UNTAG Law Review (ULREV)
Volume 8, Issue 1, MEI 2024, PP 28-40
ISSN 2549-4910 (online) & ISSN 2579-5279 (print)
http://jurnal.untagsmg.ac.id/indeks.php/ulrev/indeks
www.fakhukum.untagsmg.ac.id

JURIDICAL ANALYSIS OF PATIENT DATA PROTECTION IN NATIONAL LEGAL PERSPECTIVE

Elen Anedya Frahma[1]
[1]Department of International Law, University 17 August 1945 Semarang, Indonesia
[1]elenfrahma16@gmail.com

ABSTRACT; *The emergence of digital-based health services has garnered increased attention following the onset of the COVID-19 pandemic. The utilization of these services involves the collection of user data, a sensitive matter that holds the potential for giving rise to legal issues, thereby calling for the need for regulations concerning the protection of personal data. Indonesia has established provisions to safeguard personal data in the health sector through various legal instruments. However, the effective protection of users' data in the digital transformation of the health sector has not materialized. This is evident in instances of personal data breaches involving participants of the Health Social Security Administering Agency. The research is conducted using normative juridical legal research methods. The findings highlight the context of personal data protection in the health sector within the digital era, which is regulated in, for example, article 26 of the ITE Law, Law Number 43 of 2009 regarding Archives, article 57 of the Health Law, Minister of Health Regulation Number 24 of 2022 concerning Medical Records and Law Number 36 of 1999 on Telecommunications. Nevertheless, the occurrence of data leaks from BPJS Health indicates the failure to ensure personal data protection in the health sector in Indonesia. As a result, regulations and stringent supervision within health institutions, particularly in the digital sector, are crucial. The appointment of Data Protection Officers in health service agencies represents the solution to these issues, and it is imperative to realize digital protection of personal data in the health sector.*

Keywords: *Patient Data; Health; Regulation; Digital*

INTRODUCTION

The increase in information system activities and the current state of technology have reflected the constellation of an information-oriented world society. Moreover, the presence of the era of disruption has changed people's lifestyles and ways of working from conventional to modern using a digital approach. Society has now entered a transition phase leaving the era of disruption of the Industrial Revolution 4.0 due to the existence of the Industrial Revolution 5.0 which is arriving more quickly, triggered by 5G telecommunications technology and the massive digital platform.[1]

In line with this, if you look at the condition of Indonesia based on data in 2021, it can be seen that internet users were recorded at 202.6 million users, which is an increase of 11% compared to the previous year which amounted to 175.4 million users.[2] Apart from that, the Covid-19 pandemic has also inspired many people to switch to using digital technology.

Attempts to leverage digital advancements in the healthcare industry aim to expedite health services and mitigate issues that have historically plagued healthcare. The adoption of information technology in the Indonesian healthcare sector has been realized through the implementation of the Health Information System (GIS) and is currently evolving to incorporate the use of Electronic Medical Records (RME).

According to Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records Article 1 paragraph (2), Electronic Medical Records are defined as medical records created using an electronic system designed for the management of medical records.[3]

According to the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 regarding Medical Records, it is compulsory for all healthcare providers to have an electronic medical record, as stipulated in Article 3, which mandates that: (1) All healthcare facilities are required to uphold an Electronic Medical Record. (2) The healthcare facilities mentioned in paragraph (1) encompass: a. Individual practice venues for physicians, dentists, and/or other healthcare professionals; b. Public health centers; c. clinics; d. hospitals; e. pharmacies; f. health laboratories; g. halls; and h. Other Healthcare Facilities as determined by the Minister.[4]

In the health sector, health data includes specific or sensitive data so patient personal

[1] Malte Hellmeier and Franziska von Scherenberg, "A Delimitation of Data Sovereignty from Digital and Technological Sovereignty," *Thirty-First European Conference on Information Systems (ECIS 2023)* 1, no. June (2023).

