WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

Strengthening the Principle of Beneficence in Safeguarding Patient Data Confidentiality: An Analysis of the Roles and Responsibilities of Hospitals

Ontran Sumantri Riyanto[a], Fuad[b]
[a] Sekolah Tinggi Ilmu Kesehatan Bethesda Yakkum, Yogyakarta, Indonesia, Email: ontran27@yahoo.co.id
[b] Fakultas Hukum Universitas Widya Mataram Yogyakarta, Email: sangfuad2019@gmail.com

Abstract

Confidentiality of patient data is a crucial aspect of healthcare services, supporting accurate medical decision-making and maintaining public trust. This study aims to analyze the role of hospitals in safeguarding patient data confidentiality through the application of the principle of beneficence. The research adopts a qualitative methodology with a descriptive approach, utilizing in-depth analysis to explore technical, legal, and ethical aspects of patient data management. Data collection techniques include interviews with medical personnel, observations of data management procedures, and reviews of data protection policies implemented by hospitals. This study examines strengthening hospitals' roles and responsibilities in protecting patient data confidentiality based on the principle of beneficence, as mandated by Law No. 17 of 2023 on Health. Hospitals are obligated to store and safeguard patient data at the highest standards, yet challenges arise with advancements in digital technology that increase the risk of data breaches. Additionally, medical personnel's lack of training in protecting patient data privacy poses another significant issue. Hospitals need to design clear internal policies and implement adequate security systems, such as encryption and access control. Further discussion highlights a beneficence-based model of responsibility, which prioritizes the patient's best interests, including transparency in patient data management. Therefore, hospitals must enhance their data protection mechanisms by integrating the principle of beneficence to build patient trust and comply with legal obligations.

Keywords: *Patient Data; Principle of Beneficence; Hospitals; Responsibility*

A. Introduction

Patient data confidentiality is a vital element of healthcare services, serving not only to maintain public trust but also to support accurate medical decision-making[1]. Breaches of data confidentiality can have serious consequences, both for patients and for medical professionals responsible for its protection[2]. Therefore, safeguarding patient data confidentiality is an integral part of improving the quality of healthcare services while also reflecting respect for individuals' right to privacy. Every individual has the right to decide whether their data will be shared or not. This right also includes the authority to determine the terms and conditions related to the transfer or sharing of such data. The right to privacy has evolved into a legal foundation for protecting personal data, recognized as part of the constitutional rights of citizens. Consequently, the confidentiality of patient data must be upheld as a manifestation of respect for patients' dignity and the protection of their rights[3].

[1] Ahmad Darmawan, "Analisis Pelepasan Informasi Rekam Medis Sebagai Penjamin Aspek Hukum Kerahasiaan Data Pasien," *Jurnal Manajemen Informasi Kesehatan Indonesia (JMIKI)* 11, no. 1 (2023).
[2] Samsul Bahri et al., "Implementasi Perlindungan Hukum Pasien Tentang Rahasia Kedokteran (Studi Pada Rumah Sakit Pertamina Bintang Amin Bandar Lampung)," *Jurnal Hukum Malahayati* 3, no. 1 (2022).
[3] Sitti Aminah K and Ashabul Kahpi, "Tinjauan Terhadap Hak Dan Kewajiban Pasien Dalam Pelayanan Kesehatan," *Alauddin Law Development Journal* 3, no. 3 (2021).

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

Information related to patients' data is central to medical confidentiality, also known as medical secrecy. Medical secrecy is a patient's right that every medical professional, healthcare facility, and other related parties must respect[4]. Protecting this right not only preserves the dignity of patients but also fosters trust, which serves as the cornerstone of the relationship between patients and medical professionals[5]. In this regard, hospitals play a crucial role in ensuring that patients' rights to data confidentiality are adequately protected.

The significance of patient data confidentiality is rooted not only in ethical values but also in a strong legal framework. Article 28G Paragraph (1) of the 1945 Constitution of the Republic of Indonesia states that "every person has the right to protection of their personal privacy, family, honor, dignity, and property under their control, as well as the right to security and protection from fear of threats to perform or refrain from performing something that constitutes their human right." This provision underscores the importance of the right to self-protection, including the confidentiality of personal data.

Hospitals have both ethical and legal obligations to protect patient data[6]. This responsibility not only reflects compliance with regulations but also aligns with the principle of beneficence, which emphasizes the well-being and best interests of patients. Legal protection for patient data confidentiality is part of the state's duty to uphold its citizens' constitutional rights. Public trust in hospitals heavily relies on these institutions' consistent and accountable efforts to safeguard patient data confidentiality[7].

