's legal framework offers a more comprehensive level of protection compared to Indonesia[14] . Meanwhile, Cristian Constantin

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Francu and Stefan Sava in *the Proceedings of the International Conference on Business Excellence* highlight the development of data and artificial intelligence regulations in Romania within the context of the healthcare sector's digital transformation, and demonstrate that the existence of the GDPR does not yet fully guarantee the effectiveness of data protection at the implementation level15 . Nevertheless, these three studies still have limitations because they have not specifically compared the effectiveness of health data protection between Indonesia following the enactment of Law No. 27 of 2022 on Personal Data Protection and Romania as an EU member state implementing the GDPR, particularly by focusing on the role of supervisory authorities, enforcement mechanisms, and the gap between normative regulations and empirical practices in the healthcare sector.

The novelty of this study lies in its comparative analysis, which not only compares the substance of health data protection regulations but also evaluates the effectiveness of law enforcement and the institutional capacity of supervisory bodies within two distinct legal regime models: the *"sovereign lex"* model based on data localization in Indonesia and the *"harmonized lex"* model based on *the free flow of data* under the GDPR framework in Romania. Unlike previous studies, which generally focused on the normative aspects of data protection or mere regulatory comparisons, this study integrates administrative law analysis, health data governance, and institutional effectiveness to identify the relationship between regulatory design and the implementation of health data protection in the public sector. Thus, this study offers a more comprehensive approach to assessing the success of a health data protection regime through indicators of legal framework, enforcement mechanisms, and the performance of supervisory institutions. The objective of this study is to analyze and compare the legal frameworks and enforcement mechanisms for health data protection in Indonesia based on Law No. 27 of 2022 on Personal Data Protection and Law No. 17 of 2023 on Health with Romania's legal system based on the General Data Protection Regulation (GDPR) and Law No. 190/2018. Furthermore, this study aims to evaluate the effectiveness of supervisory bodies and enforcement mechanisms in both countries and to formulate a model for institutional strengthening capable of narrowing the gap between normative regulations and empirical implementation in health data protection.

II. Method

This study is a normative legal study focusing on the analysis of health data protection regulations and law enforcement within the legal systems of Indonesia and Romania following the digital transformation of the health sector. A normative legal study was chosen because the primary objects of this research are legal norms, legal principles, and legal policies governing health data protection in both jurisdictions. The approaches used are the comparative approach and the conceptual approach. The comparative approach is used to compare the regulations and enforcement mechanisms for health data protection in Indonesia and Romania, while the conceptual approach is used to examine the concepts of personal data protection, the right to privacy, data sovereignty, the free flow of data, and the effectiveness of law enforcement in modern legal states. Through these two approaches, this study seeks to identify the similarities, differences, strengths, and weaknesses of each legal system in providing protection for health data.

The legal materials used in this study consist of primary, secondary, and tertiary legal sources. Primary legal sources include Law No. 27 of 2022 on Personal Data Protection, Law No. 17 of 2023 on Health, Government Regulation No. 28 of 2024, Regulation (EU) 2016/679 or the General Data Protection Regulation (GDPR), and Law No. 190/2018 as the implementing instrument of the GDPR in Romania. Secondary legal materials consist of legal textbooks, articles from reputable international journals, research findings, and academic literature discussing personal data protection, cybersecurity in the health sector, and the effectiveness of data protection supervisory agencies. Tertiary legal materials include legal dictionaries, legal encyclopedias, glossaries of information technology terms, and other reference sources used to clarify concepts and terminology relevant to the research.

The legal materials were processed through the stages of inventory, identification, classification, and systematization based on the study's focus on health data protection regulations and the effectiveness of their enforcement. All collected legal materials were then grouped into main themes: regulatory frameworks, enforcement mechanisms, the authority of supervisory agencies, and health data governance in Indonesia and Romania. The legal materials were analyzed qualitatively by examining the relationship between legal norms, data protection principles, and their implementation in the practice of providing digital health services. Comparative analysis was used to identify similarities and differences between the data localization-based health data protection model in Indonesia and the free flow of data-based protection model under the GDPR regime in Romania. Conclusions were drawn using deductive reasoning to formulate legal arguments and institutional strengthening models that can enhance the effectiveness of health data protection in both countries.

III. Results and Discussion

The theory of the inner morality of law, proposed by Lon L. Fuller in his work *The Morality of Law* (1964), offers eight principles that must be met for a legal system to possess legitimate internal morality. These eight principles include generality, publicity, non-retroactivity, clarity, non-contradiction, practicability, constancy, and congruence16 . The principle of congruence requires consistency between the norms established and the enforcement practices carried out by state authorities17 . The absence of congruence undermines the legitimacy of the law because rules that are formally sound are not implemented in practice. The COVID-19 pandemic has forced the acceleration of the digitalization of health services in Indonesia and Romania, yet this acceleration has not been matched by the readiness of legal infrastructure and regulatory institutions. When a country has progressive regulations but lacks effective regulatory institutions, the law loses some of its practical legitimacy.