[2] Aptika Kominfo, "Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya Di Internet," n.d.

[3] Yudi Yasmin Wijaya, Edy Suyanto, and Fanny Tanuwijaya, "Rekam Medis: Penggunaan Informasi Medis Pasien Dalam Pelaksanaan Asas Perlindungan Publik," *Veritas et Justitia* 6, no. 2 (2020): 399–423, https://doi.org/10.25123/vej.3717.

[4] 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, https://doi.org/10.20961/hpe.v9i1.52586.

data as consumers need to be protected because it contains confidential information such as health test results, type of disease suffered, information about where they live, telephone numbers, etc.[5]

Hence, this information is safeguarded by Regulation Number 29 of 2004 regarding Medical Practices ("Medical Practice Regulation"), article 57 of the Health Law Number 36 of 2009 regarding Health ("Health Regulation"), and Regulation Number 44 of 2009 regarding Hospitals ("Hospital Regulation"). On the digital front, the protection of personal data is encompassed in the clauses of Regulation Number 19 of 2016 concerning Amendments to Regulation Number 11 of 2008 regarding Electronic Information and Transactions ("UU ITE"). Despite being articulated in the relevant regulations, the assurance of personal data protection in the digital healthcare sector has not been actualized in its execution.[6]

This can be seen in cases of personal data leaks from members of the Health Social Security Administering Body ("BPJS"). It is believed that there are 279 million personal information records of BPJS Health participants spread and traded on Raid Forums. Dedy Permadi, a representative from the Ministry of Communication and Information Technology, revealed that a study had been carried out on the data samples that experienced the leak and it had been confirmed that the personal information that was spread was suspected to have come from BPJS Health data. Dedy also said that the claim became more convincing after seeing various information spread, including BPJS participant card numbers, BPJS office codes, family information, dependents covered by health insurance, and payment status.[7]

This scenario demonstrates that the current legal regulations are inadequate in ensuring the digital safeguarding of personal data in the healthcare sector. Therefore, innovative initiatives are essential as a method to protect personal data in the digital age, particularly within the healthcare domain.

This underscores the necessity of composing this article, which aims to delve into the digital protection of personal data in the healthcare sector. The article will analyze the challenges of safeguarding personal data in the healthcare sector, the legal framework for protecting personal data in the healthcare sector, and the implementation of the role of data protection officers in healthcare institutions as a strategy for digitally securing personal data in the healthcare sector.

PROBLEM

[5] Muhammad Izzar Damargara et al., "Urgensi Realisasi Pengaturan Data Protection Officer (DPO) Pada Sektor Kesehatan Ditinjau Dari Hukum Perlindungan Data," *Padjadjaran Law Research* 10, no. 1 (2022): 38–55.

[6] Gilbert Kosegeran and Dientje Rumimpunu, "Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin," *Lex Privatum* IX, no. 12 (2021): 89–98, https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/38447.

[7] CNN Indonesia, "Kebocoran Data Pribadi, BPJS Kesehatan Bakal Digugat," n.d.

RESEARCH METHODS

The author's research employs normative juridical methodology, which conceptualizes law as the written statutory regulations (law in the books) or as norms and principles that serve as benchmarks for appropriate human conduct. The research employs the Statutory Approach and the Conceptual Approach as its foundational methodologies.[8]

The sources of legal materials utilized in this research include literature reviews, legislation, government regulations, subordinate regulations, academic journals, and legal cases referenced by the author. Analysis of the legal materials used in the study. This research is an interpretation, namely using juridical methods in discussing a legal issue. This research also uses a deductive legal material analysis method, namely a research method based on general concepts or theories applied to explain a set of existing legal facts which are then researched and analyzed using the legal material obtained.