Law No. 17 of 2023 on Health, Article 4 Paragraph (i), explicitly states that every individual has the right to the confidentiality of their personal health data and information. Furthermore, Law No. 27 of 2022 on Personal Data Protection, Article 4, categorizes health data as specific personal data that requires stricter protection. In this context, hospitals must ensure that patient health data remains confidential and that it is processed with the utmost care to prevent misuse.

In today's digital era, the challenges of maintaining patient data confidentiality have intensified, particularly with the rapid development of information technology in health data

[4] Marini V. Pandi, "Sanksi Pidana Atas Pelanggaran Rahasia Kedokteran Oleh Dokter," *Lex et Societatis* I, no. 2 (2013).
[5] Arif Wicaksana and Tahar Rachman, "Rahasia Kedokteran Di Antara Moral Dan Hukum Profesi Dokter," *Angewandte Chemie International Edition, 6(11), 951–952.* 3, no. 1 (2018).
[6] Arya Wirai Khalifatullah et al., "Perlindungan Data Pribadi Pasien Terhadap Serangan Cyber Crime," *Sanskara Hukum dan HAM* 1, no. 02 (2022).
[7] Calvin Anthony Putra and Muh Ali Masnun, "Analisis Pertanggungjawaban Rumah Sakit Terkait Potensi Kebocoran Data Rekam Medis Elektronik Akibat Cyber Crime," *Novum : Jurnal Hukum* 9, no. 2 (2022).

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

management[8]. While digitalization in the healthcare sector has brought convenience, it has also heightened risks such as data breaches and information misuse. For example, the 2021 breach of Social Security Agency for Health user data, involving approximately 279 million personal records of Indonesian citizens, highlighted the critical need for more cautious data management[9]. This incident exposed significant risks in managing health data and underscored the necessity for stricter security measures. Such breaches not only risk the misuse of personal information but also erode public trust in the national healthcare system[10]. A similar case occurred at a private hospital in Jakarta, where patient medical records were used without authorization for non-medical purposes. These incidents reveal gaps in the data protection system that must be urgently addressed by strengthening the accountability of medical professionals and healthcare facilities.

The principle of beneficence, which emphasizes medical professionals' obligation to act in the best interests of patients and prevent potential harm[11]. Applying this principle aims to safeguard patient data confidentiality by ensuring that personal and health information is not only protected but also used for legitimate and beneficial purposes[12]. Moreover, the application of the beneficence principle becomes crucial in addressing challenges arising from the use of health data for research or other purposes that require balancing individual interests with collective needs.

Strengthening the beneficence principle in maintaining patient data confidentiality requires a systemic approach involving medical professionals, healthcare facilities, and supportive regulations[13]. Hospitals are responsible for developing clear data protection policies, while medical professionals must be adequately trained to understand the technical, legal, and ethical aspects of managing patient data. Enhancing this accountability aims to prevent privacy violations and foster a healthcare ecosystem that is safe, transparent, and

[8] Handryas Prasetyo Utomo, Elisatris Gultom, and Anita Afriana, "Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Teknologi Di Indonesia," *Jurnal Ilmiah Galuh Justisi* 8, no. 2 (2020).
[9] Syailendra caesar akbar, Persada, "6 Kasus Kebocoran Data Pribadi Di Indonesia," *Tempo.Com*.
[10] Calvin Anthony Putra and Muh Ali Masnun, "Analisis Pertanggungjawaban Rumah Sakit Terkait Potensi Kebocoran Data Rekam Medis Elektronik Akibat Cyber Crime," *Novum : Jurnal Hukum* 9, no. 2 (2022): 1–14.
[11] Johan Christiaan Bester, "Beneficence, Interests, and Wellbeing in Medicine: What It Means to Provide Benefit to Patients," *American Journal of Bioethics* 20, no. 3 (2020).
[12] Basil Varkey, "Principles of Clinical Ethics and Their Application to Practice," *Medical Principles and Practice*, 2021.
[13] Lynn A. Jansen, "Medical Beneficence, Nonmaleficence, and Patients' Well-Being," *The Journal of clinical ethics* 33, no. 1 (2022).

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

trustworthy. Collaboration among all stakeholders will ensure the protection of patient data confidentiality while reinforcing public trust in the existing healthcare system.

This study aims to analyze the role of hospitals in safeguarding patient data confidentiality through the application of the beneficence principle. The primary focus is to identify concrete steps that hospitals can take to enhance their ethical responsibilities in protecting patient data. Additionally, this research explores how a responsibility model based on the principle of beneficence can be implemented in hospital settings to ensure the adequate protection of patient data privacy. The application of this model is expected to create a system that not only prioritizes patient interests but also integrates moral and ethical values into every process of medical data management[14]. Thus, this study seeks to contribute to the development of more effective policies and practices for maintaining the confidentiality of health information within hospitals.