Establishing the protection of health data as a fundamental right carries the normative consequence that the state has a

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

negative obligation not to interfere with the right to privacy, as well as a positive obligation to build a protective legal ecosystem and cyber infrastructure. In Indonesia, this is regulated in Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, which explicitly guarantees every person's right to protection of their personal self, family, honor, dignity, and property—a provision that, by interpretation, encompasses the right to health data privacy. Meanwhile, in the European Union's legal system, a similar right is guaranteed more explicitly through Article 8 of the Charter of Fundamental Rights of the European Union, which states that everyone has the right to the protection of personal data concerning them. In the post-pandemic digital era, this positive obligation of the state is tested by the reality of massive data breaches occurring precisely when the healthcare system is most reliant on digital infrastructure. The state's failure to provide effective enforcement mechanisms can be classified as a violation of the data subject's constitutional rights18 , as data subjects lose control over their health information, which is permanent and irreversible. Therefore, the standard for objectively evaluating the performance of cyber regulations in both countries must measure the extent to which these positive obligations are fulfilled through the availability of independent oversight bodies and accessible redress mechanisms.

Health data protection in Indonesia has a normative foundation through Law No. 27 of 2022 on Personal Data Protection (PDP Law). Article 4(2) of the PDP Act states that "Specific Personal Data includes: a. health data and information; b. biometric data; c. genetic data; d. criminal records; e. children's data; f. personal financial data; and/or g. other data as provided by applicable laws and regulations." The classification of health data into the specific category carries legal consequences, meaning that its processing requires a stronger legal basis compared to general personal data. This is as stipulated in Article 20 of the Personal Data Protection Act (PDP Act), which mandates that data controllers must have a processing basis that includes "explicit and valid consent from the Data Subject for one or more specific processing purposes that have been communicated by the Data Controller to the Data Subject." This provision incorporates the crucial principle of *explicit consent,* given that health platforms such as PeduliLindungi and SATUSEHAT collect health data on a massive scale without always seeking consent that meets the standards of informed consent19 . The Personal Data Protection Law adopts the principle *of informational self-determination*; however, its effectiveness heavily depends on the existence of oversight mechanisms that can ensure the consent given is genuinely valid and not overridden by the state's administrative interests during a public health emergency.

As *a lex specialis* in the health sector, Law No. 17 of 2023 on Health regulates the protection of medical data in a more technical manner through provisions on electronic medical records and integration into the SATUSEHAT platform . Article 137 of the Health Law mandates that "every medical and health worker providing health services is obligated to create medical records" and that "the Central Government and Regional Governments shall establish a nationally integrated health information system" based on the principle that "health data storage must be conducted domestically." This data localization requirement, which is also technically reinforced in Government Regulation No. 28 of 2024, reflects a data sovereignty policy that fundamentally distinguishes Indonesia from Romania's approach, which adheres to the principle of the free flow of data within the European Union framework. Article 296(1) of the Health Law reaffirms the duty of confidentiality by stating that "every medical and health professional providing health services is obligated to maintain patient health confidentiality, which is embodied in the form of medical confidentiality." The intersection between the Personal Data Protection Act (PDP Act) as *the lex generalis* and the Health Act as *the lex specialis* creates a layered regulatory architecture that has the potential to cause overlapping jurisdictions if inter-agency harmonization mechanisms are not systematically designed.

The transformation of medical records from physical files to encrypted digital data through the integration of Application Programming Interface (API) systems within SATUSEHAT—the National Health Information System—creates a massive national health data repository20 . Article 25 of the GDPR on data protection by design and by default emphasizes that protection must be built into the system's design from the outset, rather than implemented after an incident occurs. Therefore, implementing regulations in Indonesia must specify minimum technical requirements and audit obligations for the National Health Information System (SIKN). Without binding technical provisions, large-scale integration could exacerbate the risk of mass data breaches.

The enforcement mechanisms under the Personal Data Protection Act (PDP Act) are structured into three tiers of sanctions that are, by definition, punitive in nature: administrative sanctions, criminal penalties for individuals, and criminal penalties for corporations. Article 67(2) of the PDP Act provides that "any person who intentionally and unlawfully discloses Personal Data that does not belong to them shall be punished by imprisonment for a maximum of 4 (four) years and/or a fine of up to Rp4,000,000,000.00 (four billion rupiah)." Additionally, Article 70 of the PDP Act establishes corporate criminal penalties in the form of fines up to 10 times the maximum individual fine, accompanied by additional sanctions ranging from the suspension of business operations to the dissolution of the corporation. The COVID-19 pandemic demonstrated that the lack of integrated cybersecurity preparedness led to the exposure of 1.3 million records of old eHAC users and the vaccination certificate of the President of the Republic of Indonesia due to a security flaw in the open server at7 . The post-pandemic shift in legal paradigms has driven the accelerated enactment of the Personal Data Protection Law (PDP Law) in 2022; however, the effectiveness of its enforcement is hindered by institutional issues, as the Personal Data Protection Enforcement Agency—the independent supervisory authority—remains in the transitional phase of establishment by the President21 . According to Fuller's theory, this situation reflects a failure of the principle of congruence because the state has formulated positive law (*das Sollen*) but has not yet established an independent administrative law enforcement apparatus to implement it on the ground (*das Sein*), resulting in a critical institutional void during the institutional transition phase.

