Health Data Protection and Patient Privacy in the Context of Digitalization Public Health Services in Indonesia

Syahrial[1], Rineke Sara[2]
{syahrial699@gmail.com[1], rineke_sara@borobudur.ac.id[2]}

Universitas Borobudur[1, 2]

Abstract. Digital healthcare services have emerged as one of the innovations in current information technology development, garnering increasing attention from the public since the onset of the COVID-19 pandemic. The utilization of digital healthcare services necessitates the health data, rendering it a sensitive matter with the potential to raise legal issues, thus requiring regulations concerning personal data protection. However, in its implementation, the assurance of health data and patient privacy in the digitalization of the healthcare sector remains unrealized. This raises legal issues regarding patient data protection and privacy, as well as their legal protection in the digital era. To address this question, the research analysis utilizes a normative juridical research approach. The results of the study show the foremost concern regarding the legal issue of patient data protection and privacy is the security of the data. There are also threats associated with the use of technology in the digital era. Patient data and privacy are protected by the 1945 Constitution of the Republic of Indonesia and the Personal Data Protection Law. Nevertheless, careful implementation is necessary to prevent further cases related to data breaches or patient privacy infringement.

Keywords: Health Data, Patient Privacy, Digitalization

1 Introduction

Paragraph (1) of Article 28H in the 1945 Constitution of Indonesia confirms that "everyone has the right to obtain health services" and Article 34 Paragraph (3) mandates the 1945 Constitution of the Republic of Indonesia that "The State Responsible for providing health service facilities and public service facilities worthy". These provisions can provide services that health services are very important and improve its quality by the Government according to standards and technological advances applies.

The increasing use of information systems and technological advancements have resulted in a global population that is more reliant on information. [1] Further, the dissolution of the monarchy has transformed the way the general public lives and works, which were formerly done in a conventional manner, into a modern one through the use of digital technology. The current society has almost completely entered the phase of transitioning out of the industrial revolution 4.0 era due to the emergence of the industrial revolution 5.0, which happened more quickly thanks to the advancement of 5G telecommunication technology and the corresponding digital platforms. [2]

ICLSSEE 2024, May 25, Jakarta, Indonesia

DOI 10.4108/eai.25-5-2024.2349352

Such occurrences are likely to have a significant impact on the efficiency and innovation of digital transformation. One major advancement in health care today is digital health, or electronic health (e-health), which is becoming more and more sophisticated and is becoming a concern for the general public since the COVID-19 pandemic. Utilizing digital technology in the health sector can improve patient care by interacting with relevant stakeholders and enhancing patient care, capabilities, and efficiency.[3] However, using digital health tools will require consumer personal information, which can become sensitive information and potentially cause legal issues if not handled properly. Therefore, countries must take action to keep up with the advancement of technology in the digital age by providing protection for the private health data of users of digitally based services.

On a global scale, various policies and guidelines exist regarding digital health, one example being the Global Digital Health Strategy 2020–2025 released by the World Health Organization (WHO). This strategy is aimed at improving service systems based on digital health technology for patients, professionals, and healthcare supervisors in hospitals and other healthcare facilities. Its goal is to transform the industry towards patient empowerment and realize the vision of health for all. The strategy is crafted to be adopted by Member States facing challenges in accessing digital technologies, products, and services.[4] On an international level, there are several policies and guidelines regarding digital health, one of which is the World Health Organization (WHO) that released the Global Digital Health Strategy 2020–2025. This strategy seeks to improve healthcare systems by using digital health technologies for patients, healthcare professionals, and service providers. This transformation aims to empower patients and work towards the goal of health for all. It is tailored to be adopted by Member States that have limited access to digital technologies, products, and services.

The medical record system in Singapore has transitioned to health data storage since the launch of the National Electronic Health Record system in 2011. The implementation of this system has also been adopted by other Asian countries like Thailand and South Korea, which have strong healthcare models. However, experts in India have expressed concerns about the broad digital policy, indicating significant capacity limitations, transportation challenges in rural areas, and issues such as resource scarcity and specific conditions hindering the capacity and full realization of health digitization in the country.

"Data is the new oil," a phrase that highlights the significance of data in the current digital era and the need to protect it from potential threats. This is also stated by President Joko Widodo, who clarifies that data represents a new category of knowledge for the masses, meaning that Indonesia must embrace data sovereignty.[5] As a legal state, Indonesia guarantees personal data protection through its national constitution, the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945). This is stipulated in Article 28G, which determines that the protection of personal dignity and security forms the constitutional basis for safeguarding personal data as a fundamental human right.