B. Research Method

This study uses a legal research methodology[15] to analyze the roles and responsibilities of hospitals in maintaining patient data confidentiality, focusing on the application of the principle of beneficence. The research adopts several approaches to provide a deeper understanding. The legislative approach is applied by examining Law No. 17/2023 on Health, which regulates patient data protection in Indonesia. Additionally, the conceptual approach is used by applying the beneficence principle as a foundation for evaluating hospitals' ethical obligations in protecting patient data, along with related principles such as privacy rights and patient autonomy. The research also employs a comparative approach to examine how other countries, such as the United States (under HIPAA) and European Union (under GDPR), regulate patient data protection, identifying strengths and weaknesses in Indonesia's legal framework. Utilizing a qualitative approach, the study collects data through in-depth interviews with medical professionals and hospital management, direct observations of patient data management procedures, and a review of documentation on data protection policies implemented in hospitals. This approach enables the study to offer a comprehensive

[14] Ontran Sumantri Riyanto and Fuad, "Perlindungan Hukum Praktik Kedokteran Di Rumah Sakit: Implementasi Kenyamanan Dokter Dalam Memberikan Pelayanan Kesehatan," *Juris Humanity: Jurnal Riset dan Kajian Hukum Hak Asasi Manusia* 2, no. 1 (2023): 1–14, https://www.jrkhm.org/index.php/humanity/article/view/14.
[15] Hari Sutra Disemadi, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies," *Journal of Judicial Review* 24, no. 2 (2022): 289–304.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

view of the challenges and solutions in strengthening the implementation of the beneficence principle in maintaining patient data confidentiality.

C. Results and Discussion

1. Strengthening the Role and Responsibilities of Hospitals

Strengthening the role and responsibilities of hospitals in safeguarding patient data confidentiality is a crucial aspect of maintaining integrity and trust in the relationship between patients and medical professionals. Article 4 of Law No. 17/2023 emphasizes every individual's right to the confidentiality of their personal health data and information. Hospitals, as healthcare service providers, are obligated under Article 177(1) of Law No. 17/2023 to store and protect patient health information with high standards. This serves as a fundamental basis for establishing an effective data protection system within hospitals. However, hospitals face increasingly complex challenges in maintaining patient data confidentiality due to the rapid development of digital technology, which heightens the risk of data breaches through hacking or misuse of information by unauthorized parties.

Another significant challenge is the lack of adequate training for medical professionals in understanding and implementing the principles of patient data protection in every medical action. Therefore, hospitals must take an active role in educating medical professionals through continuous training programs that integrate the principle of beneficence—requiring medical professionals to act in the best interest of patients and protect their rights, including the confidentiality of their personal data. In this context, strengthening the principle of beneficence becomes a key strategy to ensure that medical professionals not only focus on medical aspects but also uphold patient privacy as part of their moral and professional obligations[16].

Strengthening the role of medical professionals aligns with Article 274 of Law No. 17/2023, which mandates that medical and healthcare personnel must uphold patient data confidentiality. In this context, hospitals must establish clear policies, including procedures for handling patient data effectively. Article 301(1) of the same law further emphasizes this obligation, asserting that every medical professional involved in healthcare services is required to protect the confidentiality of patient health information. Therefore, hospitals

[16] Kevin O'Donoghue, "Learning Analytics within Higher Education: Autonomy, Beneficence and Non-Maleficence," *Journal of Academic Ethics* 21, no. 1 (2023).

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

must implement mechanisms to monitor and enforce compliance with these obligations rigorously and measurably.

While the digitalization of healthcare services offers efficiencies in data management[17], it also introduces new challenges in protecting sensitive information. Hospitals must adapt to advanced technologies in information security to prevent data breaches caused by hacking or technical errors. Policies governing the storage and management of patient data should include sophisticated security measures, such as data encryption and strict access controls, to safeguard patient information from unauthorized access. The implementation of robust security systems is crucial, as any breach of patient data can lead to significant harm for both patients and the hospital itself. To address these challenges, hospitals must develop comprehensive strategies to prevent data breaches and the misuse of information. These strategies should include clear internal policies and regular oversight of their implementation. Leveraging technology to minimize risks, alongside continuous training and capacity-building programs for hospital staff, is essential to reinforce the hospital's role in safeguarding patient data confidentiality. In this regard, Law No. 17/2023 provides a strong legal foundation for protecting patient data confidentiality, requiring hospitals to securely store personal health information and use it solely for legitimate purposes.

Moreover, the Ministry of Health Regulation No. 36 of 2012 on Medical Confidentiality and Law No. 27 of 2022 on Personal Data Protection impose strict obligations to protect patient data. These regulations provide a clear legal framework for healthcare facilities and personal data controllers to ensure the security of patient information. Failure to maintain confidentiality not only risks the reputation of healthcare facilities and medical professionals but also threatens patients' rights to privacy, thereby violating the principle of beneficence.