Unlike Indonesia's approach of building a data protection regime within the national legal system, Romania operates within a uniform supranational framework that applies directly through the General Data Protection Regulation (GDPR) or Regulation (EU) 2016/679. Article 9(1) of the GDPR establishes the fundamental prohibition principle (prohibition by

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

default) by stating that “the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.” Violations of Article 9 are subject to sanctions as set forth in Article 83(5), which stipulates that such violations “shall be subject to administrative fines of up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.” Article 35 of the GDPR also emphasizes preventive mechanisms through the *Data Protection Impact Assessment* (DPIA) process, as well as the principles *of data protection by design and by default* in Article 25 of the GDPR. This regulatory framework is more robust compared to Article 34 of Indonesia’s Personal Data Protection Law, which lacks equivalent technical guidelines.

Romania adopted *Law No. 190/2018 on Measures for the Implementation of Regulation* (EU) 2016/679 (Law No. 190 of 2018 on Measures for the Implementation of the GDPR) as a national instrument that aligns supranational regulations with domestic administrative governance. Article 3 of the law states that "*the processing of genetic, biometric, or health data, for the purpose of automated decision-making or profiling, is permitted only with the explicit consent of the data subject*," meaning that the processing of genetic, biometric, or health data for the purpose of automated decision-making or profiling is permitted only with the explicit consent of the data subject. The data protection supervisory authority in Romania is *the Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (ANSPDCP), which has the authority to monitor compliance, receive complaints, conduct investigations, and impose administrative sanctions independently22 . The acceleration of medical digitization in the European Union is driving the transformation of Romania’s healthcare services toward cross-border digital connectivity (*cross-border data flow*) among member states. However, the contact tracing app and the European Union’s COVID-19 digital certificate system ( ) actually expand *the attack surface* against clinical databases23 .

Data protection implementation in Romania’s healthcare sector faces enforcement deficits similar to those in Indonesia. When a massive ransomware attack crippled the Integrated Hospital Information System (Hipocrate) databases in over 20 hospitals in 2024, the ANSPDCP tended to remain passive and did not impose significant sanctions on the public sector. This incident reflects a violation of the obligations under Article 32(1)(d) of the GDPR, which requires that “the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, inter alia: (d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.” This reality is exacerbated by the varying levels of technical understanding of the GDPR among Romanian healthcare workers, coupled with competency gaps in implementing daily technical protocols for handling data breach incidents. Post-pandemic policy implications in Romania indicate that the pressures of the pandemic exposed structural weaknesses that cannot be addressed solely by the existence of sophisticated supranational regulations. This situation suggests that the issue of post-pandemic health data protection no longer lies at the level of normative law, but rather in structural implementation capacity and an institutional compliance culture that remains underdeveloped.

Table 1. Post-COVID-19 Digital Health Data Protection Regulations and Mechanisms in Indonesia and Romania

Dimensions of Comparison	Faculty	Program
Legal Basis	Law No. 27/2022 (PDP Law) + Law No. 17/2023 (Health Law): independent, multi-layered national regulations	GDPR Regulation (EU) 2016/679 + Act No. 190/2018: a supranational framework that is *self-executing*
Status of Health Data	Specific personal data (Article 4(2) of the Personal Data Protection Act): requires a stronger legal basis for processing	Special categories prohibited (Article 9(1) of the GDPR): limited exceptions
Sanction Regime	4–6 years’ imprisonment + a fine of IDR 4–6 billion (Article 67 of the PDP Law); corporate fines of up to 10 times the amount (Article 70 of the PDP Law)	Administrative fines of up to €20 million or 4% of global turnover (Article 83(5) of the GDPR): proportional and scale-based
Supervisory Authority	Data Protection Authority not yet established; interim oversight by Komdigi creates *an institutional void*	Selective and passive enforcement against the public sector by ANSPDCP
Effectiveness of Protection	Deficit in *certainty* and *celerity*: no precedent for formal sanctions following the PDP Law’s enactment	Deficit of *certainty*: authority exists but is not

Source: Author

Indonesia and Romania both adopt an approach aimed at creating a deterrence effect against health data breaches. The difference lies in the design of the sanctions used, where the GDPR prioritizes administrative sanctions based on a percentage of annual turnover as stipulated in Article 83(5) of the GDPR, while Indonesia’s Personal Data Protection Law combines administrative sanctions with criminal penalties of imprisonment and nominal fines. In legal enforcement theory, the effectiveness of sanctions is determined by three main elements: certainty (the certainty of imposing sanctions), severity (the severity of the punishment), and celerity (the speed of enforcing sanctions). These three elements have not been optimally fulfilled in either country because Indonesia still faces issues regarding the certainty of enforcement due to the lack of an operational independent supervisory body, while Romania faces issues regarding the certainty and speed of enforcement due to the ANSPDCP’s relatively passive stance toward violations in the public sector. Therefore, the effectiveness of health data protection is determined not only by the severity of the threat of sanctions, but also by the

consistency and courage of supervisory institutions in exercising their authority.