DISCUSSION

The Role of Digital Platforms in the Health Sector

The COVID-19 pandemic, which began two years ago, has changed the order of life in general and has specifically caused a shift in people's habits regarding health services. The Association of Hospitals in Indonesia ("PERSI") stated that after the COVID-19 pandemic, the decline in hospital income reached 40% of the average monthly income. This is due to appeals not to visit hospitals, patients who are hesitant to visit hospitals, restrictions on the number of hospital patients, and a reduction in the number of doctors' practices.[9]

The solution is that people are becoming more open to health consultations via electronic-based platforms. In this case, the use of telemedicine application services has increased by up to 600%.[10] The various telemedicine service options provided consist of doctor consultations, booking appointments with doctors, to online drug purchase transactions. During the Covid-19 pandemic, the emerging telemedicine and digital health services were initially sanctioned by Ministerial Decree Number HK.01.07/MENKES/4829/2021, which outlines the Guidelines for Health Services via Telemedicine During the Corona Virus Disease 2019 (COVID-19).

Presently, the decree serves as the legal foundation for the function of telemedicine platforms, catering to individuals with Covid-19 who are under self-isolation. In general, Minister of Health Decree 4829/2021 provides a comprehensive set of

[8] S. Notoatmodjo, *Metodologi Penelitian Kesehatan*, 2018.

[9] Indah Maria Maddalena Simamora, "Perlindungan Hukum Atas Hak Privasi Dan Kerahasiaan Identitas Penyakit Bagi Pasien Covid-19," *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 1, no. 7 (2022): 1089–98, https://doi.org/10.54443/sibatik.v1i7.126.

[10] Kastania Lintang and Yeni Triana, "Perlindungan Hukum Terhadap Hak Privasi Dan Rekam Medis Pasien Pada Masa Pandemi Covid-19 (Legal Protection Of Patients Privacy Rights And Medical Records In The Covid-19 Pandemic)," *Rewang Rencang : Jurnal Hukum Lex Generalis* 2, no. 10 (2021): 913–27.

guidelines that are used as a reference by the Indonesian Government, as well as medical personnel, health-based service provider facilities, digital health platform service providers, and related stakeholders about the provision of health-based services via digital health platforms during this era. covid-19 pandemic.[11]

Based on the third dictum of Minister of Health Decree 4829/2021, telemedicine as a digital platform in the health sector itself can be interpreted as an online service in the health sector that involves information and communication technology facilities in providing health information including treatment, diagnosis, assessment of the patient's health condition, prevention of deterioration and/or services in the pharmaceutical sector, including monitoring the condition of Covid-19 sufferers who are carrying out self-isolation.[12]

Telemedicine services must be carried out by medical personnel through health service provider facilities according to their capabilities and authority, taking into account the quality of service and the health condition of patients using telemedicine services. The presence of digital platforms in the health sector also supports the provision of better and more effective health services.

The Chairman of the Indonesian Doctors Association ("IDI Bogor") stated that digital transformation in the health sector provides benefits, namely making it easier for people to access services, the effectiveness of human resources, encouraging improvements in service quality, and being able to reduce costs for health services. Observing the significance and progress of digital platforms, the Ministry of Health, through Regulation Number 21 of 2020, strives for the digital transformation of healthcare services as part of the Ministry's Strategic Plan for 2020-2024.[13]

This initiative involves integrating information systems, conducting research, and enhancing healthcare services. As a result of this digital transformation in the healthcare sector, an Integrated Electronic Medical and Health Record, known as the Individual-Based National Health System, is currently under development.

The integration of health platform services will later focus on various services such as health emergency response, primary services, pharmaceuticals and medical devices, referral health services, health funding, COVID-19 vaccination, as well as internal governance and infrastructure of the Ministry of Health.[14] However, to realize the role of a good digital platform in the health sector, it is necessary to pay attention to several things, one of which is related to security aspects that can guarantee the protection of the personal data of service users.