The imposition of administrative sanctions on healthcare facilities or personal data controllers that violate regulations reflects the state's commitment to enhancing the protection of patient data. Sanctions such as verbal warnings, the revocation of operational licenses, or administrative fines are designed to create a deterrent effect and ensure compliance with obligations to maintain patient data confidentiality. This approach underscores the reinforcement of the principle of beneficence, where the state strives to safeguard the well-being and fundamental rights of patients by demanding higher commitments from healthcare facilities in managing medical information.

[17] Sidhi Laksono, "Kesehatan Digital Dan Disrupsi Digital Pada Layanan Kesehatan Di Rumah Sakit," *Jurnal Kebijakan Kesehatan Indonesia* 11, no. 1 (2022): 36–42.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

Law No. 27/2022, particularly Article 36, mandates that personal data controllers safeguard confidentiality, including medical records. This provision emphasizes that protecting patient data is not merely an ethical responsibility of medical personnel but also a legal obligation. Violations of this provision may result in severe administrative sanctions, such as fines or temporary suspension of data processing activities. The transparent enforcement of these sanctions aims not only to enhance compliance but also to strengthen the protection of patients' interests by preventing potential harm or risks associated with the leakage of medical data[18]. This firm and consistent legal approach aligns with the principle of beneficence, which prioritizes patient protection. In doing so, the state ensures that patients' medical data is securely managed and used solely for legitimate purposes while encouraging healthcare facilities to improve their information security systems continually.

Integrating the principle of beneficence into every hospital policy and action, coupled with enhancing data protection systems, is a crucial step in safeguarding patients' rights to privacy and data confidentiality. The effective implementation of Law No 17/2023, which explicitly regulates the protection of patient data, provides a solid legal foundation for hospitals to fulfil this responsibility. Strengthening internal policies, utilizing advanced technology, and providing continuous training for medical professionals and all hospital staff are essential components in building a more reliable data protection system. These measures not only enhance the protection of patient data but also increase public trust in healthcare services. Ultimately, they contribute to the creation of a safer, more trustworthy medical environment that prioritizes the protection of patients' rights.

Table 1: Hospital Responsibilities and Risks in Patient Data Breaches

Aspects	Hospital Responsibilities	Risks Due to Data Leakage
Data Protection	Protect patient data from leakage	Data can be misused by unauthorized parties for criminal purposes, such as fraud.
Legal Compliance	Comply with laws related to personal data protection and patient confidentiality.	Hospitals may be subject to fines, criminal prosecutions, or administrative sanctions.
Incident Notification	Report data leaks to the relevant authorities and notify affected patients.	Failure to notify can exacerbate legal losses and public trust.

[18] Ridwan Ridwan, "Pertanggungjawaban Hukum Pidana Terhadap Pelanggaran Rahasia Medis," *Jurnal Hukum & Pembangunan* 49, no. 2 (2019): 338–348.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

Aspects	Hospital Responsibilities	Risks Due to Data Leakage
Staff Training	Provide training to staff to increase awareness of maintaining the confidentiality of patient data.	Staff negligence can increase the likelihood of breaches, including unauthorized access to data.
IT System Security	Conduct periodic audits and updates on the hospital information system.	Weak systems have the potential to be targeted by cyberattacks, such as hacking.
Reputation and Trust	Building trust by keeping patient data secure is a top priority.	Reputational damage can lead to a decrease in the number of patients using the service.

Source: Based on the research findings of this study.

Table 1 shows that hospitals are legally and ethically obligated to protect patient data to prevent misuse, such as identity theft or fraud. Non-compliance with regulations and failure to report breaches to authorities can result in legal consequences, including fines and loss of public trust. Staff training is crucial to prevent breaches caused by negligence, and regular IT system audits are necessary to mitigate cyberthreats. Hospitals must ensure transparent communication regarding data protection, especially when breaches occur, to maintain trust and minimize the risk of patient loss. By addressing these responsibilities and risks, hospitals can better protect sensitive patient information and uphold their obligations to confidentiality and ethical practice.

2. A Beneficence-Based Responsibility Model for Protecting Patient Data Privacy in Hospitals

The principle of beneficence mandates that medical professionals and hospitals focus not only on the physical well-being of patients but also on the security and confidentiality of their health data. A beneficence-based responsibility model designed for hospitals to safeguard patient data privacy should prioritize comprehensive protection of patients' personal information. Therefore, hospitals must develop internal policies that strengthen patient data protection by placing the patient's best interests as the top priority. This approach ensures that hospitals fulfil not only their legal obligations but also foster an environment that respects patients' privacy rights, ultimately strengthening the trust between patients and medical professionals. In accordance with Articles 274 and 301 of Law No. 17/2023, hospitals have a legal obligation to maintain the confidentiality of patients' health data.