The most fundamental structural similarity between Indonesia and Romania is the gap between legal formalism and enforcement realities in the post-pandemic digital era. Both jurisdictions possess adequate textual normative instruments to protect data subjects' medical data, yet exhibit deficits in the enforcement dimension. In Indonesia, the issue lies in the Data Protection Agency (Lembaga PDP) not yet operating independently, while in Romania, it lies in the passivity of the National Authority for the Protection and Supervision of Personal Data (ANSPDCP) regarding violations in the public sector. Philippe Nonet and Philip Selznick, through the concept of responsive law, state that effective law is not merely law with a complete body of norms, but law that is capable of responding to social needs in an adaptive manner. In the context of post-pandemic health digitalization, adaptive social needs include the ability of supervisory authorities to protect citizens from the permanent and irreversible exploitation of health data. Both Indonesia and Romania remain stuck in a transitional phase toward responsive law in health data governance, as neither has yet been able to bridge the gap between enacted legal norms and fair enforcement practices.

The fundamental difference between the two systems lies in the sources of legitimacy and regulatory harmonization mechanisms, which directly impact readiness to face the challenges of post-pandemic health digitalization. Indonesia builds its data protection system independently (bottom-up) through a national legislative process that is prone to sectoral fragmentation, as reflected in the potential for dual coordination between the Personal Data Protection Act (PDP Act) and the Health Act. Conversely, Romania adopts protection standards from outside (top-down) through the GDPR, which applies directly without requiring a national transposition process, thereby ensuring greater consistency in minimum standards for protecting patient rights. The supranational GDPR model offers the advantage of universal cross-border legal certainty, which is critically needed in an era where the flow of health data transcends territorial boundaries due to cross-border telemedicine. However, this supranational model may lack flexibility regarding local administrative needs, while Indonesia's national model is more adaptive to domestic interests but vulnerable to regulatory fragmentation and delays in institutional strengthening.

1. **Regulations and Law Enforcement Mechanisms for Health Data Protection in Indonesia and Romania Post-COVID-19**
2. **The Effectiveness of Health Data Protection Mechanisms and Institutional Strengthening Models for Indonesia and Romania**

The effectiveness of health data protection cannot be measured solely by the existence of legal norms; rather, it must be evaluated based on the ability of those norms to generate compliance and prevent violations in practice. The deterrence theory developed by Cesare Beccaria in *On Crimes and Punishments* (1764) and expanded upon by Jeremy Bentham identifies three key elements determining the effectiveness of legal sanctions: certainty that every violation will be prosecuted, the severity of the punishment, and the speed of sanction enforcement (celerity)24 . This theory is based on the assumption that individuals will tend to comply with the law if there is certainty that every violation will be detected and punished. Indonesia exhibits deficits in the aspects of certainty and celerity due to supervisory authorities that are not yet fully operational and sanction imposition procedures that have not yet been established in a stable manner. Romania, despite having a well-established supervisory authority (ANSPDCP), faces a certainty deficit due to an enforcement approach that tends to be passive and reluctant to exercise its repressive powers against public sector institutions, including government hospitals. Both jurisdictions reflect enforcement gaps that directly undermine the deterrent effect of the health data protection system.

In *Law and Society in Transition: Toward Responsive Law* (1978), Philippe Nonet and Philip Selznick divide the evolution of law into three types: repressive law, which is oriented toward the legitimization of power; autonomous law, which promises certainty through rigid institutional order; and responsive law, which prioritizes flexibility and substantive justice in responding to the dynamics of social change25 . Based on this typology, Indonesia's current health data protection system is in a transitional phase toward autonomous law. This is because formal norms in positive law are already in place, but their enforcement remains interim and dependent on transitional coordination among ministries. On the other hand, Romania is formally established in the realm of autonomous law thanks to the adoption of the supranational GDPR, but has not yet fully achieved responsive legal standards in healthcare governance due to selective and discriminatory enforcement of sanctions against private actors compared to public actors. It is this gap between the normative position of regulatory maturity and the factual reality that poses a challenge to the effectiveness of patient privacy protection in the post-pandemic digital era, where technological acceleration outpaces institutional capacity.

Normatively, Indonesia has established a layered and comprehensive legal architecture for health data protection in the post-pandemic era. The Personal Data Protection Act (PDP Act) serves as *the lex generalis* through Article 4(2), which classifies health data and information as specific personal data, while Law No. 17 of 2023 on Health reinforces this at the sectoral level as *the lex specialis* through Article 296 on the obligation to maintain medical confidentiality and Article 137 on the implementation of a nationally integrated health information system. The technical framework for digitalization is regulated by Minister of Health Regulation No. 24 of 2022, which mandates that all healthcare facilities adopt Electronic Medical Records (EMR) and integrate them with the SATUSEHAT Platform under the oversight of Government Regulation No. 28 of 2024. Textually, this framework is highly comprehensive and on par with international standards, reflecting the legislature's rapid response ( ) to the COVID-19 pandemic stress test, which previously exposed the vulnerabilities of the eHAC system. However, in practice, the system's effectiveness is paralyzed by three factors: the Personal Data Protection Enforcement Agency mandated by Article 58 of the Personal Data Protection Law has not yet been established as an operationally independent entity; although technical regulations on sanctions have been enacted via Government Regulation No. 20 of 2024, their implementation remains provisionally fragmented under the Ministry of Communication and Digital Affairs

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

alongside the Ministry of Health; There is a disparity in the technological readiness of health facilities across regions in implementing uniform data security standards.