Personal Data Protection Issues in the Health Sector

In Indonesia, the legal protection concerning personal data is perceived to be insufficient. For instance, the prevalent misuse of personal data often occurs without the knowledge of the data owner. This misuse can lead to privacy infringements that

[11] Kurniawan and Setiawan, "Perlindungan Data Rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19."

[12] Ririn Noviyanti Putri, "Indonesia Dalam Menghadapi Pandemi Covid-19" 20, no. 2 (2020): 705–9, https://doi.org/10.33087/jiubj.v20i2.1010.

[13] Aptika Kominfo, "Digitalisasi Pelayanan Kesehatan Dengan Penerapan Revolusi Industri," n.d.

[14] Wijaya, Suyanto, and Tanuwijaya, "Rekam Medis: Penggunaan Informasi Medis Pasien Dalam Pelaksanaan Asas Perlindungan Publik."

may affect individuals.[15] This shows that there are gaps in supervision and system weaknesses that allow misuse of personal data information and can be detrimental to the data owner.

This can be seen in the issue of BPJS Health patient data leakage, which according to the spokesperson for the Ministry of Communication and Information, Dedy Permadi, said there was an alleged leak of 279 million data belonging to BPJS Health which was also traded on a forum. Timboel Siregar as the Advocacy Coordinator of BPJS Watch explained that there were two suspected causes of data leaks in the BPJS Health case.

First, the data leak was caused by a hack in a third-party application. Based on the results of the analysis, the number of applications owned by BPJS Health includes eight applications for the health service insurance management information system, six applications for the public service information system, and six applications to support the membership management information system.

Reviewing the many applications that BPJS Health has, he suspects that the leak was caused by hacking, especially in the membership management information system application and also in the health service application. Then the second suspicion is that there was a data leak carried out by an internal party. Timboel considers that the hack proves the low security of the BPJS Health application.[16]

Some IT operating frameworks and standards implemented to protect application security cannot be guaranteed by government agencies. As a result, organizations are urged to streamline the array of applications within BPJS Health and implement rigorous data security measures in order to effectively and efficiently ensure the confidentiality of personal and public health data.

The recent data leak incident at BPJS Health serves as evidence that patient personal data within the healthcare sector is vulnerable to potential misuse. Patient personal data comprises more than just information collected during the registration process and serves as a crucial link between patients and healthcare service providers. Nowadays in Indonesia, technology assistance has been widely used by health service providers in processing patient data information so that it becomes digital.[17]

Hence, it is a critical priority to establish legal safeguards for personal and health data, ensuring that this information is not disclosed to the public unless explicitly authorized by law. Any unauthorized disclosure of patient data to the public would contravene legal provisions. The existing regulations on personal data protection in Indonesia are fragmented across various legal instruments, resulting in a lack of specificity and robustness in outlining the rules for safeguarding personal data.[18]

For instance, the ITE Law does not offer explicit and comprehensive regulations on personal data protection, failing to address the significant issues widely debated in relation to safeguarding personal data. The current provisions of the ITE Law do not provide assurances for protecting personal data in the healthcare sector, which is the

[15] Kosegeran and Rumimpunu, "Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin."

[16] CNN Indonesia, "Kebocoran Data Pribadi, BPJS Kesehatan Bakal Digugat."

[17] Lalu Anugrah Nugraha et al., "Perlindungan Hukum Rumah Sakit Atas Penggunaan Data Pasien Dalam Peresepan Elektronik," *Unizar Law Review* 6, no. 2 (2023), https://doi.org/10.36679/ulr.v6i2.45.

[18] Tiromsi Sitanggang, *Aspek Hukum Kepemilikan Rekam Medis Terhadap Perlindungan Hak Pasien*, ed. Feriyansyah, 1st ed. (Medan: Yayasan Kita Menulis, 2019).

focal point of the discussion in this article.