In the Public Health Services Sector, health data, including specific or sensitive data, necessitates protection of patients' personal data as consumers due to containing confidential information such as health test results, types of diseases, residential details, phone numbers, and others. [6] Hence, concerning such data, “protection is provided through the enactment of Law Number 17 of 2023 concerning Health (hereinafter referred to as the Health Law 2023). Meanwhile, in the digital sector, personal data protection is regulated under Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Information and Electronic Transactions

(hereinafter referred to as the ITE Law) and Law Number 27 of 2022 on Personal Data Protection (hereinafter referred to as the Personal Data Protection Law)."

Despite being regulated by relevant legislation, the implementation of personal data protection in the digital public health service sector has not yet materialized. This situation indicates that the existing legal instruments do not currently provide adequate guarantees for personal data protection in the digital public health service sector. Therefore, innovative efforts are needed as a strategy for personal data protection in the digital era, particularly in the public health service sector. "The public health service sector in Indonesia faces challenges in data protection, data standardization, as well as patient rights and privacy Interoperability capabilities are required to integrate all information systems and applications into a centralized database", aimed at facilitating users, both patients, and service providers.

This study is descriptive and utilizes a normative juridical research approach. This legal investigation involves analyzing "library materials or secondary data, including primary legal sources, secondary legal sources, and tertiary legal sources. The primary legal materials used consist of legislation. The secondary legal materials used consist of books, journals, and other research." Subsequently, the tertiary legal materials used include newspapers and internet articles

2 Discussion

2.1 The Issue of Healthcare Data Protection and Patient Privacy in The Public Health Services Sector.

The implementation of digitalization programs faces various challenges, including the fact that Indonesia's healthcare infrastructure lacks nearly half of the number of doctors, nurses, medical personnel, and healthcare facilities recommended by the WHO to adequately serve the population. [7] For many years, overburdened and insufficient budgetary support, the Indonesia country healthcare system under strain managing infectious diseases like tuberculosis and neglected tropical diseases, as well as lifestyle disorders such as diabetes, stroke and cardiovascular and neurological issues). [8]

Current understanding meaning of speaks to privacy, which essentially generally covers individuals' or groups' ability to determine when to keep something private, how those conditions deemed important to be kept private are, and to what extent the communicated information is limited in being known by others. "Although this understanding of privacy is more progressive than oath-based concepts, it fundamentally fails to cover all types of privacy. In comparison, in digital health, privacy can be categorized into two types: informational and physical." [9]

Physical privacy is when digital health reduces the number of doctor visits to homes and in-person clinic visits. However, this also poses a threat to informational privacy since patients medical data is stored online, making it susceptible to unauthorized use and vulnerabilities. It is important to note that not only are there more than just these two types of privacy, but they can also "the conflict with each other, potentially requiring trade-offs between them. According to the Stanford Encyclopedia of Philosophy, the most crucial types of privacy for ensuring data protection in digital health services are informational privacy and decisional privacy." As

mentioned, informational privacy typically involves the protection and security of data, especially in monitoring health, particularly with the increasing use of DNA tests and electronic copies of medical records, which can indicate limited control over medical privacy. Decisional privacy in the medical context usually refers to autonomy in health-related decision-making refers to the right of individuals to make choices about their own medical care and treatment, such as cases of contraception and abortion, which require reproductive autonomy and decision-making. This decisional privacy also encompasses the right to refuse medical services when there is a need for consent and action from the concerned party, consciously agreeing or disagreeing.

The meaning of privacy and confidentiality, although similar, have inherent differences, where confidentiality involves a relational aspect and the involvement of two parties, occurring when personal information is disclosed by one person to another with the expectation that the information will remain secret. For instance, in the doctor-patient relationship, it resembles a therapeutic transaction that requires confidentiality and consent. With such an agreement, if breached, like violating patient privacy, it can lead to diminished trust in healthcare providers, and patients become reluctant to share personal information. Especially when patients face issues that might carry a negative stigma, such as risky sexual behavior leading to HIV, substance abuse like marijuana or other drugs, or mental health problems. risky sexual behavior, substance abuse, and mental health problems are interconnected and can have serious consequences on an individual's health and well-being. Addressing these issues requires comprehensive approaches that focus on prevention, education, access to healthcare services, and support for mental health and substance abuse treatment.