The combination of these factors results in a “deficiency of congruence” within the framework of Lon L. Fuller’s theory of the “inner morality of law,” where norms have been legally declared but an independent administrative law enforcement apparatus is not yet available to implement them[26] . This inconsistency in enforcement is evident in the absence of precedents for the imposition of administrative sanctions against public health institutions for post-pandemic medical data breaches that materially constitute violations of administrative law since the Personal Data Protection Act (PDP Act) came into full effect. Article 67(2) of the PDP Act states that “any person who intentionally and unlawfully discloses Personal Data that does not belong to them shall be punished by imprisonment for a maximum of 4 (four) years and/or a fine of up to Rp4,000,000,000.00 (four billion rupiah),” however, this threat loses its sociological impact without the certainty of enforcement. The lack of enforcement precedents weakens the compliance signal for data controllers in the medical sector, which in turn reduces the level of voluntary compliance. Based on the principles of deterrence theory, the aspect of certainty is far more decisive for compliance than the severity of sanctions; thus, the phenomenon of severe penalties without enforcement certainty has proven ineffective in driving institutional compliance within Indonesia’s digital health sector.

Unlike Indonesia, Romania faces a paradox in the form of a strong legal framework that is not yet fully supported by consistent enforcement. As an EU member state, Romania is subject to the General Data Protection Regulation (GDPR), which is *directly applicable* and *self-executing*[27] . Article 83(5) of the GDPR states that violations of the fundamental principles of data processing, including health data under Article 9, may be subject to administrative fines of up to €20 million or 4% of total global annual turnover. This executive authority is normatively very strong, but its effectiveness still depends on the willingness and consistency of the supervisory authority in enforcing it. The enforcement pattern by ANSPDCP reveals a problematic trend in which this agency is far more aggressive in imposing fines on private sector entities compared to public institutions.

The gap in institutional compliance culture in Romania exacerbates the existing law enforcement paradox. There is a gap in practical application within clinical settings, even though Romanian healthcare professionals understand the theoretical aspects of patient consent as stipulated in Article 3 of Law No. 190/2018. This gap is particularly related to data breach incident management protocols, where healthcare workers are not trained to respond quickly and appropriately when a cybersecurity breach occurs. This phenomenon indicates that the issue of effectiveness in Romania stems not solely from the passivity of regulatory bodies, but is also driven by a deficit in legal literacy and a compliance culture at the operational level of digital health services[28] . Within the Nonet-Selznick framework, Romania’s legal system is experiencing internal tensions. At the formal normative level, Romania has achieved mature legal autonomy through the GDPR, but at the sectoral implementation level, the system is trapped in procedural formalism. Romania requires a transformation of its compliance culture, moving from mere fulfillment of formalities toward the substantive internalization of patients’ rights.

Based on the principles of good governance formulated by UNESCAP, accountability, transparency, effectiveness, and adherence to the rule of law are essential characteristics that must mutually reinforce one another within a state data protection supervisory agency[29] . For Indonesia, the operationalization of the Personal Data Protection Enforcement Agency mandated by Article 58 of the PDP Law must be designed to have full independence from political pressure and sectoral ministries, be equipped with executive investigative powers and the authority to impose sanctions independently, and have a specialized sectoral oversight division that understands the complexities of the digital medical data ecosystem, including electronic medical records. Meanwhile, for Romania, the ANSPDCP needs to adopt a more proactive supervisory stance toward the public sector and develop sector-specific guidelines for healthcare services. Both countries can adopt a risk-based supervision model, where supervisory resources are focused on entities managing high-sensitivity and high-volume data[30] . This approach enhances supervisory efficiency while strengthening the effectiveness of deterrence.

The concept of *Privacy by Design* developed by Dr. Ann Cavoukian emphasizes the core principle that privacy protection must be proactive and preventive[31] . For Indonesia and Romania, integrating the Privacy by Design principle into health technical regulations must include standardized DPIA requirements, data encryption in transit and at rest, role-based access controls, and tamper-proof audit logging. Article 32(1)(d) of the GDPR requires “a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures,” which can serve as a model for implementing regulations in Indonesia and Romania. Government Regulation No. 20 of 2024 on the “ ” in Indonesia needs to be elaborated with concrete technical standards for SATUSEHAT, including requirements for external audits and cybersecurity certification. Technical implementation must be accompanied by swift administrative sanctions to ensure the timeliness of deterrence. Without an independent inspection mechanism, technical requirements will be difficult to monitor consistently.