The existing regulations remain inadequate, particularly due to the absence of a specific law in Indonesia that clearly and comprehensively outlines regulations for the protection of personal data. Personal data within the healthcare sector, which includes the patient's sensitive identity information such as name, contact details, and address, as well as medical records, is regarded as confidential and private.[19]

Consequently, patients are entitled to assured privacy and confidentiality regarding their medical conditions and related information, underscoring the critical importance of patient confidentiality. This extends to digital health services, which involve the collection of sensitive personal data, necessitating clear guidelines on the extent to which healthcare providers can safeguard patient information in e-health platforms. Therefore, there is a clear need for regulations that address this aspect and sufficient oversight to ensure the protection of personal data in the healthcare sector.[20]

Legal Protection Of Patient Personal Data In Health Services

The significance of personal data in the healthcare industry is highlighted by the fact that medical records are considered ten times more valuable to cybercriminals than credit card information. The value of personal data in the health sector is determined by the comprehensiveness of the information it contains, as healthcare providers typically manage a wide range of data, including the patient's identity, financial details, and medical records.[21]

The significance of safeguarding personal data in the healthcare sector necessitates adherence to the existing legal framework in Indonesia. With regard to personal data in the healthcare sector, article 57 of the Health Law underscores the patients' right to confidentiality of their medical information shared with healthcare providers, unless specified otherwise within the terms and parties delineated in that article.

Additionally, Article 47 Paragraph (2) of the Medical Practice Law fundamentally mandates physicians and healthcare facility leaders to ensure the confidential protection of each individual's medical records, encompassing various documents and notes pertaining to the health information furnished to patients.[22]

The regulations pertaining to personal data protection in Indonesia are currently characterized by their broad and general nature, as they are dispersed across multiple laws and regulations. These legal provisions only offer a general concept of personal data protection and are primarily outlined in a regulation issued by the Minister of Communication and Information of the Republic of Indonesia.

Notable among these separate legal provisions are laws such as the Information and

[19] 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): 168, https://doi.org/10.25157/justisi.v8i2.3479.

[20] Dipika Jain, "Regulation of Digital Healthcare in India: Ethical and Legal Challenges," *Healthcare (Switzerland)* 11, no. 6 (2023), https://doi.org/10.3390/healthcare11060911.

[21] Bambang Dwi Hs, "Legal Aspect of Patient's Medical Record," *Advances in Economics, Business and Management Research* 121, no. Inclar 2019 (2020): 76–79, https://doi.org/10.2991/aebmr.k.200226.015.

[22] Lalu Anugrah Nugraha et al., "Perlindungan Hukum Rumah Sakit Atas Penggunaan Data Pasien Dalam Peresepan Elektronik."

Electronic Transactions (ITE) Law No. 11 of 2008, Law Number 43 of 2009 regarding Archives, Law Number 8 of 1997 concerning Company Documents, Law Number 10 of 1998 on Amendments to Law Number 7 of 1992 concerning Banking, article 57 of the Health Law Number 36 of 2009, Law Number 36 of 1999 on Telecommunications (Telecommunications Law), and Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration (UU Adminduk).

The Indonesian Constitution (UUD NKRI 1945) also implicitly addresses the protection of personal data, as seen in Article 28G paragraph (1), stating, "Everyone has the right to protect himself, his family, honor, dignity, and property under his control...".[23]

The protection of personal data is addressed in multiple articles within the ITE Law. However, the law currently lacks stringent and all-encompassing regulations specifically focused on the protection of personal data. Nevertheless, it indirectly establishes a novel interpretation concerning the preservation of electronic data and information, encompassing both public and private domains.

The ITE Law mandates a comprehensive definition of personal electronic data in the Regulation on the Implementation of Electronic Systems and Transactions (PSTE). The protection of personal data within an electronic system as outlined in the ITE Law encompasses prevention against unauthorized usage, safeguards provided by electronic system operators, and protection from unlawful access and interference.[24] Article 26 of the ITE Law pertains to the protection of personal data from unauthorized use. It stipulates that the utilization of any personal data in electronic media necessitates the consent of the data owner. Individuals who violate this regulation may be subject to legal action for resulting damages.