Privacy is an integral part of all forms of healthcare, including digital health services. In the context of modern Indonesia, which increasingly relies on technology, there is a growing need to protect patients' medical data. Measures must be “put in place to control who has access to this data, and patient information should only be released with the patient's consent.”

In Indonesia, legal protection regarding personal data is still considered suboptimal. Issues such as the misuse of personal data, which still commonly occurs without the knowledge of its owners, highlight privacy violations that may occur to individuals. This problem of personal data misuse indicates loopholes in supervision and weaknesses in the system that allow for information misuse, potentially harming data owners. This is evident in the case of leaked data of BPJS Kesehatan patients, where according to the spokesperson of the Ministry of Communication and Informatics, Dedy Permadi, there are allegations of 279 million BPJS Kesehatan data being leaked and traded on a forum.[10]

The Coordinator of Advocacy Division at BPJS Watch, Timboel Siregar, explained that there are two alleged causes of data leakage in the BPJS Kesehatan case. Firstly, the data leakage is attributed to hacking in third-party applications. Based on his analysis, BPJS Kesehatan has numerous applications, including eight applications in the healthcare service assurance management information system, six applications in the public service information system, and six applications supporting the membership management information system. Considering the multitude of applications owned by BPJS Kesehatan, he suspects that the leakage is due to hacking, particularly in the membership management information system application and healthcare service application. Secondly, there is an allegation of data leakage perpetrated by internal parties. Timboel evaluates that the hacking incident demonstrates the inadequacy of security measures in BPJS Kesehatan's applications. [10]

The case of data leakage in BPJS Kesehatan above serves as evidence that patients' personal data in the The Public Health Services Sector are susceptible to misuse. Patients' personal data establishes a connection between the patients and healthcare service providers, extending beyond registration information to include other data. Nowadays, in Indonesia, healthcare service providers extensively utilize technological assistance in processing patient data, rendering it digital. Therefore, this issue warrants serious attention to provide legal protection for personal and health data, which should not be disclosed to the public unless authorized by law, as the breach of patient data confidentiality violates legal provisions.

Personal data in the The Public Health Services Sector, which is confidential and private, consists of patients' personal identities, such as name, phone number, address, and others. Additionally, it pertains to medical secrets resulting from examinations conducted on patients. Consequently, patients have the right to privacy and confidentiality regarding their medical conditions and information, making patient confidentiality crucial. This extends to digital healthcare services, where the collection of sensitive personal patient data necessitates protection to the extent that healthcare service providers can safeguard patients' personal data in e-health.

Several types of security threats should be taken into account regarding Health Data and Patient Privacy, namely malware attacks, DDoS attacks, phishing attacks, man-in-the-middle attacks, and data loss or theft. Malware in this context refers to malicious software that can damage or take control of health information systems. Common types of malware include viruses, worms, and Trojans. Next, Distributed Denial of Service (DDoS) attacks are aimed at shutting down access to health information systems by redirecting network traffic and rendering the system unresponsive. Phishing attacks are attempts to obtain personal or confidential information by impersonating trustworthy entities. An example is a fake email directing users to submit login information or passwords to a fake website. Furthermore, man-in-the-middle attacks are a type of attack where hackers attempt to intercept communication between two parties and obtain transmitted information. Lastly, data loss or theft is the most common security threat to healthcare information systems. This can occur when hackers gain access to the system or when information is stored on insecure media. [11]

2.2 Health Data Protection and Patient Privacy in the Digital Era

Data is considered personal data if it relates to an individual, thus enabling the identification of that person, who is the data subject. [12] For example, For example, “A phone number on a blank sheet is not personal data because it cannot be used to identify the owner, whereas data that includes both the phone number and the owner's name can be used for identification and is therefore considered personal data.” The explanation connects the concept of personal data with its ability to identify individuals. This reflects a good understanding of the basic concept of personal data.

An identifiable person is someone who can be recognized directly or indirectly based on identifiers. “Basically, individuals who can be identified directly or indirectly through identifiers or specific factors related to their physical, psychological, mental, cultural, or social identity. The legal entity protected in the personal data protection mechanism is the individual (natural person), so other legal entities (referred as legal entity) are not an identifiable person. [13] The right to personal data protection stems from the right to respect for private life. The

concept of private life pertains to humans as living beings. Therefore, individuals are the primary holders of the right to personal data protection." [14]

Digitalization of health services involves two main components: "the utilization of technology to deliver health services and the digitalization of medical data. The digitalization of medical data includes the creation of Electronic Health Records (EHR), which are digital versions of patients' health records that allow doctors to access comprehensive health histories wherever and whenever the data is collected, significantly simplifying the medical service process."[15] A comprehensive legal and regulatory framework is required to support digitalization projects to harness the vast potential while embracing the benefits of digital health services, such as telemedicine and health information systems, it's crucial to ensure that legal and regulatory measures are in place to protect patient rights, privacy, and confidentiality. These regulations should address issues like data security, patient consent, interoperability, and the ethical use of technology in healthcare.

The regulations on privacy and personal data protection are stipulated in Article 28G of UUD NRI 1945, which governs the right to *"protect personal, family, honor, dignity, and property under one's control."* To understand these regulations concerning privacy and personal data, about the text accurately conveys the original meaning using different words. That explains the interpretation of privacy and personal data protection according to "Warren and Brandeis's perspective, emphasizing the right to live freely and have one's emotions and thoughts respected. Warren and Brandeis's viewpoint in their work *The Right to Privacy* suggests that privacy entails the right to live freely and to have one's emotions and thoughts respected."[16] Explanation about the relationship between privacy and personal protection according to Allan Westin's explanation, privacy is the right to determine the disclosure of information as informational privacy, which is well conveyed where privacy protection itself is closely related to the fulfillment of the right to personal data Based on Article 28G of UUD NRI 1945, personal data protection in Indonesia is dispersed across various laws.

According to that, the relationship between privacy and personal data is clear and consider were making fit the concept to involves the right to control the disclosure of information, particularly personal data. Additionally, personal data protection is a form of privacy protection directly mandated by UUD NRI 1945, encompassing respect for human rights values, equality, and individual rights. Therefore, a legal foundation is needed to enhance privacy and personal data security and to ensure the creation of a conducive business environment. privacy protection is closely related to ensuring individuals' rights over their personal data are fulfilled.

Several privacy and personal data protection laws outside Indonesia, such as the European Union Directive, differentiate between "sensitive" and "non-sensitive" data based on the perceived risk to individuals if accessed by unauthorized parties. One type of sensitive data is health-related information. In this context, Indonesia has regulations on privacy and personal data protection for health data. Indonesia ensures that every individual has the right to the confidentiality of personal conditions disclosed to healthcare providers.[14] However, health laws do not explicitly state that personal health data is sensitive. Thus, Indonesia has not yet differentiated between general personal data and sensitive personal data. However, sensitive personal data requires higher protection compared to general personal data.

Personally identifiable health data can be exploited for identity theft, medical fraud, or even physical threats to the individuals concerned. Therefore, protecting health information

must be a top priority for all healthcare organizations and information technology companies providing health services. This protection can be achieved by implementing stringent security and privacy standards, such as “the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in the European Union.”

The Health Insurance Portability and Accountability Act (HIPAA) in the United States focuses on the protection of privacy and security of health information. It strengthens patient privacy rights and mandates hospitals, clinics, and other healthcare institutions to safeguard patient health information. Similarly, the General Data Protection Regulation (GDPR) in the European Union aims to protect the personal data of EU citizens, including health information. GDPR requires companies to protect personal data and provide access to individuals whose personal data has been collected. These laws represent significant steps in ensuring the confidentiality and security of health data, both in the United States and the European Union, thereby enhancing trust in healthcare systems and promoting patient privacy rights globally.

The enactment of the Personal Data Protection Law represents one of Indonesia's advancements in safeguarding health data and patient privacy. Under the Data Protection Law, personal data is categorized into two groups: general personal data and specific personal data. General personal data refers to information that can be obtained publicly and is listed in official documents, the unauthorized disclosure of which could harm the Personal Data Owner, such as full name, gender, residential address, and others. Meanwhile, specific personal data pertains to sensitive information that affects the comfort and security of the Personal Data Owner and can only be obtained with the owner's consent unless otherwise specified by law. Unauthorized disclosure of this data could violate the privacy of the Personal Data Owner, including health information, biometric data, genetic data, and others.

The presence of the Personal Data Protection Law (PDPL) is expected to limit the misuse, leakage, and trading of personal data arising from cyber-attacks, human error, and system failures. However, the implementation of the Personal Data Protection Law also requires an increase in information security literacy. Many hospitals still use pirated software and do not utilize official applications, and even the internet security in hospitals is inadequate. Additionally, the healthcare sector faces challenges in protecting data spread across various platforms, especially with the proliferation of endpoints created by the Internet of Medical Things (IoMT), exposing vulnerabilities that have not been fully addressed. Choosing a secure electronic medical record system in accordance with the Personal Data Protection Law is a crucial step in keeping patients' personal data safe and complying with the law

3 Conclusion

The issue of data protection in healthcare services and patient privacy in the public healthcare sector is widely encountered in the field. Privacy in the context of digital health encompasses both informational and physical privacy. While technological advancements can enhance the accessibility of healthcare services, they also pose threats to privacy as patients' medical data are stored online and vulnerable to breaches. Additionally, there are other security threats such as malware attacks, DDoS attacks, phishing attacks, man-in-the-middle attacks, and data loss or theft. Protecting patients' health data from these threats becomes an urgent priority.

Legal Protection of Health Data and Patient Privacy in the Digital Era has been undertaken by the Indonesian government through the enactment of the Data Protection Law. The Data Protection Law represents a significant step forward in safeguarding the confidentiality and security of health data. However, implementing these regulations requires an increase in information security literacy and the selection of appropriate electronic medical record systems. This can be supported by healthcare systems in some countries, such as the United States and the European Union, which have stringent regulations on the protection of privacy and security of health information, such as HIPAA and GPR. This enhances trust in the healthcare system and promotes patients' privacy rights globally. Therefore, the protection of personal data in the context of digitizing healthcare services requires a comprehensive legal framework, stringent security standards, and an increase in information security literacy to ensure the confidentiality, security, and integrity of patient health data

References

[1] D. Budhijanto, *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi : Regulasi dan Konvergensi*. Bandung: PT Refika Adhitama, 2010.

[2] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "A Literature Review of the Challenges and Opportunities of the Transition from Industry 4.0 to Society 5.0," *Energies (Basel)*, vol. 15, no. 17, p. 6276, Aug. 2022, doi: 10.3390/en15176276.

[3] H. P. Utomo, E. Gultom, and A. Afriana, "URGENSI PERLINDUNGAN HUKUM DATA PRIBADI PASIEN DALAM PELAYANAN KESEHATAN BERBASIS TEKNOLOGI DI INDONESIA," *Jurnal Ilmiah Galuh Justisi*, vol. 8, no. 2, p. 168, Sep. 2020, doi: 10.25157/justisi.v8i2.3479.

[4] World Health Organization, "Global strategy on digital health 2020-2025," Geneva, 2021.

[5] N. Ro'is, "Cyber Sovereignty Gotong Royong, Indonesia'a Way of Dealing with the Challenges of Global Cyber Sovereignty," *Pancasila and Law Review*, vol. 3, no. 1, pp. 15–30, Jun. 2022, doi: 10.25041/plr.v3i1.2573.

[6] A. N. Mahira, "Perlindungan Hukum Terhadap Kerahasiaan Data Kesehatan Pasien Berdasarkan Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan.," *Dinamika: Jurnal Ilmiah Ilmu Hukum*, vol. 27, no. 10, pp. 1501–1516, 2021.

[7] S. Ranganathan, "Towards a Holistic Digital Health Ecosystem in India," *ORF Issue Brief No. 351*, 2020.

[8] R. Gillon, "Consent.," *BMJ*, vol. 291, no. 6510, pp. 1700–1701, Dec. 1985, doi: 10.1136/bmj.291.6510.1700.

[9] A. L. Allen, "Privacy and Medicine," 2009.

[10] E. A. Frahma, "Juridical Analysis of Patient Data Protection in National Legal Perspective," *Untag Law Review*, vol. 8, no. 1, 2024.

[11] G. Arie, *Pengantar Sistem Informasi Kesehatan*. Malang: PT. Literasi Nusantara Abadi Grup, 2023.

[12] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*. France: European Union Agency for Fundamental Rights and Council of Europe, 2018.

[13] *Civil Code*.

[14] Indonesian Government, *Law Number 17 of 2023 concerning Health*. Indonesia: LN 2023 (105), TLN (6887), 2023.

[15] S. Dewi Rosadi and G. Gumelar Pratama, “URGENSI PERLINDUNGAN DATA PRIVASI DALAM ERA EKONOMI DIGITAL DI INDONESIA,” *Veritas et Justitia*, vol. 4, no. 1, pp. 88–110, Jun. 2018, doi: 10.25123/vej.2916.

[16] M. M. M. Pai, R. Ganiga, R. M. Pai, and R. K. Sinha, “Standard electronic health record (EHR) framework for Indian healthcare system,” *Health Serv Outcomes Res Methodol*, vol. 21, no. 3, pp. 339–362, Sep. 2021, doi: 10.1007/s10742-020-00238-0.