The principle of “ubi ius ibi remedium” dictates that the recognition of normative rights must be accompanied by the availability of practical and accessible redress mechanisms for rights holders[32] . For Indonesia, the personal data dispute adjudication mechanism regulated in Government Regulation No. 20 of 2024 must be immediately operationalized technically through the establishment of a special medical dispute committee under the PDP Agency, which has the authority to adjudicate violations of health data protection. Given that data subjects (patients) are generally in a position of economic and informational weakness (informational asymmetry) vis-à-vis healthcare institutions or digital platform corporations[33] , Indonesia needs to develop a complaint-based dispute resolution pathway that is free of charge and does not require legal representation. This mechanism is strengthened by integrating the roles of legal aid institutions and sectoral ombudsmen to ensure that patients from economically disadvantaged groups retain access to justice. Meanwhile, in Romania, although Article 82 of the GDPR guarantees full compensation rights for data subjects harmed by data processing that violates regulations, local public legal awareness remains very low, resulting in many patients being unaware of their right to file a claim[34] . The strengthening model needed by Romania is the implementation of rights-based public education

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

programs specifically targeting the community of patients in public healthcare facilities to bridge the gap between supranational compensation instruments and the empirical realization of claims on the ground.

One of the structural weaknesses in Indonesia is the absence of a lex specialis legal instrument that comprehensively harmonizes the intersections between the Personal Data Protection Act (PDP Act), the Health Act, and their technical regulations into a single consistent and non-contradictory framework. The principle of legal certainty, as formulated by Fuller in the principles of clarity and non-contradiction, requires that legal norms must be clearly understandable to the subjects they regulate and must not contain internal contradictions among legal regulations35 . Indonesia needs to draft *a Joint Regulation* or an integrative Institutional Memorandum of Understanding between the Personal Data Protection Agency (PDP), the Ministry of Communication and Digital Affairs, and the Ministry of Health to establish a single-point cyber reporting process within the SATUSEHAT ecosystem. Romania requires more specific sectoral guidelines from the ANSPDCP to ensure that GDPR implementation in clinical settings is more targeted. This harmonization also facilitates cross-agency audits and a coordinated response to health data protection issues.

Responsive law, as conceived by Nonet and Selznick, is characterized by flexibility, participation, and the ability to achieve substantive justice36 , rather than merely adhering to rigid, context-insensitive formal procedural order. The transformation toward responsive law requires attention to non-normative dimensions such as a culture of compliance and long-term institutional capacity. A comprehensive strengthening model must include two non-normative dimensions: the implementation of mandatory training on personal data protection for all medical personnel and healthcare facility information system managers to transform data literacy into a mandatory professional competency for every healthcare worker; and the acceleration of standardization and the appointment of sectoral Data Protection Officers (DPOs) in every hospital, as mandated by Article 37 of the GDPR and Article 53 of the Personal Data Protection Law. Sustained investment in human resources, certification programs, and organizational incentives for compliance is necessary to ensure long-term effectiveness.

For Indonesia, the momentum of institutional transition must be leveraged not only to complete the administrative establishment of the Personal Data Protection Agency (PDP) but also to build a foundation of a compliance culture through national training programs for healthcare workers and the development of equitable cybersecurity infrastructure extending to healthcare facilities in remote areas. For Romania, the necessary reform involves shifting the ANSPDCP's paradigm from a reactive and selective authority to a proactive and equitable one, prioritizing oversight of the public sector due to its management of large volumes of citizens' health data. The effectiveness of health data protection mechanisms in the post-pandemic digital era is not determined by the tension between Indonesia's localization model or Romania's free data flow model, but rather by the political courage to strengthen supervisory institutions, the seriousness in implementing the Privacy by Design principle, and a long-term commitment to building a culture of compliance rooted in the awareness that health data is a fundamental right that must be protected by the state.

IV. Conclusion

Indonesia and Romania already have adequate legal frameworks to protect health data in the post-COVID-19 digital era, yet the effectiveness of this protection still faces challenges in the areas of implementation and law enforcement— . The main issue in both countries does not lie in a lack of legal norms, but rather in the gap between normative regulations and their implementation, as reflected in the suboptimal functioning of oversight, enforcement of sanctions, and institutional accountability mechanisms. The supranational regulatory model implemented by Romania through the GDPR provides a higher level of harmonization and legal certainty, while Indonesia's national model offers greater flexibility but still faces challenges in coordination and institutional strengthening. Therefore, the effectiveness of health data protection in both countries requires the strengthening of independent supervisory authorities, the application of the "privacy by design" principle, the harmonization of sectoral regulations, and the development of a compliance culture oriented toward the substantive protection of patients' rights. Further research needs to examine in greater depth the effectiveness of health data protection policy implementation following the full operationalization of the supervisory agency in Indonesia, as well as developments in GDPR enforcement practices within the public health sector in European Union member states.

Acknowledgments

This section expresses gratitude to those who played a role in the conduct of the research activities, such as the research laboratory. The roles of donors or those supporting the research are briefly mentioned.