Additionally, the article emphasizes that personal data represents an integral component of an individual's rights. The ITE Law (Law No. 11 of 2008 amended by Law No. 19 of 2016), functioning as a general law, encompasses norms for personal data protection in Article 26, which essentially requires that any use of data and information in electronic media pertaining to an individual's data must be conducted with the individual's consent or in accordance with existing legislation. This provision establishes two fundamental principles for the lawful processing of personal data: (a) consent and (b) adherence to positive legal norms. These principles serve as the foundation for legitimate data processing.[25]

Based on the aforementioned regulations, it is evident that Indonesian law places significant emphasis on the responsibilities of entities offering healthcare services to safeguard patient health data. Nonetheless, various data breach incidents in Indonesia, such as those encountered by BPJS Health, underscore the inadequate protection of personal data within the country's healthcare sector. Therefore, enhancing the safeguarding of personal data in the healthcare domain should be a

[23] Kurniawan and Setiawan, "Perlindungan Data Rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19."

[24] Anny Retnowati, "Politik Hukum Dalam Menata Rekam Medis Sebagai Sarana Perlindungan Hukum Terhadap Rumah Sakit, Dokter Dan Pasien," *Yustisia Jurnal Hukum* 2, no. 2 (2018), https://doi.org/10.20961/yustisia.v2i2.10208.

[25] Nabbilah Amir, "Legal Protection of Patient Data Confidentiality Electronic Medical Records (Perlindungan Hukum Kerahasiaan Data Pasien Dalam Rekam Medik Elektronik)," *SOEPRA Jurnal Hukum Kesehatan* 5, no. 2 (2019): 198–208, http://journal.unika.ac.id/index.php/shk198.

collective priority aimed at addressing challenges associated with health data and information.[26]

Implementation of the Role of Data Protection Officers in Health Service Agencies

Given the pressing need to enhance the protection of personal data in the healthcare sector, the government must recognize the significance of appointing authorized individuals to oversee personal data protection endeavors within every entity and/or organization operating in the healthcare field, encompassing both traditional and digital platforms.

The responsibilities associated with safeguarding personal data in the healthcare domain can be entrusted to a Data Protection Officer (DPO). The concept of a DPO was originally introduced in Article 37 of the GDPR, which specifically mandates the appointment of a DPO when data processing activities are conducted by a public body or agency. Subsequently, these provisions were integrated into articles 45 and 46 of the Draft Law on Personal Data Protection ("RUU PDP").

Under Article 45, Paragraph (2) Letter A and Paragraph (3) of the PDP Bill, it is stipulated that officials fulfilling functions related to the protection of personal data in areas of personal data processing oriented towards the public interest should be appointed based on their professional expertise, legal acumen, and proficiency in the practices of personal data protection, thereby signifying their capability to assume responsibility for their assigned tasks.[27]

Realizing the significance of the DPO's role within health service entities lies in safeguarding personal data within the healthcare sector, particularly concerning the public interest. As stipulated in Article 46 of the PDP Bill, the function of the DPO underscores its crucial role in enhancing the protection of personal data, as the DPO holds the authority to oversee all data processing activities conducted by personal data processors.

Consequently, various companies and agencies operating within the healthcare sector, including public health agencies, hospitals, digital health service platforms, health laboratories, health insurance providers, and other healthcare facilities engaged in processing personal data for public services, are mandated to have a DPO. This measure is aimed at ensuring that personal data processing activities remain oriented towards optimal personal data protection, aligning with substantial legal frameworks within Indonesia.[28]

Apart from that, DPOs in companies and/or health service agencies are also responsible for the performance of personal data processors by providing regular training and audits so that the protection of patient personal data in companies

[26] Calvin Anthony Putra, "Data Rekam Medis Elektronik Akibat Cyber Crime Calvin Anthony Putra," *Jurnal Novum* 1, no. 1 (2021): 0–216.

[27] Damargara et al., "Urgensi Realisasi Pengaturan Data Protection Officer (DPO) Pada Sektor Kesehatan Ditinjau Dari Hukum Perlindungan Data."

[28] Tri Putri Simamora et al., "Perlindungan Hukum Terhadap Pasien Dalam Pelayanan Medis Di Rumah Sakit Umum," *Al-Adl : Jurnal Hukum* 12, no. 2 (2020): 270, https://doi.org/10.31602/al-adl.v12i2.3091.

and/or health service agencies is maintained.[29]

Another responsibility that DPOs within healthcare organizations and agencies can undertake is the management of risks associated with processing health data and information to reduce the likelihood of personal data breaches that could adversely affect patients or healthcare service users. From the functions outlined for DPOs, it is evident that they play a critical role in maximizing the protection of personal data within the healthcare sector, particularly within companies and public healthcare service agencies.[30]

CONCLUSION

The incident of data leakage at BPJS Health highlights the inadequate protection of personal data in Indonesia's healthcare sector. The regulations governing personal data protection are currently dispersed across various laws and regulations, resulting in generalized and weak provisions. Consequently, there is a crucial need for stringent regulation and oversight within healthcare institutions, particularly in the digital realm.

Recognizing the significance of DPOs within health service agencies is an essential step in addressing these challenges and is integral to the digital protection of personal data within the healthcare sector. Yet, the pressing need to acknowledge the significance of the DPO in enhancing the digital protection of personal data within the healthcare sector is not substantiated by comprehensive regulations outlining the DPO's role.

Hence, it is imperative to establish stringent and comprehensive regulations to ensure the security of information technology users and enhance technology-based health services. Additionally, the creation of an institution to act as an independent regulatory body or a data protection commission is crucial to provide oversight, supervision, and control in this regard.

REFERENCES

Akangbe, Raphael. "Healthcare Data Protection in the Era of Digital Health." *Researchgate*, no. August (2022).

Amir, Nabbilah. "Legal Protection of Patient Data Confidentiality Electronic Medical Records (Perlindungan Hukum Kerahasiaan Data Pasien Dalam Rekam Medik Elektronik)." *SOEPRA Jurnal Hukum Kesehatan* 5, no. 2 (2019): 198–208. http://journal.unika.ac.id/index.php/shk198.

Aptika Kominfo. "Digitalisasi Pelayanan Kesehatan Dengan Penerapan Revolusi Industri," n.d.

———. "Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya Di Internet," n.d.

[29] Raphael Akangbe, "Healthcare Data Protection in the Era of Digital Health," *Researchgate*, no. August (2022).

[30] Ni Putu Yuliana Kemalasari and I Putu Harry Suandana Putra, "Protection of Medical Record Data as a Form of Legal Protection of Health Data through the Personal Data Protection Act," *Journal of Digital Law and Policy* 2, no. 3 (2023): 111–18, https://doi.org/10.58982/jdlp.v2i3.338.

CNN Indonesia. "Kebocoran Data Pribadi, BPJS Kesehatan Bakal Digugat," n.d.

Damargara, Muhammad Izzar, Muhammad Alhidayah, Muhammad Raihan Faiqy, and Jatnika Maulana. "Urgensi Realisasi Pengaturan Data Protection Officer (DPO) Pada Sektor Kesehatan Ditinjau Dari Hukum Perlindungan Data." *Padjadjaran Law Research* 10, no. 1 (2022): 38–55.

Hellmeier, Malte, and Franziska von Scherenberg. "A Delimitation of Data Sovereignty from Digital and Technological Sovereignty." *Thirty-First European Conference on Information Systems (ECIS 2023)* 1, no. June (2023).

Hs, Bambang Dwi. "Legal Aspect of Patient's Medical Record." *Advances in Economics, Business and Management Research* 121, no. Inclar 2019 (2020): 76–79. https://doi.org/10.2991/aebmr.k.200226.015.

Jain, Dipika. "Regulation of Digital Healthcare in India: Ethical and Legal Challenges." *Healthcare (Switzerland)* 11, no. 6 (2023). https://doi.org/10.3390/healthcare11060911.

Kemalasari, Ni Putu Yuliana, and I Putu Harry Suandana Putra. "Protection of Medical Record Data as a Form of Legal Protection of Health Data through the Personal Data Protection Act." *Journal of Digital Law and Policy* 2, no. 3 (2023): 111–18. https://doi.org/10.58982/jdlp.v2i3.338.

Kosegeran, Gilbert, and Dientje Rumimpunu. "Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin." *Lex Privatum* IX, no. 12 (2021): 89–98. https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/38447.

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. https://doi.org/10.20961/hpe.v9i1.52586.

Lalu Anugrah Nugraha, Sutarno Sutarno, Ninis Nugraheni, and Andika Persada Putra. "Perlindungan Hukum Rumah Sakit Atas Penggunaan Data Pasien Dalam Peresepan Elektronik." *Unizar Law Review* 6, no. 2 (2023). https://doi.org/10.36679/ulr.v6i2.45.

Lintang, Kastania, and Yeni Triana. "Perlindungan Hukum Terhadap Hak Privasi Dan Rekam Medis Pasien Pada Masa Pandemi Covid-19 (Legal Protection Of Patients Privacy Rights And Medical Records In The Covid-19 Pandemic)." *Rewang Rencang : Jurnal Hukum Lex Generalis* 2, no. 10 (2021): 913–27.

Maria Maddalena Simamora, Indah. "Perlindungan Hukum Atas Hak Privasi Dan Kerahasiaan Identitas Penyakit Bagi Pasien Covid-19." *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 1, no. 7 (2022): 1089–98. https://doi.org/10.54443/sibatik.v1i7.126.

Notoatmodjo, S. *Metodologi Penelitian Kesehatan*, 2018.

Putra, Calvin Anthony. "Data Rekam Medis Elektronik Akibat Cyber Crime Calvin Anthony Putra." *Jurnal Novum* 1, no. 1 (2021): 0–216.

Putri, Ririn Noviyanti. "Indonesia Dalam Menghadapi Pandemi Covid-19" 20, no. 2 (2020): 705–9. https://doi.org/10.33087/jiubj.v20i2.1010.

Retnowati, Anny. "Politik Hukum Dalam Menata Rekam Medis Sebagai Sarana Perlindungan Hukum Terhadap Rumah Sakit, Dokter Dan Pasien." *Yustisia Jurnal Hukum* 2, no. 2 (2018). https://doi.org/10.20961/yustisia.v2i2.10208.

Simamora, Tri Putri, Sonya Airini Batubara, Indra Efrianto Napitupulu, and Robinson Tamaro Sitorus. "Perlindungan Hukum Terhadap Pasien Dalam Pelayanan Medis Di Rumah Sakit Umum." *Al-Adl : Jurnal Hukum* 12, no. 2 (2020): 270. https://doi.org/10.31602/al-adl.v12i2.3091.

Sitanggang, Tiromsi. *Aspek Hukum Kepemilikan Rekam Medis Terhadap Perlindungan Hak Pasien*. Edited by Feriyansyah. 1st ed. Medan: Yayasan Kita Menulis, 2019.

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): 168. https://doi.org/10.25157/justisi.v8i2.3479.

Wijaya, Yudi Yasmin, Edy Suyanto, and Fanny Tanuwijaya. "Rekam Medis: Penggunaan Informasi Medis Pasien Dalam Pelaksanaan Asas Perlindungan Publik." *Veritas et Justitia* 6, no. 2 (2020): 399–423. https://doi.org/10.25123/vej.3717.