



Challenges and Opportunities in the Management of Public Health Data in Indonesia under the Personal Data Protection Law

Hetsa Himawati¹ and Zahra Shafira Belanusa²

¹ Master of Law, Faculty of Law, Gadjah Mada University (Jakarta Campus), Indonesia

² Master of Law, Faculty of Law, Gadjah Mada University (Jakarta Campus), Indonesia
hetsahimawati@mail.ugm.ac.id

Abstract. This article investigates the interplay between data privacy, Big Data, and public health within the framework of Indonesian legislation, specifically focusing on the implications of the Health Law and the Personal Data Protection Law. This analysis elucidates the paramount importance of managing patient data in accordance with legal standards while ensuring the safeguarding of personal information in the era of Big Data analytics. The discussion delineates the rights of data subjects, emphasizing their capacity to pursue redress through established dispute resolution mechanisms outlined in the Personal Data Protection Law. Furthermore, the paper examines the obligations of healthcare providers in protecting personal data amidst the challenges posed by Big Data utilization and the potential legal ramifications of non-compliance. Through a comprehensive review of case studies and contemporary practices, this article aims to elucidate the challenges and opportunities inherent in the implementation of effective data privacy measures within the healthcare sector. Ultimately, this analysis advocates for a balanced approach that fosters innovation in public health through Big Data while concurrently upholding the fundamental rights of individuals regarding their personal data.

Keywords: Big Data, Data Privacy, Public Health, Health Data Governance, Personal Data Protection Law, Health Law, Healthcare Sector.

1 Introduction

1.1 Health as an Investment of Sustainable National Growth

Health is one of the strategic sectors that determines the quality of human resources and makes a significant contribution to national development [1]. This is affirmed in Article 1 of Law Number 17 of 2023 on Health (“**Health Law**”), which defines health as a condition that reflects an individual's complete physical, mental, and social well-being, and not merely the absence of disease or infirmity, thereby enabling individuals to live productively. In this context, health is regarded as a fundamental human need, the presence of which is crucial in determining one's quality of life and capacity to actively participate in social life and development [2].

Without optimal health conditions, the attainment of higher education or mastery of advanced technology may not be fully leveraged to enhance individual productivity. Therefore, a high level of public health is regarded as a strategic investment in the development of human resources capable of contributing both socially and economically [3].

A high standard of public health is a critical prerequisite for poverty alleviation, economic growth, and the realization of sustainable economic development. Historical evidence demonstrates that many countries' success in achieving rapid economic growth has often been preceded by significant advancements in public health, such as disease control and improved nutritional status. Conversely, countries grappling with serious public health challenges tend to face greater obstacles in attaining stable and sustainable economic growth compared to those with more favorable public health conditions [4].

Considering health's pivotal role in national development, it is imperative to acknowledge that a central aim of the national health system is to guarantee the provision of high-quality healthcare services that are accessible to all members of society on an equitable basis [4].

1.2 Challenges in Health Policy in Indonesia

The formulation of public policy is one of the key instruments used by the government to address various issues faced by society. Ideally, public policies should be developed based on robust scientific evidence. However, in practice, evidence-based policy approaches often do not function optimally, partly due to limited access to relevant and accurate scientific data [5]. This challenge becomes even more complex in the context of Indonesia, which is facing demographic changes and a triple health burden: high rates of infectious diseases, increasing prevalence of non-communicable diseases, and the resurgence of diseases that were previously under control. This situation presents a particular obstacle for the government in formulating effective and sustainable health policies. As a result, the policy-making process tends to be time-consuming, and the policies produced may not necessarily address the needs and challenges on the ground effectively. In the long term, without regular evaluation and improvement, this could lead to negative consequences in terms of social, economic, and public health impacts [6].

1.3 Big Data in the Health Sector

To achieve the provision of high-quality and equitable healthcare services, continuous innovation within the healthcare system is essential. Such innovation must be responsive to the evolving needs of society and capable of adapting to changing times, thereby fostering the progressive and sustainable advancement of healthcare services [7].

On the other hand, advancements in information technology in the digital era have become a significant driver in the transformation of various sectors of life, including the healthcare sector [8]. One form of utilizing this technology is the use of electronic health records, which have now been widely implemented in hospital information

systems and other healthcare facilities in Indonesia. This system serves as a replacement or complement to conventional paper-based medical records, offering advantages in terms of speed, accuracy, and the efficiency of managing and storing patient data [9].

Various digital health services, such as medical consultations, telemedicine, online pharmacy services, and the dissemination of health information through digital media, have also become integral to the use of internet-based applications in the healthcare sector [10]. In addition, digital transformation has been implemented by the government in managing public health data administration. Examples of this can be seen in the use of the "*PeduliLindungi*" app during the Corona Virus Disease 19 pandemic, the "*SATUSEHAT*" platform for integrating electronic health records, and the "*Mobile JKN*" app, which facilitates more efficient access to Social Health Security Management Agency (*Badan Penyelenggara Jaminan Sosial Kesehatan*) services.

The use of information technology in the healthcare sector involves the management of vast and complex datasets, which in technological literature is referred to as Big Data. This concept not only emphasizes the volume of data but also its diversity, the speed of acquisition and processing, and the high level of precision required at each stage [11]. Furthermore, Big Data has the capacity to process, analyze, and utilize large-scale heterogeneous datasets [12]. Consequently, this technology facilitates the provision and management of information, supports the integration of critical data into strategic decision-making processes, and can generate high-speed information outputs. In short, the application of Big Data transforms data management into a structured, directed digital resource with high strategic value [13].

In the healthcare sector, Big Data analysis offers significant potential to enhance various aspects, from improving diagnostic accuracy and tailoring treatment to individual needs, to streamlining the management of healthcare systems for greater efficiency. This undoubtedly contributes positively to the quality of decision-making in health policy [14].

Moreover, Big Data has become a key tool in addressing public health challenges by integrating and processing data from various sources, such as electronic health records, laboratory results, and genetic information, thereby providing deep insights at both the individual and population levels [15]. In the fields of medical research and drug development, Big Data plays a crucial role in identifying disease trends, predicting epidemics, and accelerating the discovery of more effective health solutions [16].

The ability of Big Data to uncover hidden patterns and trends across diverse datasets enables more accurate disease predictions, the design of targeted interventions, and support for precision medicine tailored to the unique characteristics of each patient [17]. Thus, the application of Big Data clearly offers strategic benefits in the transformation of the healthcare sector, both for developing more responsive policies and for advancing more precise and efficient therapies.

1.4 The Role of the National Health Information System as Big Data in Indonesia under the Health Law

Health Law was drafted to support the transformation of the healthcare system in Indonesia, with a focus on strengthening the Big Data system managed by each healthcare facility, in this case, the Health Information System. One of the key aspects of this law is the authority of the government to manage and utilize health data through the integration of various Health Information System into Big Data managed by the Ministry of Health, referred to as the National Health Information System. Health Information System is defined as a system that integrates various stages of reporting processes and the utilization of necessary information to improve the effectiveness and efficiency of healthcare service delivery. National Health Information System is defined as the Health Information System managed by the ministry responsible for government affairs in the health sector, which integrates and standardizes all Health Information System to support health development.

It can be understood that there are two types of Big Data in health care as outlined in the Health Law: Health Information System is the Big Data managed by each healthcare facility, while National Health Information System is the Big Data managed by the Ministry of Health and represents the integration of all Health Information System. Health Law also regulates the rights, obligations, and responsibilities of both the central and regional governments in the implementation of Health Information System, ensuring that healthcare resources are available equitably, including in remote areas. The processing of Health Information System begins with data collection, data processing, evaluation, and the transfer of information necessary for managing and controlling healthcare services, as well as for research and training purposes [18].

The central and regional governments are responsible for ensuring the availability of an adequate Health Information System, enabling the public to access healthcare services more easily. Healthcare facilities are required to report the results of services, education, research, and development to the central and regional governments through Health Information System. Hospitals, as part of healthcare facilities, must also implement an integrated Hospital Health Information System that connects to the National Health Information System.

Information and communication technology play a critical role in the provision of healthcare services, including through telehealth and telemedicine integrated with National Health Information System. Some of the key roles of the National Health Information System include data integration within network systems to support primary healthcare services, healthcare referral systems, and organ transplantation management. Additionally, Health Information System plays a role in medical workforce planning, the management of health reserves, and the integration of healthcare service records and medical supplies.

The National Health Information System also integrates data and information in the operation of biobanks and biorepositories, managed by healthcare facilities and research institutions. In this context, the principles of confidentiality and privacy are paramount, ensuring that the identity of individuals providing specimens is protected.

Therefore, the role of Big Data in Health Information System is crucial for enhancing the efficiency and effectiveness of healthcare services across Indonesia.

1.5 Risks and Impacts of Health Data Breaches

Like two sides of the same coin, the use of Big Data in the healthcare sector not only promises extraordinary efficiency and innovation but also carries potential risks that should not be overlooked. Behind the sophistication of this technology, there are serious challenges that demand attention, particularly concerning privacy protection, data security, and the potential for information misuse. Therefore, appropriate mitigation measures are essential to ensure that the significant benefits of Big Data do not transform into hidden threats.

Based on Social Health Security Management Agency's data on 2021, Social Health Security Management Agency breach case serves as a real example of how cybersecurity violations can occur and have a significant impact on public trust and the stability of public services. Over 279 million pieces of personal data from Social Health Security Management Agency participants, including names, national identification numbers, addresses, phone numbers, and health data, were reported to have been leaked and sold on online forums [19].

Personal health data is highly sensitive information and poses a risk to privacy if not carefully managed. Health data breaches result in far-reaching consequences, including the potential misuse of personal information, the use of data for illegal activities such as identity theft and other financial violations, material and immaterial harm to individuals, and a decline in public trust in health data governance [20].

2 Research Methodology

Legal research can generally be classified into three types: normative legal research, empirical legal research, and normative-empirical legal research [21]. This study adopts a normative legal research approach. Normative legal research is a method that focuses on analyzing legal rules, principles, and doctrines to identify solutions to existing legal issues [22]. This approach involves examining the law as a system of rules, norms, legal principles, doctrines, legal maxims, theories, and other scholarly literature in order to address the legal problems formulated in the research questions [23].

In this study, the legal norm system is positioned as the object of analysis. This system encompasses all normative elements of law that reflect values guiding how individuals ought to behave, and it is examined systematically in accordance with the hierarchical structure of the legal system. The aim is to formulate legal arguments or opinions that serve as justification for specific legal events [24]. This research is conducted by presenting a legal event, identifying the legal issues it raises, and subsequently analyzing those issues to find an appropriate resolution.

Legal research must be supported by comprehensive data sources to allow for an in-depth analysis in relation to the legal issues under investigation. This study utilizes secondary data sources as the basis for its analysis. Secondary data refers to information obtained through literature or library materials that are relevant to the object of study

[25]. In the context of normative legal research, such data sources are referred to as legal materials, which are used to conduct analysis of applicable laws. These legal materials are categorized into primary, secondary, and tertiary legal materials [26], which will be further elaborated below:

a. Primary Legal Materials

Primary legal materials are authoritative sources of law, meaning they possess binding legal force [27]. The primary legal materials used in this study include Law Number 27 of 2022 on Personal Data Protection and Law Number 17 of 2023 on Health.

b. Secondary Legal Materials

Secondary legal materials refer to all legal publications that are not official legal documents. These include textbooks, legal journals, and commentaries on court decisions [28]. The secondary legal materials used in this research consist of various publications related to health, patient data protection, and personal data protection.

c. Tertiary Legal Materials

Tertiary legal materials serve as references that provide guidance or clarification on primary and secondary legal materials [29]. These include legal dictionaries, encyclopedias, and utilized in this study include health dictionaries, legal dictionaries (especially those related to personal data protection), the *Kamus Besar Bahasa Indonesia* (Indonesian Dictionary), and the English Dictionary.

The data collection methods employed in this research fall under the category of secondary data collection, specifically through literature review (bibliographic study), document study, and archival study (file or record study) [30]. Legal materials relevant to the legal issues examined in this study were collected through a systematic search conducted in bookstores, libraries, online databases, and other media or repositories that house such materials.

More concretely, the researcher identified relevant legislation associated with the legal issue under investigation and gathered supporting sources such as books, academic journals, legal dictionaries, and other pertinent literature. A snowball sampling method was applied to expand the search, after which the materials were classified according to their sources and legal hierarchy. All findings were documented systematically in research notes to facilitate comprehensive legal analysis [31].

The method of drawing conclusions employed in this study is the deductive reasoning method. This approach is commonly used in normative legal research, where conclusions about specific legal issues are derived from general principles or legal norms [32].

3 Result

3.1 Regulatory Framework and Protection of Health Data Privacy Rights

The management of big data in Indonesia has undeniably become a vital component of the national health system transformation. Health data and information, including medical records, disease status, and social security claims, are collected and integrated

through the National Health Information System, which serves as the backbone of healthcare digitalization, as outlined in the Health Law [33].

On the other hand, Law No. 27 of 2022 on Personal Data Protection (“**Personal Data Protection Law**”) provides a general, cross-sectoral regulatory framework on the management of personal data [34]. This law establishes fundamental principles for the management of personal data, including personal health data, although the implementation of the Personal Data Protection Law has yet to be fully optimized [35].

Article 4 paragraph (1) of the Health Law emphasizes that everyone has the right to protection of the confidentiality of their personal health data and information. This provision reflects the state's recognition of the importance of privacy rights as part of human rights in the healthcare sector. Health information is highly personal and sensitive as it includes aspects that can describe a person's physical condition, mental health, medical history, and overall medical records. Therefore, protection of such information is not only administrative but also serves as an ethical and legal foundation in the management of health data by healthcare professionals, healthcare institutions, and digital systems based on information technology.

3.2 Management of Personal Health Data in the Health Information System based on the Health Law

Regarding the management of patient data within the Health Information System, Health Law permits the system to be operated by the Central Government, Regional Governments, healthcare providers, and members of the public—both individuals and groups—as part of initiatives to enhance the efficiency and effectiveness of healthcare delivery. Health Information System operators are obligated to integrate their systems with the National Health Information System. Additionally, the Ministry of Health may provide support to these administrators through technical assistance, such as training and software tools. This section discusses how patient data is managed within the Health Information System, in line with the provisions of the Health Law.

Health Information System encompasses both personal and public health data, sourced from a variety of entities including healthcare facilities, central and local government institutions, organizations managing national social security and health programs, community health activities outside of formal healthcare services, individual self-reporting, and other relevant sources. To effectively manage this data, Health Information System administrators hold key responsibilities in the handling and protection of health information. They must conduct comprehensive data processing, including collection, acquisition, analysis, storage, correction, updating, display, dissemination, transfer, disclosure, deletion, or destruction of data.

Moreover, Health Information System administrators are expected to maintain a reliable health information system and ensure that the data provided is of high quality. They are also responsible for documenting all stages of data processing. This includes activities such as planning, data gathering, storage, verification, transmission, use, and disposal, all in compliance with existing legal frameworks. Should a breach in data protection occur, it is mandatory for administrators to notify the affected data subject.

The Health Law outline the full cycle of processing the health data and health information by Health Information Providers. Health Information System Providers are obligate to ensure system reliability, data security, and to conduct regular audits of health information processing.

3.3 Personal Health Data Protection in Health Information Systems based on Health Law

Article 351 of the Health Law demonstrates a strong regulatory awareness of the importance of personal data protection. In managing the Health Information System, administrators are responsible for safeguarding individuals' personal and health data. Any processing of such data that involves personal health information must either obtain the explicit consent of the data subject or rely on other lawful bases as outlined in applicable data protection regulations. This section focuses on the personal data protection framework established under the Health Law. Individuals, as data subjects, are granted specific rights concerning the handling of their health data.

These rights include being informed about the purpose of data collection, accessing and correcting their data via Health Information System operators, and requesting the transfer of their data to another Health Information System provider. If any stored data is found to be inaccurate, data subjects have the right to request its deletion with their consent. Further rights are provided under broader personal data protection legislation, although some may be limited under legal conditions. The Health Law also emphasizes the obligation to protect the confidentiality of patient health information.

Individuals have the legal right to keep their health data confidential, except in certain circumstances specified by law. These exceptions include situations involving law enforcement requests, responses to public health crises or disasters, and limited educational or research purposes. Disclosure may also occur to safeguard the safety of individuals or the public or for the purpose of delivering healthcare services, including diagnosis, treatment, and patient care. Additionally, information may be disclosed upon the patient's request, for administrative purposes, insurance claims, or health financing needs, as well as under other lawful provisions. In instances where healthcare professionals suspect or identify criminal activity involving a patient, confidentiality may also be lifted.

Healthcare providers are legally bound to uphold the confidentiality of patient health data and may decline to release such information to the public unless allowed by law. Medical and healthcare professionals are equally required to protect patient information during their practice. Moreover, healthcare workers, including facility administrators, must ensure that medical records are stored and maintained securely, preserving their confidentiality, integrity, and accessibility. These records are the property of the healthcare facility, which is accountable for their protection.

All medical professionals delivering healthcare services must uphold patient confidentiality and are only permitted to disclose health information under clearly defined legal conditions. The term "*health confidentiality*" encompasses a patient's medical history, diagnosis, treatments, mental and physical care, and other personal data. In the context of human subject research, the rights of participants must be fully

respected, ensuring that no harm comes to them and that their identity and personal information remain protected.

This means that through Article 351 of the Health Law, the legislation recognizes the right to health data privacy for data subjects, including the right to be informed about the purpose of data collection, the right to access and rectify data, the right to request data transfer to another provider, and the right to request deletion of inaccurate data with the data subject's consent.

3.4 Protection of Personal Health Data Based on the Personal Data Protection Law

In the Personal Data Protection Law, individuals whose data is collected and processed are referred to as "*Personal Data Subjects*." This term denotes any person to whom identifiable data relates, whether the identification is made directly or indirectly, independently or in combination with other information, and whether processed through electronic or non-electronic means. Personal data under this law is divided into two main categories:

- a. General personal data, which includes details such as full name, gender, nationality, religion, marital status, and other attributes that may be used to identify an individual; and
- b. Specific personal data, which encompasses sensitive information such as health records, biometric and genetic data, criminal history, child-related data, personal financial details, and other data types as specified by prevailing legislation.

Within this framework, health-related data is explicitly classified as specific personal data due to its sensitive nature.

This section focuses on the protection of personal data belonging to individuals classified as Personal Data Subjects. The handling of such data is primarily governed by the responsibilities of the Personal Data Controller, defined in the Personal Data Protection Law as any individual, public institution, or international organization—acting alone or collaboratively—who determines the purposes of and exercises authority over personal data processing activities.

Within the framework of personal data management by a Personal Data Controller, this section addresses the legal provisions related to personal data protection as outlined in the Personal Data Protection Law. Prior to discussing the specific responsibilities of Personal Data Controllers, it is essential to first consider the rights granted to Personal Data Subjects, which must be acknowledged and upheld by the controllers.

Personal Data Subjects are granted various rights to safeguard their personal data. These include the right to clear and transparent information regarding the identity of the data requester, the legal grounds for data processing, the intended purpose of data collection and use, and the obligations of the data processor. They are also entitled to rectify, update, or complete inaccurate data, in alignment with the objectives of the data processing.

Moreover, Personal Data Subjects have the right to access their personal data and obtain copies of it, and they may request that data processing be discontinued, or that their data be deleted or destroyed. They are further entitled to withdraw their previously

given consent and to object to any decisions derived solely from automated processing mechanisms.

Under certain conditions, Personal Data Subjects may request a delay or limitation in the processing of their data, as long as it remains consistent with the processing purpose. In instances of data breaches or violations, they reserve the right to lodge a complaint and seek redress. Additionally, Personal Data Subjects may access and make use of their personal data from one controller and request its transfer to another controller.

The system for exercising the rights of Personal Data Subjects is implemented through a formal request, which can be submitted electronically or non-electronically to the Personal Data Controller. Furthermore, in the management of personal data, the Personal Data Controller is obligated to process the data in accordance with the principles of personal data protection. These principles include the collection of personal data that is limited, specific, legally valid, and transparent.

Data processing must be conducted in alignment with the specified purpose, while ensuring the rights of the Personal Data Subjects are upheld. Additionally, processing must be accurate, complete, non-misleading, up-to-date, and accountable. The security of personal data must be maintained throughout the entire process. The Personal Data Controller is required to provide information regarding the purpose and activities of data processing, including in cases of data protection failures. Personal data must be destroyed or deleted once the retention period has expired or upon request from the Personal Data Subject. All processing activities must be carried out responsibly and verifiably.

To ensure comprehensive protection of personal data, the Personal Data Controller has several key responsibilities. One of these is to ensure that data processing is based on a clear legal foundation, such as consent from the Personal Data Subject (either in writing or recorded), contractual obligations, legal duties, protection of vital interests, public service tasks, or other legitimate interests. Personal Data Controller must also be able to prove the existence of this consent and ensure that processing is conducted in a limited, lawful, transparent manner, and in accordance with the intended purpose. Additionally, they must ensure that the data remains accurate, complete, and consistent, as well as correct any inaccuracies and inform the Data Subject of these changes.

Personal Data Controller is required to maintain a record of all data processing activities and provide Personal Data Subjects with access to their data, including a history of processing during the retention period. However, access may be denied if it poses a security risk, affects health, or reveals the data of others. The Personal Data Controller is also tasked with evaluating the impact on data protection, ensuring data security and confidentiality, monitoring all parties involved, and preventing unauthorized access or processing. If a Personal Data Subject revokes consent, the processing must be halted, paused, or limited. Processing should also cease once the retention period ends, the purpose has been fulfilled, or upon the Personal Data Subject's request. Any data that is no longer required, has been obtained unlawfully, or is requested for deletion must be promptly destroyed, and the Personal Data Subject must be informed.

The Personal Data Controller must issue a written notice in the event of a data protection failure, take responsibility for all processing activities, and adhere to data protection principles. In cases of data transfers resulting from mergers, divisions, acquisitions, consolidations, or dissolutions, the Personal Data Controller is required to notify the Personal Data Subject. Ultimately, all activities must comply with the directives of the relevant authority responsible for personal data protection, as outlined in the Personal Data Protection Law.

The government plays a crucial role in ensuring the implementation of personal data protection in line with the Personal Data Protection Law provisions. This is carried out by an institution appointed by the president and directly accountable to the president, as per presidential regulations. This institution will be responsible for:

- a. Developing and establishing policies and strategies for personal data protection, serving as guidelines for Data Subjects, Personal Data Controllers, and Personal Data Processors;
- b. Overseeing the implementation of personal data protection;
- c. Enforcing administrative penalties for violations of the Personal Data Protection Law; and
- d. Facilitating out-of-court dispute resolution.

Substantively, the Personal Data Protection Law provides a comprehensive and prescriptive framework for personal data management, including personal health data, which is classified as specific personal data.

4 Discussion

4.1 Health Personal Data Protection under the Health Law and the Personal Data Protection Law in the Context of Big Data

In relation to Big Data in healthcare setting, the protection of personal data is critically important. Provisions regarding the management of Big Data in healthcare sector are specifically regulated under the Health Law. According to the Health Law, there are two types of Big Data in healthcare sector:

- a. Health Information Systems, which are managed by individual healthcare facilities, such as public health centers, hospitals, and other similar healthcare service providers; and
- b. National Health Information Systems, which are managed by the Ministry of Health.

In this regard, the Ministry of Health, as the organizer of the National Health Information System, is obligated to integrate all Health Information Systems managed by individual healthcare facilities. For this discussion, both Health Information System and National Health Information System Nasional will collectively be referred to as **"Big Data in Healthcare"**.

When the Health Law is linked to the Personal Data Protection Law, healthcare facilities, as the organizers of Health Information Systems, and the Ministry of Health, as the organizer of the National Health Information System, are considered Personal

Data Controllers. Additionally, patients, as individuals whose data is part of Big Data in Healthcare, are considered as the Personal Data Subjects.

In managing and processing patient data, healthcare facilities, such as Personal Data Controllers, are required to obtain prior consent from patients, as Personal Data Subjects, and must consider the rights of patients as Personal Data Subjects in data processing. In this context, healthcare facilities are obligated to maintain the confidentiality of each patient's health data, comply with all obligations required of Personal Data Controllers, and adhere to the principles of personal data protection outlined in the Personal Data Protection Law in managing and processing patient data.

Furthermore, in managing and processing patient data, healthcare facilities are responsible for providing quality health data and information so that the public can access it. This management and processing of patient data must be carried out by healthcare facilities while ensuring compliance with the provisions of the Personal Data Protection Law. Healthcare facilities are also required to inform patients in the event of a data protection failure, and these actions must be carried out in accordance with the provisions of the Personal Data Protection Law.

Referring to the explanation above, the protection of personal data is a critical aspect that healthcare facilities must implement in the management and processing of patient data. If a healthcare facility, acting as the Personal Data Controller, violates the provisions related to personal data protection as stipulated in the Health Law and the Personal Data Protection Law, it may face criminal penalties, including imprisonment and/or fines, in accordance with applicable regulations. Violations include actions such as collecting or obtaining a patient's personal data with the intent to benefit oneself, others, or a legal entity in a way that harms the patient, disclosing or using personal data that does not belong to them, and creating or falsifying a patient's personal data for personal gain or the benefit of others, all of which may harm the patient.

Furthermore, if a patient, as a Personal Data Subject, feels harmed due to their personal data being disclosed, used, falsified, or collected by the healthcare facility, as the Personal Data Controller, with the intent to benefit the healthcare facility, the patient may report such a situation and file a lawsuit with the appropriate institution. This could involve arbitration, a court, or another alternative dispute resolution institution. The dispute resolution procedure will be carried out in accordance with the provisions outlined in the Personal Data Protection Law and in compliance with the regulations of the respective dispute resolution institution chosen by the patient.

4.2 Challenges in Enforcing Personal Health Data Protection under Big Data in Indonesia's Healthcare Sector

The finding indicates that Article 351 of the Health Law serves as a normative reference that explicitly aligns the protection of health data with the Personal Data Protection Law. The healthcare sector is subject to the general data protection regime, thereby facilitating cross-sector harmonization. In the context of Big Data in Healthcare, where the volume, variety, and velocity of data are continuously expanding, this alignment is crucial due to the data sensitivity and high risk of privacy breaches.

Although no legal conflict exists at the normative level, challenges arise in the implementation of Personal Data Protection Law principles within the management of

Big Data in Healthcare. The Personal Data Protection Law detailed obligations, including the rights of data subjects, fairness and transparency principles, and requirements for Data protection Impact Assessments. However, implementing regulations under the Health Law, such as Government Regulation Number 28 of 2024 has not yet incorporated these provisions with sufficient specificity and enforceability.

4.3 Legal Remedies for Violations of Personal Health Data Protection

Given the complexities in implementing personal data protection in managing Big Data in Healthcare, the risk of non-compliance and data breaches are significantly heightened. These enforcement challenges not only undermine individual's trust in digitalization of health care system but also expose institutional gaps in accountability and control. The following section examines the sanctions and mechanisms for legal remedies as established under Personal Data Protection Law.

4.4 Prohibition on the Use of Personal Data and Its Sanctions

Based on the Personal Data Protection Law, there are provisions that prohibit individuals from disclosing personal data to the public, especially if such actions lead to harm for the Personal Data Subject. The following outlines the prohibitions and the corresponding sanctions for violations of these rules. In this case, it is unlawful for anyone to:

- a. Acquire or collect personal data that does not belong to them with the intention of benefiting themselves or others, which could result in harm to the Personal Data Subject. If proven guilty, the violator will be subject to a prison sentence of up to 5 (five) years and/or a fine of up to IDR 5,000,000,000 (five billion rupiahs);
- b. Disclose personal data that does not belong to them. If proven guilty, the violator will be subject to a prison sentence of up to 4 (four) years and/or a fine of up to IDR 4,000,000,000 (four billion rupiahs);
- c. Use personal data that does not belong to them. If proven guilty, the violator will be subject to a prison sentence of up to 5 (five) years and/or a fine of up to IDR 5,000,000,000 (five billion rupiahs);
- d. Create or falsify personal data with the intent of benefiting themselves or others, which could result in harm to others. If proven guilty, the violator will be subject to a prison sentence of up to 6 (six) years and/or a fine of up to IDR 6,000,000,000 (six billion rupiahs).

4.5 Dispute Resolution

Dispute resolution in personal data protection is one of the mechanisms that individuals and/or other parties who feel harmed can pursue through a dispute resolution institution. According to the Personal Data Protection Law, it is stipulated that those who feel aggrieved may report their loss and seek dispute resolution through arbitration, court, or other alternative dispute resolution institutions. The dispute resolution procedure to be followed is determined by the institution chosen by the aggrieved party, with the applicable procedural law for resolving the dispute and/or the judicial data protection process being carried out in accordance with the procedural law of the chosen dispute

resolution institution, as well as the provisions of relevant laws and regulations. Court hearings may be held in closed sessions when necessary to protect personal data. The legitimate evidence in the examination of the case under the Personal Data Protection Law includes:

- a. Evidence in accordance with the procedural law of each dispute resolution institution; and
- b. Other evidence is in the form of electronic information and/or electronic documents in accordance with the applicable laws and regulations.

5 Conclusions

Legal Reflection and Recommendations for Regulatory Advancements

The management of public health data in Indonesia has experienced rapid development in line with digital transformation and the utilization of Big Data within health information systems. The Health Law and the Personal Data Protection Law provide a legal framework to ensure privacy rights and the security of health data, while also opening opportunities for the strategic use of data in policy formulation and more holistic and efficient healthcare services.

Big Data in Healthcare administrators (particularly in this case, Health Information System administrators) must adhere to the provisions for personal data protection as outlined in the Health Law and the Personal Data Protection Law. It can be understood that the protection of personal data within Big Data in Healthcare is already regulated by the Health Law and the Personal Data Protection Law.

However, in terms of implementation, the main challenge lies in the suboptimal execution of the Personal Data Protection Law, including the absence of implementing regulations and a functional personal data protection authority, which are mandated by the Personal Data Protection Law. Upon closer examination, there are several issues that need to be addressed, as the implementing regulations for the Personal Data Protection Law have yet to be issued since its enactment. Moreover, the deadline for issuing these regulations has passed. This has resulted in an uneven understanding and compliance with personal data protection, especially at the level of healthcare facilities that control the data. The potential for misuse and health data breaches remains a serious risk that could undermine public trust in the healthcare service system.

Given the importance of the authority, tasks, and functions of the personal data protection authority in implementing personal data protection as per the Personal Data Protection Law, it is essential for the government to take immediate action to:

- a. Establish the personal data protection authority to ensure the protection of personal data in accordance with the Personal Data Protection Law mandate.
- b. Develop comprehensive and clear implementing regulations for the Personal Data Protection Law that are applicable to health data management.
- c. Enhance human resource capacity through training and adequate infrastructure support for managing health information systems in accordance with applicable regulations.

- d. Raise awareness of patient data rights through massive educational efforts to the public regarding their rights as personal data subjects, including the right to know, access, and control their health data.
- e. Implement data security audit systems and certifications to ensure compliance with data protection standards and mitigate potential violations or data breaches.

References

1. A. Ananta & S. H. Hatmadji. Mutu modal manusia: suatu analisis pendahuluan. Lembaga Demografi Fakultas Ekonomi Universitas Indonesia (1985).
2. I. D. G. K. Wisana. Kesehatan sebagai suatu investasi. *Jurnal Ekonomi dan Pembangunan Indonesia*. 1(2): 42–51 (2001).
3. Badan Legislasi DPR RI. Naskah akademik RUU tentang Kesehatan. BALEG RJ 20230216 115014 6297.pdf (2023).
4. V. Safitri & H. Noviarita. Modal manusia: pendidikan, kesehatan dalam pembangunan ekonomi. *SALAM: Islamic Economics Journal*. 3(1): 80–100 (2022).
5. G. H. Saunders et al. Application of Big Data to support evidence based public health policy decision making for hearing. *Ear & Hearing*. 41: 1057–1063 (2020).
6. D. N. Hakim, F. Ramadan & Y. I. Cahyono. Studi pemanfaatan Big Data dalam perumusan kebijakan publik pada sektor kesehatan. *SPECTA Journal of Technology*. 5(3): 308–322 (2021).
7. T. W. Sulaiman, B. Fitriansyah, R. Alaudin & M. H. Ratsanjani. Literature review: penerapan Big Data dalam kesehatan masyarakat. *SATUKATA: Jurnal Sains, Teknik, dan Studi Kemasyarakatan*. 1(3): 129–138 (2023).
8. E. D. Absharina & E. S. Negara. Penerapan model EUCS dan Delone and McLean untuk melihat tingkat kesuksesan dan kepuasan pengguna dalam penerapan aplikasi RF Mobile. *Jurnal Ilmiah Betrik*. 14(03): 445–458 (2023).
9. W. Handiwidjojo. Rekam medis elektronik. *Jurnal Eksplorasi Karya Sistem Informasi dan Sains*. 2(1): – (2015).
10. A. Annan. Tinjauan yuridis perlindungan data pribadi pada sektor kesehatan berdasarkan Undang Undang No. 27 Tahun 2022. *Synergy: Jurnal Ilmiah Multidisiplin*. 1(4): 247–254 (2024).
11. N. Elgendy & A. Elragal. Big Data analytics in support of the decision-making process. *Procedia Computer Science*. 100: 1071–1084 (2016).
12. S. S. N. Sudaryanto & F. B. Desain model integrasi data terstruktur (heterogen) untuk mendukung analisis Big Data kesehatan. In: *Seminar Nasional Industri dan Teknologi (SNIT) Politeknik Negeri Bengkalis*. 217–226 (2018).
13. Z. A. Al Sai & L. M. Abualigah. Big Data and E Government: a review. In: *2017 8th International Conference on Information Technology (ICIT)*. 580–587 (2017).
14. S. Giest. Big Data for policymaking: fad or fast-track? *Policy Sci*. 50: 367–382 (2017). DOI: 10.1007/s11077-017-9293-1.
15. F. P. Nugraha, H. Ritchi & Z. Adrianto. Interaksi Big Data, kualitas data, dan kinerja keputusan: studi kasus BPJS Kesehatan. *Jurnal Pendidikan Akuntansi & Keuangan*. 11(2): 224–238 (2023).
16. S. Suharni. Eksplorasi metode pengolahan Big Data untuk pemodelan prediktif dalam bidang kesehatan. *Jurnal Review Pendidikan dan Pengajaran*. 7(1): 1353–1360 (2024).

17. M. Nurmallasari, W. Z. Qomarania, N. A. Temesvari & T. S. Pertiwi. Bimbingan teknis peramalan jumlah kunjungan pasien dengan Tableau. *Indonesian Journal of Health Information Management Service (IJHIMS)*. 1(1): – (2021).
18. S. I. Putri and P. S. Akbar. *Health Information System*. Uwais Inspirasi Indonesia (2019).
19. C. Sorisa, C. L. Kiareni & J. Parhusip. Etika keamanan siber: studi kasus kebocoran data BPJS Kesehatan di Indonesia. *Journal Sains Student Research*. 2(6): 586–593 (2024).
20. A. H. S. Nusantara, I. K. Umam & M. Lubis. Jaminan informasi dan keamanan yang lebih baik: studi kasus BPJS Kesehatan. *Nuansa Informatika*. 18(2): 120–127 (2024).
21. W. S. Widiarty. *Buku Ajar Metode Penelitian Hukum*. Yogyakarta: Publika Global Media (2024), hlm 19.
22. P. M. Marzuki. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group (2010), hlm. 47.
23. Muhaimin. *Metode Penelitian Hukum*. Mataram: Mataram University Press (2020), hlm. 48.
24. W. S. Widiarty, *Buku Ajar Metode Penelitian Hukum*. Yogyakarta: Publika Global Media (2024), hlm. 35-36.
25. Ishaq. *Metode Penelitian Hukum dan Penulisan Skripsi, Tesis, serta Disertasi*. Bandung: Alfabeta (2017), hlm. 67.
26. S. Soekanto and S. Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo Persada (2010), hlm. 13.
27. P. M. Marzuki. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group (2010), hlm. 141.
28. P. M. Marzuki. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group (2010), hlm. 141.
29. B. Sunggono, *Metodologi Penelitian Hukum*. Jakarta: RajaGrafindo Persada (1998), hlm. 119.
30. A. Muhammad, *Hukum dan Penelitian Hukum*. Bandung: Citra Aditya Bakti (2004), hlm. 81.
31. J. Ibrahim, *Teori dan Metode Penelitian Hukum Normatif*. Malang: Bayumedia (2005), hlm. 338.
32. Muhaimin. *Metode Penelitian Hukum*. Mataram: Mataram University Press (2020), hlm. 71.
33. Law Number 17 of 2023 on Health.
34. Law Number 27 of 2022 on Personal Data Protection.
35. C. Meher, R. Sidi & I. Risdawati. Penggunaan data kesehatan pribadi dalam era Big Data: tantangan hukum dan kebijakan di Indonesia. *Jurnal Ners*. 7(2): 864–870 (2023).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits any noncommercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if you modified the licensed material. You do not have permission under this license to share adapted material derived from this chapter or parts of it.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