References

1. [1] M. M. Ahmed et al., "Integrating Digital Health Innovations to Achieve Universal Health Coverage: Promoting Health Outcomes and Quality Through Global Public Health Equity," Healthcare, vol. 13, no. 9, p. 1060, May 2025, doi: 10.3390/healthcare13091060.
2. [2] M. Kritika, "Ethical and legal dimensions of integrating neurotechnology with cybersecurity, a critical reflection for information and communication technology (ICT) policy and practice," Int. Cybersecurity Law Rev., vol. 7, no. 1, pp. 69–129, Mar. 2026, doi: 10.1365/s43439-026-00168-6.
3. [3] M. E. Gonçalves, "The risk-based approach under the new EU data protection regulation: a critical perspective," J. Risk Res., vol. 23, no. 2, pp. 139–152, Feb. 2020, doi: 10.1080/13669877.2018.1517381.
4. [4] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health Care Cybersecurity Challenges and Solutions Under the Climate of

COVID-19: Scoping Review," J. Med. Internet Res., vol. 23, no. 4, pp. 1–18, Apr. 2021, doi: 10.2196/21747.
5. [5] A. de Lucas Ancillo, M. T. del Val Núñez, and S. G. Gavrila, "Workplace change within the COVID-19 context: a grounded theory approach," Econ. Res. Istraživanja, vol. 34, no. 1, pp. 2297–2316, Jan. 2021, doi: 10.1080/1331677X.2020.1862689.
6. [6] R. R. Colwell, K. D. Brumfield, M. Usmani, A. Huq, and A. S. Jutla, The COVID-19 Pandemic. Cham: Springer International Publishing, 2024.
7. [7] Irwandy, "Bocornya 1,3 Juta Data eHac, Mengapa Terjadi dan Bahayanya bagi Pasien," 03-Sep-2021. https://www.kompas.com/sains/read/2021/09/03/080000023/bocornya-1-3-juta-data-ehac-mengapa-terjadi-dan-bahayanya-bagi-pasien?page=all (accessed Jun. 07, 2026).
8. [8] C. Vallance and J. Tidy, "Ransomware attack hits dozens of Romanian hospitals," 14-Feb-2023. https://www.bbc.com/news/technology-68288150 (accessed Jun. 07, 2026).
9. [9] L. Hornuf, S. Mangold, and Y. Yang, "Data Protection Law in Germany, the United States, and China," in Data Privacy and Crowdsourcing, Cham: Springer, 2023, pp. 19–79.
10. [10] T. detikcom, "Saling Lempar Tanggung Jawab Bocornya Data PeduliLindungi," 07-Sep-2021. https://news.detik.com/foto-news/d-5712805/saling-lempar-tanggung-jawab-bocornya-data-pedulilindungi (accessed Jun. 07, 2026).
11. [11] I. V Nastasa, F.-L. Furtunescu, and D. G. Mincă, "Challenges and Progress in General Data Protection Regulation Implementation in Romanian Public Healthcare," Cureus, pp. 1–12, Jan. 2025, doi: 10.7759/cureus.78008.
12. [12] A.-G. Nacu, D.-A. Constantin, and L. M. Rogozea, "Ethical Dilemmas and Legal Responsibilities in Patient Care: An Analysis of Hospital Safety," Healthcare, vol. 13, no. 21, pp. 1–21, Nov. 2025, doi: 10.3390/healthcare13212800.
13. [13] E. N. A. . Sihombing, "Legal Securities Against Privacy Data for Covid-19 Patients in Indonesia," Veteran Law Rev., vol. 4, no. 1, pp. 35–52, Apr. 2021, doi: 10.35586/velrev.v4i1.2618.
14. [14] D. B. Kharisma and A. Diakanza, "Patient personal data protection: comparing the health-care regulations in Indonesia, Singapore and the European Union," Int. J. Hum. Rights Healthc., vol. 17, no. 2, pp. 157–169, May 2024, doi: 10.1108/IJHRH-04-2022-0035.
15. [15] C. C. Francu and Ștefan Sava, "Global Perspectives on Digital and AI Legislation: A Comparative Study of Data Protection, AI Governance, and Healthcare Innovations with a Focus on Romania," Proc. Int. Conf. Bus. Excell., vol. 19, no. 1, pp. 2469–2481, Jul. 2025, doi: 10.2478/picbe-2025-0191.
16. [16] N. Lamp, "The 'practice turn' in international law: insights from the theory of structuration," in Research Handbook on the Sociology of International Law, Cheltenham: Edward Elgar Publishing, 2018, pp. 273–295.
17. [17] J. T. de Souza and L. Rossoni, "How the congruence between public servants' schemas and legal legitimacy affects top-down public policy implementation," Front. Sociol., vol. 10, pp. 1–13, May 2025, doi: 10.3389/fsoc.2025.1505494.
18. [18] F. Brito Bastos and P. Pałka, "Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?," Eur. Const. Law Rev., vol. 19, no. 3, pp. 487–517, Sep. 2023, doi: 10.1017/S1574019623000202.
19. [19] R. T. Budiyanti, P. M. Herlambang, A. Fuad, and W. Kusumastuti, "Integration of Electronic Medical Record and SATUSEHAT's Platform : Patient's Legal Protection Perspective," Int. J. Heal. Lit. Sci., vol. 1, no. 2, pp. 1–8, Dec. 2023, doi: 10.60074/ihelis.v1i2.18.
20. [20] D. Wijayanti, S. Urbaya, S. Yusuf, C. Sulton, D. S. Sumunar, and T. Sitompul, "Towards Federated Health Information Exchange Architecture in Indonesia: Design and Implementation," in 2025 International Conference on Information Management and Technology (ICIMTech), 2025, pp. 282–287, doi: 10.1109/ICIMTech67074.2025.11264924.
21. [21] D. Cantik and A. Prabawati Rahmahani, "The Urgency of Establishing a Supervisory Agency for the Implementation of Personal Data Protection in the Implementation of the Personal Data Protection Law," Int. J. Sci. Environ., vol. 6, no. 1, pp. 300–308, Jan. 2026, doi: 10.51601/ijse.v6i1.332.
22. [22] L. A. Nimineț, A. Feraru-Prepeliță, and V. Nimineț, "The Role of Artificial Intelligence and Neuroscience in Business Ethics: A Human Resources Perspective," BRAIN. Broad Res. Artif. Intell. Neurosci., vol. 17, no. 2, pp. 144–158, Jun. 2026, doi: 10.70594/brain/17.2/9.
23. [23] G. Ishmaev, M. Dennis, and M. J. van den Hoven, "Ethics in the COVID-19 pandemic: myths, false dilemmas, and moral overload," Ethics Inf. Technol., vol. 23, no. S1, pp. 19–34, Nov. 2021, doi: 10.1007/s10676-020-09568-6.
24. [24] H. Hirtenlehner and H. Leitgöb, "Deterrence Perceptions, Self-Control Ability and the Moral Filter: Conceptualizing and Testing a Model of a Subsidiary Relevance of Deterrence," Deviant Behav., vol. 45, no. 10, pp. 1391–1418, Oct. 2024, doi: 10.1080/01639625.2023.2298512.
25. [25] A. F. S. Alfikri and M. R. Wahda, "Compilation of Islamic Law: The Face of Responsive Legal Products as the Accommodative Politics of the New Order Government," R. Stud. Law Rev., vol. 4, no. 1, pp. 1–11, May 2025, doi: 10.32734/rslr.v4i1.18591.
26. [26] J. Webber, "A Democracy-Friendly Theory of the Rule of Law," Hague J. Rule Law, vol. 16, no. 2, pp. 339–374, Aug. 2024, doi: 10.1007/s40803-024-00240-5.
27. [27] V. G. Hatzopoulos, "The EU as an exporter of digital rules and standards? The case of the DSA and the DMA," Yearb. Eur. Law, Mar. 2026, doi: 10.1093/yel/yeag003.
28. [28] I.-M. Păcuraru, A. Năstac, A. Zamfir, Ștefan S. Busnatu, O. Andronic, and A.-R. Artamonov, "Digital Transformation of Medical Services in Romania: Does the Healthcare System Meet the Current Needs of Patients?," Healthcare, vol. 13, no. 20, pp. 1–31, Oct. 2025, doi: 10.3390/healthcare13202549.
29. [29] S. Marcucci, N. G. Alarcón, S. G. Verhulst, and E. Wüllhorst, "Informing the Global Data Future: Benchmarking Data Governance Frameworks," Data Policy, vol. 5, pp. 1–25, Aug. 2023, doi: 10.1017/dap.2023.24.
30. [30] E. Anklam et al., "Emerging technologies and their impact on regulatory science," Exp. Biol. Med., vol. 247, no. 1, pp. 1–75, Jan. 2022, doi: 10.1177/15353702211052280.
31. [31] C. Del-Real, E. De Busser, and B. van den Berg, "A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies," Int. Rev. Law, Comput. Technol., vol. 39, no. 3, pp.