Hospitals must also improve transparency with patients regarding how their data is managed and protected[19]. In many cases, patients remain unaware of how their data is stored

[19] Awaluddin Musaini, Andi Tenri, and Syahril Ramadhan, "Transparansi Pelayanan Publik Di Rumah Sakit Umum Daerah Kabupaten Buton," *Administratio Jurnal Ilmiah Ilmu Administrasi Negara* 11, no. 1 (2022): 9–21.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

and used. Providing patients with a clear understanding of the protection of their data, including their right to be informed in the event of a data breach, is a key component of the beneficence-based responsibility model. By adopting this approach, hospitals not only fulfil their legal obligations but also demonstrate a commitment to prioritizing the best interests of their patients and safeguarding patient privacy and data as part of a broader effort to reinforce patient trust.

In developing an ethical responsibility model based on beneficence to protect patient data privacy, a comparative study with countries such as the United States and members of the European Union, which have implemented stringent healthcare data protection standards, is essential. In the United States, patient data protection is regulated by the Health Insurance Portability and Accountability Act (HIPAA)[20], which imposes legal obligations on healthcare providers to maintain the confidentiality and security of patient data. Additionally, HIPAA grants patients the right to access their health records and ensures that such data is used solely for legitimate purposes[21]. Strict enforcement of policies against violations, supported by advanced technologies such as encryption, forms a cornerstone of the U.S. patient data protection system. These measures can serve as a reference for hospitals in Indonesia to strengthen the principle of beneficence in managing health data. By adopting similar approaches, Indonesia can enhance patient data privacy protections and ensure that hospitals fulfil their ethical and legal responsibilities in managing healthcare information.

In the European Union, patient data protection is regulated by the General Data Protection Regulation (GDPR), which establishes stringent rules for processing personal data, including health data[22]. One key aspect of the GDPR is that personal data must be processed on a lawful, transparent, and accountable basis. The GDPR also grants individuals broader rights to control their data, including the right to delete or restrict its processing. This policy emphasizes the importance of data privacy and security as an integral part of human rights. Hospitals in the EU are required to comply with these principles, and violations of data protection regulations can result in significant penalties. This model offers

[20] Jeffrey N. Weiss, "The Health Insurance Portability and Accountability Act (HIPAA)," in *Physician Crisis*, 2023.
[21] Karen Colorafi and Bryan Bailey, "It's Time For Innovation In The Health Insurance Portability And Accountability Act (HIPAA)," *JMIR Medical Informatics*, 2016.
[22] Bocong Yuan and Jiannan Li, "The Policy Effect Of The General Data Protection Regulation (GDPR) on the Digital Public Health Sector In The European Union: An Empirical Investigation," *International Journal of Environmental Research and Public Health* 16, no. 6 (2019).

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

valuable lessons for hospitals in Indonesia, which could adopt a similar approach to strengthen patient data protection in line with the principle of beneficence[23].

This comparative study provides a clear perspective on the importance of building a more potent ethical responsibility model based on beneficence in Indonesian hospitals. By adopting more advanced personal data protection principles in accordance with international standards, hospitals can not only prevent patient data breaches but also ensure that the healthcare services provided always prioritize patient well-being. The success of hospitals in maintaining the confidentiality of patient data will positively impact the relationship between healthcare providers and patients while also boosting public trust in Indonesia's healthcare system.

The comparison with these two countries highlights the shared emphasis on the importance of patient data privacy and legal protection. However, the approaches adopted in the United States and the European Union place a greater focus on more formal protection systems and advanced technology to prevent data breaches. Hospitals in Indonesia, although regulated by Law No. 17 of 2023 on Health, still face significant challenges in strengthening internal policies and monitoring the storage and use of patient data. Cases of data breaches in Indonesia demonstrate that hospitals still lack data protection mechanisms that meet international standards, often due to inadequate technology and insufficient training for healthcare providers on the importance of maintaining patient data confidentiality.

Data breaches in hospitals can be seen as violations of patients' privacy rights, which should be firmly protected. These breaches also fail to uphold the principle of beneficence, which should serve as the foundation for healthcare practices. Hospitals not only fail to protect patient data but also damage the trust that should exist between healthcare providers and patients.

Previous data breaches should prompt hospitals to evaluate and improve their systems to prevent recurrence. Hospitals should view these incidents as opportunities to strengthen their patient data protection policies by implementing a more robust application of the beneficence principle. All efforts must aim to protect patients' privacy rights and ensure that their data remains safeguarded. By adopting an ethical responsibility model based on

[23] Miftahul Jannah, F. Yudhi Priyo Amboro, and Rina Shahrullah, "Personal Data Protection in Telemedicine: Comparison of Indonesian and European Union Law," *Journal of Law and Policy Transformation* 8, no. 2 (2024): 145–163.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

beneficence, which prioritizes the interests of patients, hospitals will not only fulfil their legal obligations but also strengthen trust and build long-term relationships with patients.

Protecting patient data in Indonesian hospitals requires a holistic approach, given the importance of maintaining the privacy of personal health information. Hospitals in Indonesia can learn from practices implemented in the United States and the European Union when designing a more effective ethical responsibility model based on the principle of beneficence. One step that can be taken is to strengthen the use of secure information technology, such as data encryption and strict access control, to ensure that only authorized parties can access patient data. Additionally, hospitals need to develop transparent policies regarding patients' rights to their data and ensure that patients understand how their information will be used and protected. By adopting the principles applied in these advanced countries, hospitals in Indonesia can strengthen patient data protection and enhance patient trust in the healthcare system.

Protecting patient data is not just about meeting regulatory obligations but also about building an ethical culture among healthcare providers and all hospital staff[24]. In this regard, the principle of beneficence, which emphasizes the best interests of patients, must be translated into concrete actions through continuous training, the implementation of clear policies, and strict supervision. The ethical responsibility model based on beneficence, applied in developed countries, can serve as a reference for designing training programs that emphasize the importance of maintaining patient confidentiality and protecting data, as well as preventing the misuse of medical information that could harm patients.

Confidentiality is the fundamental principle in safeguarding patient data privacy. Personal health information should only be accessible to those with legitimate authority and solely for legitimate healthcare purposes. Therefore, hospitals must ensure that all healthcare providers and staff understand their obligation to maintain confidentiality, which is an integral part of their professional ethics. The ethical responsibility model based on beneficence requires hospitals to ensure that patient data is protected not only physically but also during the processing and digital storage of the data. This data protection involves administrative measures as well as proper management of the information systems used by the hospital.

[24] Alfian Listya Kurniawan and Anang Setiawan, "Perlindungan Data Rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19," *Jurnal Hukum dan Pembangunan Ekonomi* 9, no. 1 (2021): 95–112.

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

The importance of strict supervision over the implementation of data confidentiality policies in hospitals cannot be overlooked. Effective internal monitoring includes regular training for healthcare providers on the importance of maintaining patient data confidentiality and applying the principle of beneficence in every aspect of medical practice. Hospitals need to implement strict access controls to patient data to ensure that only authorized individuals can access the information. This is essential to avoid potential violations, whether intentional or accidental and to ensure that the principle of beneficence is upheld ensuring that actions taken always benefit patients and do not harm them.

The secure and advanced management of patient data is an urgent need to support a model of ethical responsibility based on beneficence. Hospitals must ensure that the information systems they use not only support administrative efficiency but also incorporate reliable security mechanisms. Technologies such as data encryption, firewalls, and two-factor authentication are essential tools to minimize the risk of data breaches. In addition, strict internal policies and regular audits are needed to identify and close potential vulnerabilities to cyberattacks, which are often a leading cause of data breaches in the healthcare sector.

Technology also plays a strategic role in strengthening patient data confidentiality, which is in line with the principle of beneficence. Secure information systems not only protect data from unauthorized access but also provide patients with peace of mind, knowing their personal information is being managed responsibly. In addition to complying with applicable legal regulations, hospitals need to take proactive steps to enhance data security, such as user-rights-based access restrictions and real-time system monitoring. These efforts are essential in the face of an ever-evolving and challenging digital ecosystem to maintain patient trust and prevent damage caused by data breaches.

It is also crucial for hospitals to ensure compliance with the regulations outlined in laws such as Health Law No. 17/2023, which emphasizes the protection of patient personal data. The ethical responsibility model based on beneficence must be grounded in these regulations, ensuring that hospitals not only fulfil their legal obligations but also implement policies that respect and protect patients' rights. Hospitals must ensure that the management of patient data is conducted in accordance with the standards set out in the law while also considering the moral and ethical aspects of every process involved.

Transparent management of patient data is also a crucial factor in the model of ethical responsibility based on beneficence. Hospitals must provide clear information to patients about how their data will be used, stored, and protected. This allows patients to make

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

informed decisions regarding the use of their data. This ethical responsibility model not only involves the hospital's obligation to protect patient data but also empowers patients to participate actively in the management of their personal information. Transparency, aligned with the principle of beneficence, fosters trust between patients and healthcare providers, establishing a mutually supportive relationship in the protection of personal data.

Continuous oversight and evaluation of data confidentiality policies are essential to maintain the effectiveness of the ethical responsibility model based on beneficence. Hospitals must regularly assess the success of their policies in safeguarding patient data and ensure that all healthcare professionals and staff comply with the established regulations. This can be achieved through strict internal audits and ongoing training to remind healthcare providers of their ethical responsibilities in maintaining patient data confidentiality. A continuous evaluation system helps hospitals detect and address potential gaps in policies that could jeopardize patient data confidentiality while also improving existing mechanisms to uphold high ethical standards in healthcare services.

By designing a model of ethical responsibility based on beneficence, hospitals not only comply with existing laws but also provide better protection for patients. This model integrates adherence to regulations with the moral responsibility to safeguard the privacy and security of patient data. Ultimately, by strengthening comprehensive and ethically grounded data protection systems, hospitals can create a safer and more trustworthy environment for patients, ensuring that the principle of beneficence remains the guiding principle in every action taken.

Table 2. Model of Ethical Responsibility Based on the Principle of Beneficence

Aspect	Description	Implementation
Hospital Internal Policy	Hospitals need to develop policies that prioritize patient data protection with the patient's best interests as the top priority.	Policies that ensure patient privacy is prioritized and promote transparency in data management.
Use of Advanced Technology	Technologies such as data encryption, firewalls, and double authentication need to be used to protect patient data from leaks.	Implementation of technology to secure data and prevent unauthorized access.
System Evaluation and Improvement	Data breach cases should be an impetus for evaluation and improvement of systems in hospitals to prevent similar incidents from recurring.	Evaluate internal policies and implement stricter security systems following a data breach incident.
Routine Supervision and Training	Strict supervision of policy implementation and ongoing training for medical personnel regarding the	Routine training and supervision of the implementation of the

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

	importance of maintaining patient data confidentiality.	principle of beneficence in hospitals.
Culture of Ethics and Responsibility	The principle of beneficence is implemented through supervision and training to maintain the confidentiality of patient data.	Building an ethical culture that ensures every hospital staff maintains patient privacy as part of their professional ethics.
Data Security Mechanism	The data security system must be equipped with a reliable security mechanism to avoid data leaks.	Use of secure information technology, including encryption and strict access controls to patient data.

Source: Based on the research findings of this study.

Based on Table 2, hospitals must develop comprehensive internal policies that prioritize patient data protection, ensure privacy, and ensure transparency in data management. Hospitals are encouraged to utilize advanced technologies such as data encryption, firewalls, and dual authentication to protect patient data from unauthorized access. Hospitals must evaluate and improve systems in the event of a data breach and strengthen security to prevent future incidents. A culture of ethics and responsibility is integral to ensuring that every hospital staff member understands their critical role in protecting patient privacy. This approach is further supported by robust data security mechanisms, including encryption and strict access controls, to ensure that patient information remains secure and protected from potential breaches.

D. Conclusion

Strengthening the role of hospitals in safeguarding patient data confidentiality is crucial for maintaining integrity and trust between patients and healthcare providers. Law No. 17/2023 mandates hospitals to store and protect patient health data to high standards and requires healthcare professionals to maintain patient data confidentiality. Challenges faced by hospitals include the risk of data breaches resulting from hacking or technical errors, as well as the lack of training for healthcare professionals on patient data protection. Therefore, hospitals need to implement comprehensive policies that involve the latest technologies, such as data encryption and strict access controls, to prevent data leaks.

The principle of beneficence must be integrated into every hospital policy and procedure as part of the moral responsibility of healthcare providers to protect patient privacy. Hospitals should also enhance transparency with patients regarding how their data is managed and protected. By adopting a beneficence-based responsibility model, hospitals not only fulfil legal obligations but also strengthen the trust-based relationship between patients

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

and healthcare providers. The implementation of this policy, supported by appropriate technology and training, will strengthen the patient data protection system, increase public trust in healthcare services, and create a safer and more reliable medical environment.

BIBLIOGRAPHY

Bahri, Samsul, Fathul Mu'in, Rissa Afni Martinouva, and Nurlis Effendi. "Implementasi Perlindungan Hukum Pasien Tentang Rahasia Kedokteran (Studi Pada Rumah Sakit Pertamina Bintang Amin Bandar Lampung)." *Jurnal Hukum Malahayati* 3, no. 1 (2022).

Bester, Johan Christiaan. "Beneficence, Interests, and Wellbeing in Medicine: What It Means to Provide Benefit to Patients." *American Journal of Bioethics* 20, no. 3 (2020).

caesar akbar, Persada, Syailendra. "6 Kasus Kebocoran Data Pribadi Di Indonesia." *Tempo.Com*.

Colorafi, Karen, and Bryan Bailey. "It's Time For Innovation In The Health Insurance Portability And Accountability Act (HIPAA)." *JMIR Medical Informatics*, 2016.

Darmawan, Ahmad. "Analisis Pelepasan Informasi Rekam Medis Sebagai Penjamin Aspek Hukum Kerahasiaan Data Pasien." *Jurnal Manajemen Informasi Kesehatan Indonesia (JMIKI)* 11, no. 1 (2023).

Disemadi, Hari Sutra. "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies." *Journal of Judicial Review* 24, no. 2 (2022): 289–304.

Jannah, Miftahul, F. Yudhi Priyo Amboro, and Rina Shahrullah. "Personal Data Protection in Telemedicine: Comparison of Indonesian and European Union Law." *Journal of Law and Policy Transformation* 8, no. 2 (2024): 145–163.

Jansen, Lynn A. "Medical Beneficence, Nonmaleficence, and Patients' Well-Being." *The Journal of clinical ethics* 33, no. 1 (2022).

K, Sitti Aminah, and Ashabul Kahpi. "Tinjauan Terhadap Hak Dan Kewajiban Pasien Dalam Pelayanan Kesehatan." *Alauddin Law Development Journal* 3, no. 3 (2021).

Khalifatullah, Arya Wirai, Afifah Fitri Apsari, Anifatun Lutfiyah, Ervina Anisya Qoriah, Anisya Qoriah, Gesit Syaifrudin Zukhri, and Muh. Rizal Rosyid Ridho. "Perlindungan Data Pribadi Pasien Terhadap Serangan Cyber Crime." *Sanskara Hukum dan HAM* 1, no. 02 (2022).

Kurniawan, Alfian Listya, and Anang Setiawan. "Perlindungan Data Rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19." *Jurnal Hukum dan Pembangunan Ekonomi* 9, no. 1 (2021): 95–112.

Laksono, Sidhi. "Kesehatan Digital Dan Disrupsi Digital Pada Layanan Kesehatan Di Rumah Sakit." *Jurnal Kebijakan Kesehatan Indonesia* 11, no. 1 (2022): 36–42.

Musaini, Awaluddin, Andi Tenri, and Syahril Ramadhan. "Transparansi Pelayanan Publik Di Rumah Sakit Umum Daerah Kabupaten Buton." *Administratio Jurnal Ilmiah Ilmu Administrasi Negara* 11, no. 1 (2022): 9–21.

O'Donoghue, Kevin. "Learning Analytics within Higher Education: Autonomy, Beneficence and Non-Maleficence." *Journal of Academic Ethics* 21, no. 1 (2023).

Pandi, Marini V. "Sanksi Pidana Atas Pelanggaran Rahasia Kedokteran Oleh Dokter." *Lex et Societatis* I, no. 2 (2013).

Putra, Calvin Anthony, and Muh Ali Masnun. "Analisis Pertanggungjawaban Rumah Sakit Terkait Potensi Kebocoran Data Rekam Medis Elektronik Akibat Cyber Crime." *Novum : Jurnal Hukum* 9, no. 2 (2022).

———. "Analisis Pertanggungjawaban Rumah Sakit Terkait Potensi Kebocoran Data

WIDYA PRANATA HUKUM
JURNAL KAJIAN DAN PENELITIAN HUKUM
P-ISSN : 2654-5195 | E-ISSN : 2686-2417

Rekam Medis Elektronik Akibat Cyber Crime." *Novum : Jurnal Hukum* 9, no. 2 (2022): 1–14.

Ridwan, Ridwan. "Pertanggungjawaban Hukum Pidana Terhadap Pelanggaran Rahasia Medis." *Jurnal Hukum & Pembangunan* 49, no. 2 (2019): 338–348.

Riyanto, Ontran Sumantri, and Fuad. "Perlindungan Hukum Praktik Kedokteran Di Rumah Sakit: Implementasi Kenyamanan Dokter Dalam Memberikan Pelayanan Kesehatan." *Juris Humanity: Jurnal Riset dan Kajian Hukum Hak Asasi Manusia* 2, no. 1 (2023): 1–14. https://www.jrkhm.org/index.php/humanity/article/view/14.

Utomo, Handryas Prasetyo, Elisatris Gultom, and Anita Afriana. "Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Teknologi Di Indonesia." *Jurnal Ilmiah Galuh Justisi* 8, no. 2 (2020).

Varkey, Basil. "Principles of Clinical Ethics and Their Application to Practice." *Medical Principles and Practice*, 2021.

Weiss, Jeffrey N. "The Health Insurance Portability and Accountability Act (HIPAA)." In *Physician Crisis*, 2023.

Wicaksana, Arif, and Tahar Rachman. "Rahasia Kedokteran Di Antara Moral Dan Hukum Profesi Dokter." *Angewandte Chemie International Edition, 6(11), 951–952.* 3, no. 1 (2018).

Yuan, Bocong, and Jiannan Li. "The Policy Effect Of The General Data Protection Regulation (GDPR) on the Digital Public Health Sector In The European Union: An Empirical Investigation." *International Journal of Environmental Research and Public Health* 16, no. 6 (2019).