374–405, Sep. 2025, doi: 10.1080/13600869.2025.2457227.
32. [32] V. Capasso, “Procedural Proportionality is Fine … but up to a Point: the ‘Negative Expected Value Suits’ Exception,” Int. J. Proced. Law, vol. 15, no. 2, pp. 427–443, Nov. 2025, doi: 10.1163/30504856-15020006.
33. [33] P. Terzis, “Compromises and Asymmetries in the European Health Data Space,” Eur. J. Health Law, vol. 30, no. 3, pp. 345–363, Oct. 2022, doi: 10.1163/15718093-bja10099.
34. [34] M. C. Plaiasu, D. O. Alexandru, and C. A. Nanu, “Physicians’ legal knowledge of informed consent and confidentiality. A cross-sectional study,” BMC Med. Ethics, vol. 23, no. 1, p. 93, Sep. 2022, doi: 10.1186/s12910-022-00835-3.
35. [35] A. Bisoyi, “The Rule of Law Philosophy and Design Standards,” in Blockchain and Legitimacy, Cham: Springer, 2025, pp. 55–91.
36. [36] T. Sukmana, “Responsive Law and Progressive Law: Examining the Legal Ideas of Philip Nonet, Philip Selznick, and Sadjipto Raharjo,” Perad. J. Law Soc., vol. 2, no. 1, pp. 92–105, Jun. 2023, doi: 10.59001/pjls.v2i1.82.

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo