Available online at: http://jurnal.uns.ac.id
Yustisia Jurnal Hukum
| ISSN (Print) 0852-0941 | ISSN (Online) 2549-0907 |

Have AI-Enhanced Telemedicines in Indonesia Adopted the Principles of Personal Data Protection?

Kevin Raihan; Sinta Dewi Rosadi[2]
[1,2]Faculty of Law, Universitas Padjadjaran
Corresponding author's email: kevinraihan92@gmail.com

Article Information

Submitted : March 16, 2024
Reviewed: May 23, 2024
Revised : July 24, 2024
Accepted: August 16, 2024.

Keywords:
Artificial Intelligence; Telemedicine; Personal Data Protection

Doi:10.20961/yustisia.v13i2.85996

Abstract

Artificial Intelligence (AI)-enhanced telemedicines pertains to legal problems especially on the protection of personal data considering the its nature. However, there has not been any research specifically examining the protection of personal data in in Indonesia with the perspective of Law Number 27 of 2022 regarding Personal Data Protection (PDP Law), specifically regarding the analysis of personal data protection principles (PDP Principles). Therefore, this research aimed to evaluate and analyze the practice of telemedicines in Indonesia on the adoption of PDP Principles from the perspective of PDP Law. This research is legal research with statutory and comparative approach related to AI and personal data protection issues in the AI-enhanced telemedicines in Indonesia. The findings show that telemedicine applications is categorized as personal data controller (data controller). The obligation of telemedicine application as a data controller obligates them to comply with the personal PDP Principles as regulated in the PDP Law. Several telemedicines in Indonesia have not yet effectively adopted PDP Principles in their privacy policy. The article concludes that the telemedicines applications must update their privacy policy to comply with PDP Principles and the government of Indonesia should accelerate the enactment of implementing regulation for the PDP Law.

I. Introduction

Until today, the use of Artificial Intelligence ("**AI**") in healthcare is beneficial for the process of diagnosis (Hashiguchi et al., 2022). Furthermore, AI is also beneficial to analyze the medical records from the patient for the purpose of study, quality development, and the optimization of health services. AI which has been made properly

and trained with enough data may discover the best practice of the health services from the bundle of electronic medical records. By analyzing such electronic medical records, AI may develop new medical practices for the health care treatment (Stephenson, 2021). In the future, AI hopefully may simplify and push the development of the pharmacy industry. AI may also be used to accelerate the invention and the development of drugs by making such processes more cost-effective and efficient. Although the use of AI will not guarantee the drugs that are invented may cure the disease, in fact AI is used to identify the drugs that is recognized as potential to treat Ebola Virus.

Various telemedicine applications in Indonesia use AI in their healthcare system, (Ari Nurfikri et al., 2022) for example, Halodoc, Alodokter, and KlikDokter. In those applications, AI has been used for many activities namely for teleconsultation with virtual AI named "Alni" in Alodokter (Happy Amanda Amalia, 2023), giving information to the doctors relating to the best treatment for the patient based on millions data from the previous consultation in Halodoc by AI in the form of natural language processing in Halodoc (Mediana, 2021), and the collection of lifelog data with AI in KlikDokter (Dwi Wulandari, 2022).

Other than telemedicines in Indonesia, telemedicines applications from the other States have also adopted AI in their healthcare system. For example, the use of AI for personalized health recommendations in Doctor Anywhere telemedicine from Singapore (J. Angelo, 2023), natural language AI processing similar to Halodoc in Amwell telemedicine from United States (Heather Landi, 2021), and the use of AI to utilize data insights and deliver more effective treatment plans for the patients in Doctor2U application from Malaysia (Dashika Gnaneswaran, 2017). All in all, AI has provided magnificent benefits for the health sector especially for telemedicine applications in and outside Indonesia.

Despite various benefits that have been provided by AI in the health sector (McKinney et al., 2020), especially in the practice of telemedicines (Jefferson Gomes Fernandes, 2021), AI still poses enormous threats to the patients especially for the protection of their Personal Data (Mohsin Dhali et al., 2022). This is because AI-enhanced telemedicines process the health data of its patient, and health data is also considered as personal data. Furthermore, the nature of AI which has a continuous learning mechanism makes the data modified in real time which raises the risk of giving actual information to the potential attackers, foreign authorities, or to the manufacturer of the AI system (Chiara Gallese Nobile, 2023). Therefore, it is still highly possible that data protection issues deriving from AI may arise in the telemedicine applications in Indonesia in the future.

This article focuses on the protection of personal data in the health sector, specifically from the use of AI in the telemedicine applications in Indonesia from the perspective of Indonesian law. Although Indonesia has yet to make any specific regulations for AI other than the Circular Letter of the Ministry of Communication and Information regarding the ethical use AI (Kominfo, 2023), many attempts from the Indonesian Government ("**The**

Government") depict the effort of The Government to develop efficiency and services in the health sector through AI (Kominfo, 2023; Arip Budiyanto, 2023; BRIN, 2023). This article attempts to analyze whether the privacy policy of the telemedicine application in Indonesia is sufficient to protect the patient's personal data from the perspective of Law Number 27 of 2022 regarding Personal Data Protection ("**PDP Law**").

AI is a broad term that may include a wide variety of technologies such as Deep learning ("**DL**"), Machine Learning ("**ML**"), neural networks, and natural language processing. For the purpose of this article, all these technologies are referred to as AI in the following analysis. Big data is also referred to as AI since the mechanisms of big data use ML and DL from AI.

So far, there have been several writings regarding personal data protection in the use of telemedicines, such as Anugrah Muhtarom Pratama et al. (2021), which analyze the implementation of personal data protection principles on Digital Contract Tracing Application named PeduliLindungi. They concluded that the personal data protection principles have not been fully implemented in PeduliLindungi application since the PDP Law was not enacted yet at that time. Next is Miftahul Jannah et al. (2023), which discusses personal data protection in telemedicine by comparing PDP Law and the European Union General Data Protection Regulation ("**GDPR**"). Their writing focuses on the comparative study on the PDP Law and the GDPR to ensure personal data protection within telemedicines.

From the aformentioned articles, no authors have analyzed specifically regarding AI-enhanced telemedicines and their effort to adopt the personal data protection principle under the PDP Law. This article also specifically highlights the nature of AI in connection with the personal data protection principles within telemedicines since none of the aformention articles discussed the aspect of AI. If the AI-enhanced telemedicines were not aware with the adoption of the personal data protection principles, the protection of patient's personal data will be on the edge and potential misuse of personal data may occur.

In this paper, the authors use statutory and comparative approach which based on the PDP Law for the statutory approach and the implementation of personal data protections from GDPR as the comparative approach to demonstrate the best practices in implementing personal data protections in the field of AI-enhanced telemedicines. Both the statutory and the comparative approach are integrated within the analysis for each personal data protection principles in Section 3.

The idea presentation is structured as follows. Section 2 analyzes the position of the telemedicine application under the legal framework of PDP Law. Section 3 analyzes the implementation of personal data protection principles from the PDP Law in the context of AI in the telemedicine application. At last, section 4 covers concluding remarks.

II. The Position of Telemedicine Applications under the Legal Framework of PDP Law

The PDP law governs 2 (two) stakeholders that process the personal data, namely Personal Data Controller ("**Data Controller**") and Personal Data Processor ("**Data Processor**"). A Data Controller is a party who determines the purpose, and controls the processing of personal data, while a Data Processor is a party who processes personal data on behalf of the Data Controller. Both Data Controller and Processor can be any person (legal entity or individual), public agency, and international organizations.

In practice, hospital or telemedicine applications may become the data controllers (Chiara Gallese Nobile, 2023). Using the definition of the Data Controller under the PDP Law, telemedicine applications may possibly become the Data Controller if they determine the purpose and exercise the control over the processing of personal data. On the other hand, they can serve as a Data Processors if they conduct personal data processing on behalf of a Data Controller, which is another legal entity, in accordance with Article 51 paragraph (1) of the PDP Law.

If we look upon the privacy policy of telemedicine applications in Indonesia such as Halodoc, they regulate and determine the purpose and the exercise of the control over the processing of personal data (Halodoc, 2023). Another example, Alodokter also governs purposes of the data processing in their privacy policy (Alodokter, 2022). However, other examples of telemedicine applications like KilkDokter only determine the general purpose of the data processing such as to process a patient's transaction and manage the application (KlikDokter, 2024). Generally, it can be concluded that telemedicine applications are a data controller in most cases. Hence, as a data controller, telemedicine applications must set a comprehensive security standard to protect personal data that is shared to them (King NJ & VT Raja, 2012).

III. AI in the Telemedicine Applications and the Implementation of Personal Data Protection Principles under the PDP Law

One of the case as an example in Indonesia concerning the data breach of personal health and medical data is the data breach from 1,3 million users of the Health Alert Card (eHAC) Application. Hence, the urgency for the protection of personal health and medical data has become higher in the present time, especially in the era where AI is often being used within health care facilities such as telemedicine. For example, the usage of personal data by AI within the telemedicines is on how the Natural Language Processing ("**NLP**") to measure and provide insights that could inform doctors when making decisions for patients using health data from thousands of consultations to train a ML model in Halodoc. As health data is also considered as personal data under Article 4 (2) of the PDP Law, therefore the usage of patients from thousands of consultations which processed by AI must be scrutiny by the personal data protection principles to safeguard the patient's personal data.

Similar to every data processing activity, the regulatory framework for personal data protection is also applicable to govern AI (Mohsin Dhali et al., 2022), hence the PDP Law is also applicable to the data processed by AI. The PDP Law in the Article 16 paragraph (2) sets out seven personal data protection principles to govern the personal data processing: lawfulness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and also accountability (Rouse, 2022). These principles should be tested in the AI environment. In the context of data processing within healthcare, especially telemedicine, personal data may be in the form of health data such as individual records or information relating to physical health, mental health, and/or health services. Each of the data protection principles in the PDP Law are analyzed in the following section to understand to what extent the telemedicines have applied the principles of personal data protection within their platform.

A. Principle of Lawfulness and Transparency

The principle of lawfulness is reflected in Article 16 paragraph (2) point (a) of the PDP Law. This principle governs that every personal data collected should be limited, legally valid, and transparent. The lawfulness of the collection of personal data may determine whether the personal data can be further processed in the next phase (Harsha Perera, 2019). The concept of transparency is also intended to be implemented to avoid the personal data of the data subject being used, disseminated, or sold to the unauthorized third parties without the data subjects' consent. To overcome this issue, the data controller must disclose the mechanisms for the processing, storing, and the collecting of personal data.

One of the telemedicine applications in Indonesia, for example Halodoc, has explained in their privacy policy that they will obtain the personal data when the data subjects already consent and they will ask for an additional consent from the patients if there is additional personal data that Halodoc collects from the Patient (Halodoc, 2023). Furthermore, Halodoc also regulates that the every disclosure of personal data will be notified to the patient and the consent for such disclosure or sharing will be the prerequisite for the data disclosure. The privacy policy also sets out the provisions regarding consent for personal data transfer outside of Indonesia and the right for data subjects to withdraw the consent on the utilization of their personal data.

On the other hand, KlikDokter only regulates that once the patients register, accessing, and/or using the services available on the application, the patients should give consent to KlikDokter to obtain, collect, store, manage, and use all the data ((KlikDokter, 2024). Alodokter has similar provision regarding consent in their privacy policy where it stated that they may disclose the personal information with the prior notice to the patient's and consent is also become the prerequisite for such disclosure (Alodokter, 2022). However, Alodokter does not regulate the provisions

regarding consent for personal data transfer outside of Indonesia and other consent provisions like Halodoc.

Seeing the above privacy policy from three telemedicine applications which utilize AI, we can conclude that the depth of regulation in their privacy policy are different. In the context of lawfulness, three of the telemedicine applications have fulfilled this principle as the data processing conducted by the telemedicine applications is based on the consent from the patient as a form of the main basis for such data processing. In the context of transparency, all the three telemedicine applications have disclosed the mechanisms for the processing, storing, and the collecting of personal data in their privacy policy.

Unfortunately, only Halodoc that regulates the provisions regarding the safeguard of patient's personal data from automated decision making within its privacy policy. Regulating automated decision making in the privacy policy is important for the patient to measure to what extent the automated decision making, which usually by AI, will affect the personal data of the patients. Furthermore, Article 10 paragraph (1) stated that personal data subjects have the right to object an automated decision making which has legal consequences or have a significant impact on personal data subjects. Hence, telemedicines must update their privacy policy to safeguard the patient's personal data from the automated decision making and simultaneously comply with the PDP Law.

B. Principle of Purpose Limitation

The principle of purpose limitation is stipulated in Article 16 paragraph (2) point (b) of the PDP Law. This principle governs that any processing and collection of (personal) data should be specified and made available to the data subject in a concise and intelligible manner. This principle sets forth the notion that every personal data must be collected for a "specific, explicit, and legitimate" purpose and cannot be further processed if it is not compatible with such original purposes (Tal Z. Zarsky, 2017). In order to adhere to this principle, entities or companies which engage in Big Data analysis (including AI) need to notify their data subjects regarding the form of data processing they will conduct and closely monitor such activities. Furthermore, data processing with AI applications which utilize big data comprise algorithms that can process data unexpectedly, which may result in unforeseen outputs (GVKS Abhinav & S Naga Subrahmanyam, 2019).

However, if the companies define the limitation of the data processing in a vague and a very broad way for the future data processing, it will not align with this principle as the purpose should be "specific". In addition, setting a broad purpose of data processing might even be considered as unacceptable processing since it does not specifically define the purpose of the data processing (Viktor Mayer-Schonberger, 2016). Therefore, it is important to explicitly list the use of AI and identify the specific document and specific purposes of the upcoming data processing at an early stage

and in a proportionate manner, which is not too broad or too specific. In addition, providing transparency and meaningful technical assistance to express patient choices may be additional solutions to maintain and conduct data reuse (Matt Burgess, 2017).

The use of AI in the telemedicine application retains the risk of possible violation of the purpose limitation principle, for example AI models including in the health care system generally clash with the purpose limitation principle (Mohsin Dhali et al., 2022). Such clashes may be avoided by defining the scope of processing in a proportionate and compatible manner. Compatibility in the context of purpose limitation principle concerns the relationship between the new purpose and the original purpose of the data processing. Hence, the relevant stakeholder (e.g., data controller) must note that the compatibility of the new purpose with the original purpose should be determined by the connection between such purposes, the context of the data processing, the nature of the personal data, and the possible impact towards the data subject.

In the context of telemedicine applications in Indonesia which use AI, Halodoc is the only telemedicine that provides comprehensive regulations in their privacy policy regarding the specific purpose of their data collection and usage (Halodoc, 2023). It lists down several specific purposes such as to provide services, to process and facilitate payment, to improve and personalize the platform to meet the needs and preferences of the patients and other specific purposes. Halodoc also mentions in their privacy policy that they will act fairly and not use the personal data of the patients, not more than what is needed to achieve the intended purpose. Generally, Halodoc provides a positive effort towards implementing the principle of purpose limitation in their privacy policy.

While Halodoc provides a detailed specific purpose for the usage of patients personal data in their privacy policy, Alodokter's privacy policy also lists down several purposes of their data collection and usage although not as detailed as Halodoc and only sets the purpose more general (Alodokter, 2022). It provides that the collected personal data will be used by Alodokter for the purpose of conducting internal compliance requirements, monitoring health or medical conditions, managing or resolving any complaints, and other purposes. Yet, Alodokter did not mention that it will consistently look upon the intended purpose throughout every personal data processing activities in their telemedicine similar to what Halodoc has mentioned in their privacy Policy.

On the other hand, KlikDokter did not govern any purposes on the collection and processing of the patient's personal data in their privacy policy (KlikDokter, 2024). Hence, KlikDokter should list down the specific purposes in their privacy policy to improve the protection of patient's personal data throughout every collection and data processing in their platform, with further taking into account the

algorithms of AI that are unexpected for humans (Scherer, M.U. 2016). Regulating the specific purposes for the data collection and data processing act may be helpful for the patients to oversee the potential activities conducted by the telemedicine application and it can become the standard for the telemedicines to always base any activities relating to patients personal data with such purposes.

C. Principle of Data Minimization

In the PDP Law, this principle is enshrined in the Article 16 paragraph (2) point (b) and point (g) of the PDP Law. This principle generally governs that the data collected shall be limited, adequate, and is not excessive to the intended purpose by also taking into account a limited period of time on the usage of the personal data (Tal Z. Zarsky, 2017). AI, by its nature, may improve its performances by utilizing large-scale datasets (Chen Sun and others, 2017). The excessive collection of personal data may increase the risk of such data being discovered unexpectedly. Hence, telemedicine companies as data controller/data processor must effectuate the usage of the personal data in its personal data processing activities. In practice, this was shown for example in Article 25 of the EU's General Data Protection Regulation ("**GDPR**") which stipulates that data minimization is a part of data protection by design and default (GDPR, 2016). It indicates that this principle must be implemented alongside the concept of privacy by design and privacy by default, which obliges telemedicine companies to integrate the protection principles in the architecture/design of their platform (Chiara Gallese Nobile, 2023).

While the concept of privacy by design and privacy by default is not regulated in the PDP Law, it is highly recommended for the telemedicine companies in Indonesia to implement such concepts in their application's policy to ensure that privacy issues will not impede the delivery of the health care. For example, the Individual Privacy Act (2018) and the Individual Privacy Regulation (2020) from Nepal that requires companies such as telemedicines to apply the principle of privacy by design. Other examples include the Law Protecting the Privacy and Security of Citizens from Myanmar which also oblige the implementation of privacy by design and defaults towards platforms which process personal data like telemedicines (Sharma P et al., 2023). Company may include the provision regarding privacy by design or default in their privacy policy by stating that the telemedicines have incorporated a large number of privacy protections into the technology itself, which provide security and control both for the telemedicines and the patients (A. Cavoukian et al., 2010).

In the context of the use of AI in the telemedicine application, one of the risks pertaining to the violation of the data minimization principle is that AI activities require large amounts of personal data (M Butterworth, 2018). Predicting the specific type and amount of data required for AI applications is highly difficult considering it is yet to be determined by the application in the first place (Boris P. Paal, 2022). In this regards, the clash between the implementation of data minimization principle

and the nature of AI can be reduced if the additional personal data processed is utilized for the advantage of the patient and if such processing outweighs any additional risks to the patient. This notion is to liberalize the collection of data as long the regulation of data usage must be comprehensive, using a risk-based approach which anticipates the possible harm to promote the responsible use of personal data (Antoinette Rouvroy, 2016).

In the context of telemedicine application, Halodoc as one of the telemedicine applications in Indonesia governs the principle of data minimization in their privacy policy. It stated that the collection of the patient's personal data should always be in accordance with the original purpose for which the personal data was collected Halodoc, 2023). On the other hand, other telemedicine applications with AI such as Alodokter and Klikdokter did not regulate that every data processing should always be inline with the original intended purpose, meaning that the principle of purpose limitation is not reflected yet in their privacy policy. Hence, Alodokter and Klikdokter should amend their privacy policy to demonstrate their commitment to implement the principle of purpose limitation by also regulating that every data processing will always be in line with the original intended purpose throughout the data processing activities.

Compliance with this principle is essential in the usage of telemedicine applications, as health data is included, and the doctor is not directly monitored the patients. Such concern has arisen in the European Commission and hence classified the medical devices such as telemedicine as "high risk systems" (Chiara Gallese Nobile, 2023).

D. Principle of Accuracy

The principle of accuracy is enshrined in Article 16 paragraph (2) point (d) of the PDP Law. This principle governs that the data controllers must ensure that the collected personal data already depict the real and actual condition in order to prevent the data subjects to suffer any disadvantage from the inaccuracy of the personal data (Boris P. Paal, 2022). Hence, personal data must be accurate and kept up to date according to this principle (L Mitrou, 2018).

In addition, if there is something inaccurate about the personal data of the data subject, the data subject may correct the inaccuracy and demand the data controller to fix it. The data controller must, as soon as possible, fix and update it to ensure the future data processing is in line with the original intended purpose and use the appropriate personal data of the data subject. Therefore, data controllers must be ready to provide immediate services to delete or fix any inaccuracy of personal data to ensure the fulfillment of this principle (Diana Dimitrova, 2021).

In the context of AI, it is still questionable whether AI which uses big data analytics can make sure of the accuracy of data, considering the amount of data

being processed in AI is generally large (L Mitrou, 2018). If the inaccurate data from AI brings disadvantages towards the data subjects such as incorrect prediction and analytics regarding performance of work, it will automatically violate this principle.

If we see the privacy policy of the three telemedicine applications, Halodoc stated that the patient also has the obligation to provide the most accurate personal data and is not misleading (Halodoc, 2023). Halodoc also provides the mechanism regarding any change of personal data in the case of inaccurate data. On the other hand, KlikDokter does not regulate anything regarding the commitment to ensure the accuracy of personal data in their privacy policy (KlikDokter, 2024). Alodokter made a positive effort by stating in their privacy policy that they have the duty of care to ensure that the personal data of the patient is accurate and up-to-date and the mechanism for any changes of patient's personal data is provided (Alodokter, 2022).

Two out of three telemedicines have tried to fulfill the obligation under the principle of accuracy as can be seen in their privacy policy, especially by providing explicit mechanisms to change personal data in case of inaccuracy. Other than that, the telemedicines application may increase the compliance of this principle by ensuring the training process of the AI is inputted with accurate data, which is representative towards the real environment and does not result in any disadvantages such as bias (L Mitrou, 2018).

E. Principle of Storage Limitation

The principle of storage limitation is reflected in Article 16 paragraph (2) point (g) of the PDP Law. This principle mandates that where the personal data is stored, the usage of the personal data is permissible only as long as it is necessary (Boris P. Paal, 2022). In general, this principle is difficult to implement effectively in the platform with AI as the deletion/retention and other restriction of personal data after the processing of personal data is finished may impede the use and the development of AI. It is well established in the other states who govern the principle of storage limitation in their personal data protection act that data controllers must establish the specific time limit for the data storage, retention, or deletion in order to comply with this principle (Boris P. Paal, 2022).

The privacy policy of the telemedicine application in Indonesia for example Halodoc's privacy policy regulates that it would store the necessary personal data as long as the patients are still using the platform or according to the period of time required by the applicable laws, such as PDP Law (Halodoc, 2023). Furthermore, Halodoc's privacy policy also explicitly regulates that the retention period of patient data is pursuant to the applicable laws and regulations. Generally, Halodoc provides an acceptable policy relating to the principle of storage limitation as it mostly refers to the applicable laws and regulations.

On the other hand, Alodokter's privacy policy regulates that upon a request from the patient to deactivate their account, Alodokter will deactivate their account

and archive their personal information (Alodokter, 2022). Such archived information will be retained for a period of 5 (five) years and even longer if required legally as to be able to comply with the legal obligations. The explicit 5 (five) years period of retention in Alodokter's privacy policy is a great example to make the patient aware of how long the telemedicine application will have access to their personal data.

KlikDokter in their privacy policy governs that it will delete the patient's data in accordance with applicable legal provisions and only save the data of the patient as long as the patient's account is active (KlikDokter, 2024). KlikDokter policy on deletion of data also refers to the applicable legal provision such as the existing PDP Law. In general, KlikDokter and Halodoc have a similar policy regarding the storage limitation while Alodokter stated a specific period of time on the data retention which is 5 (five) years. The other two telemedicine applications should also govern the specific period of time on the data retention as similar to Alodokter since telemedicine applications as the data controller should establish such time limits to comply with the principle storage limitation (Boris P. Paal, 2022).

F. Principle of Integrity and Confidentiality

The principle of integrity and confidentiality is reflected in Article 16 Paragraph (2) point (e) of the PDP Law. This principle generally mandates data controllers to ensure the personal data is protected over unlawful or unauthorized data processing and also accidental damage and loss of the personal data (Borgesius Chris Jay hoofnagle at al., 2019). In consequence, data controllers must have adequate technical security systems to prevent any misuse of personal data throughout the data processing or the utilization of the personal data. The data controller is, in any case, responsible for any unexpected damage or loss towards the personal data. Therefore, not only an adequate technical security system, but data controllers must also have skilled human resources and robust systems in general.

If we see the privacy policy from the three telemedicines, Halodoc has provided that they guarantee the data and the information provided by the patients is confidential and will not be shared except for the matters that have been agreed by the patient (Halodoc, 2023). Halodoc also stated that in the event of data breach, they will notify the patient in accordance with the applicable laws and regulations to provide the data subjects affected with sufficient information regarding the data breach and will work to safeguard against the misuse of the personal data. In addition, Halodoc also mentions the type of personal data which are exempted from confidentiality such as the data disclosure with the consent of the data subject and others.

On the other hand, KlikDokter did not mention anything in their privacy policy regarding the commitment to uphold the security of the personal data (KlikDokter, 2024). While Alodokter explicitly stated in their privacy policy that all personal data is stored in their highly secure platform (Alodokter, 2022). Even so, Alodokter still gives a disclaimer that no transmission of data can be guaranteed to be 100% secure.

The implementation of the principle of integrity and confidentiality may not be fully seen from the privacy policy of the respective platform. However, Halodoc has implemented this principle with quite comprehensive provisions compared to the other telemedicines. To improve the compliance of this principle, all of the telemedicine applications may evaluate their privacy policy to include more detailed provisions regarding the commitment on integrity and confidentiality. Furthermore, telemedicine as data controllers must be aware of the rapid development of technology which pertains to wider and more unique risks towards the protection of personal data. Hence, they should improve the technical security system of their data security to consistently comply with this principle.

G. Principle of Accountability

The principle of accountability in the context of personal data processing is reflected under Article 16 Paragraph (2) point (h) of the PDP Law. This principle governs that every personal data processing must be carried out responsibly and can be clearly proven. Under the obligation of this principle, data controllers are required to prove and demonstrate that all activities including collecting and processing the personal data are in compliance with all provisions related to the personal data protection law (Christopher F. Mondschein & Cosimo Monda, 2019). The main goal of this principle is to make sure data controllers perform accountability by reporting any data processing activities to the relevant supervisor which is the government. Therefore, the existence of DPA is really essential to audit, observe, and analyze whether the data controllers such as telemedicine applications have implemented personal data protection in their data processing activities.

Currently, It is difficult to apply the principle of accountability as the supervisor for the data processing, collection, and the storage of personal data such as DPA has not been implemented in Indonesia. Since the DPA is not yet established in Indonesia, the enforcement of the compliance on personal data protection laws and regulations is still not effective, especially to supervise the telemedicine application which holds patient's specific personal data such as health data information as regulated in the Article 4 of the PDP Law. Therefore, The government of Indonesia must establish the DPA as soon as possible to keep up with the current development of technology which pose higher risk towards personal data protection.

IV. Conclusion

Besides the various benefits provided by AI, AI in the telemedicine application also poses risk, especially towards the protection of patient's personal data. Under the regime of PDP Law, telemedicine applications in Indonesia may be categorized as data controllers. This is due to the reason that most of the telemedicine applications determine the specific purpose of the data processing, as in line with the definition of the data controller under the PDP Law.

The PDP Law sets out seven principles in Article 16 paragraph (2), namely the principle of lawfulness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. The three telemedicines have different depth for their privacy's policy to adopt with the above-mentioned principles which implied that the three telemedicines have not fully implemented the personal data protection principles in the PDP Law. To deal with that problem, the telemedicines should update their privacy policy to include the provisions regading mechanism for data collection and processing to be as transparent as possible, specific purpose of the data processing, data processing activities which only based on the intended purpose, assurance on the accuracy of the personal data, specific period for the data retention, and the obligation to enhance the system security to prevent hacking or other malicious act. Lastly, the government of Indonesia must accelerate the enactment of the implementing regulation for the PDP Law in order to fully enforce the personal data protection principles towards every data controller including telemedicines.

References:

Abhinav, G V & Subrahmanyam S, Dr. (2019). Artificial Intelligence in Healthcare. Journal of Drug Delivery and Therapeutics. 9. 10.22270/jddt.v9i5-s.3634.

Alodokter, "Kebijakan Privasi", accessed from <https://www.alodokter.com/privasi>

Antoinette Rouvroy. (2016). "Of Data and Men": Fundamental Rights and Freedoms in a World of Big Data, COUNCIL OF EUR., DIRECTORATE GEN. OF HUM. RTS. AND RULE OF L., at 11 (Jan. 11, 2016), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTM Content?documentId=09000016806a6020.

Borgesius Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen. (2019). The European Union General Data Protection Regulation: What It Is and What It Means`. *Information & Communications Technology Law*, Volume 28 Number 1.

BRIN. (2020). "Pemanfaatan AI dalam Penanganan Covid-19 Berguna Hadapi Pandemi Selanjutnya", accessed from <https://www.brin.go.id/news/112883/pemanfaatan-ai-dalam-penanganan-covid-19-berguna-hadapi-pandemi-selanjutnya>

Cavoukian, A., Fisher, A., Killen, S. *et al.* (2010). Remote home health care technologies: how to ensure privacy? Build it in: *Privacy by Design . IDIS* **3**. https://doi.org/10.1007/s12394-010-0054-y

Chen Sun and others. (2017). Revisiting Unreasonable Effectiveness of Data in Deep Learning Era', *Proceedings of the IEEE International Conference on Computer Vision*.

Christopher F. Mondschein and Cosimo Monda. (2019). The EU's General Data Protection Regulation (GDPR) in a Research Context, in Fundamentals of Clinical Data Science. Springer International Publishing, Switzerland.

Dashika Gnaneswaran, Microsoft. (2017). "BP Healthcare's Doctor2U partners with Microsoft for its Digital Transformation journey", accessed from <https://news.microsoft. com/en-my/2017/05/24/bp-healthcares-doctor2u-partners-microsoft-digital- transformation-journey/>

Dimitrova, Diana, The Rise of the Personal Data Quality Principle. (2021). Is it Legal and Does it Have an Impact on the Right to Rectification? Available at SSRN: https://ssrn.com/abstract=3790602 or http://dx.doi.org/10.2139/ ssrn.3790602

Dwi Wulandari, Mix.co.id. (2021). "Gandeng GI Vita, KlikDokter Hadirkan Layanan Kesehatan Berbasis AI", accessed from <https://mix.co.id/marcomm/news-trend/gandeng- gi-vita-klikdokter-hadirkan-layanan-kesehatan-berbasis-ai/>

Edwards, Lilian and Veale, Michael. (2017). Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For (May 23, 2017). 16 Duke Law & Technology Review 18, Available at SSRN: https://ssrn.com/abstract=2972855 or http://dx.doi.org/10.2139/ssrn.2972855

Fernandes, Jefferson. (2021). Artificial Intelligence in Telemedicine. 10.1007/978-3-030-58080-3_93-1.

Gallese, Chiara. (2023). Legal Aspects of the Use Artificial Intelligence in Telemedicine. Journal of Digital Technologies and Law. 1. 314-336. 10.21202/jdtl.2023.13.

Halodoc. "Kebijakan Privasi Halodoc", accessed from <https://www.halodoc.com/kebijakan-privasi>

Happy Amanda Amalia, Investor.ID, "Alodokter Luncurkan Dua Fitur Baru Layanan Kesehatan Berbasis AI", accessed from <https://investor.id/lifestyle/325484/alodokter-luncurkan-dua-fitur-baru-layanan-kesehatan-berbasis-ai>

Hashiguchi, T. C. O., Oderkirk, J., & Slawomirski, L. (2022). Fulfilling the Promise of Artificial Intelligence in the Health Sector: Let's Get Real. *Value in health: the journal of the International Society for Pharmacoeconomics and Outcomes Research*, *25*(3), 368–373. https://doi.org/10.1016/j.jval.2021.11.1369

Heather Landi, Fierce Healthcare, "Amwell rolls out new telehealth platform that integrates with digital health tools", accessed from <https://www.fiercehealthcare.com/tech/amwell-rolls-out-new-telehealth-platform-integrates-wearables-ai-tools>

Hoofnagle, Chris Jay and van der Sloot, Bart and Zuiderveen Borgesius, Frederik. (2018). The European Union General Data Protection Regulation: What It Is and What It Means. *UC Berkeley Public Law Research Paper*, Available at SSRN: https://ssrn.com/abstract=3254511 or http://dx.doi.org/10.2139/ssrn.3254511

J. Angelo Racoma, tn global, "Doctor Anywhere's Lim Wai Mun on Adapting AI Strategies in Healthcare Across Diverse Markets", accessed from <https://technode.global/2023/10/18/doctor-anywhere-lim-wai-mun-on-adapting-ai-strategies-in-healthcare-across-diverse-markets/

Kementerian Keuangan, "Pemanfaatan Kecerdasan Buatan dalam Lembaga Pemerintah: Meningkatkan Efisiensi dan Pelayanan Publik yang Lebih Baik", accessed from <https://www.djkn.kemenkeu.go.id/kpknl-manado/baca-artikel/16383/Pemanfaatan-Kecerdasan-Buatan-dalam-Lembaga-Pemerintah-Meningkatkan-Efisiensi-dan-Pelayanan-Publik-Yang-Lebih-Baik.html>

King NJ, Raja VT. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Comput Law Secur Rev, Vol. 28 (3).

KlikDokter, "Kebijakan Privasi KlikDokter", accessed from <https://www.klikdokter.com/kebijakan-privasi>

Kominfo, "Wamenkonminfo Dorong Adopsi Teknologi AI untuk Kedokteran", accessed from <https://www.kominfo.go.id/index.php/content/detail/52557/siaran-pers-no-419hmkominfo102023-tentang-wamenkominfo-dorong-adopsi-teknologi-ai-untuk-kedokteran/0/siaran_pers>

L Mitrou. (2018). Data Protection, Artificial Intelligence and Cognitive Services: Is the GDPR "Artificial IntelligenceProof"? *Tech Report commissioned by Microsoft*, 58 https://ssrn.com/abstract=3386914 (hereafter Mitrou, 'Data Protection').

M Butterworth. (2018). The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework 34(2). *Computer Law & Security Review: The International Journal of Technology Law and Practice*.

Mayer-Schönberger, Viktor. (2016). Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation. Columbia Science & Technology Law Review. 17. 315.

Matt Burgess, "NHS DeepMind deal broker data protection law, regulator rules", accessed from <https://www.wired.com/story/google-deepmind-nhs-royal-free-ico-ruling/>

McKinney, Scott & Sieniek, Marcin & Godbole, Varun & Godwin, Jonathan & Antropova, Natasha & Ashrafian, Hutan & Back, Trevor & Chesus, Mary & Corrado, Greg & Darzi, Ara & Etemadi, Mozziyar & Garcia-Vicente, Florencia & Gilbert, Fiona & Halling-Brown, Mark & Hassabis, Demis & Jansen, Sunny & Karthikesalingam, Alan & Kelly, Christopher & King, Dominic & Shetty, Shravya. (2020). International evaluation of an AI system for breast cancer screening. Nature. 577. 89-94. 10.1038/s41586-019-1799-6.

Mediana, Kompas.Id, "Penggunaan Kecerdasan Buatan dalam Telemedik", accessed from <https://www.kompas.id/baca/dikbud/2021/02/16/penggunaan-kecerdasan-buatan-dalam-telemedik>

Michael Butterworth. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review: The International Journal of Technology Law and Practice*. Doi: 10.1016/j.clsr.2018.01.004

Mohsin Dhali, Shafiqul Hassan, Sonny Zulhuda, Suzi Fadhilah Bt Ismail. (2022). Artificial intelligence in health care: data protection concerns in Malaysia, *International Data Privacy Law*, Volume 12, Issue 2. https://doi.org/10.1093/idpl/ipac005

Mondschein, Christopher & Monda, Cosimo. (2019). The EU's General Data Protection Regulation (GDPR) in a Research Context. 10.1007/978-3-319-99713-1_5.

Naik, N., Hameed, B. M. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Rai, B. P., Chlosta, P., & Somani, B. K. (2022). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?. *Frontiers in surgery*, *9*, 862322. https://doi.org/10.3389/fsurg.2022.862322.

Nurfikri, Ari; Karnadipa, Triana; and Roselina, Elsa (2022) "TELEMEDICINE APP: WHAT'S NEXT AFTER PANDEMI?," Jurnal Administrasi Bisnis Terapan (JABT): Vol. 5: Iss. 1, Article 3. DOI: 10.7454/jabt.v5i1.1036 Available at: https://scholarhub.ui.ac.id/jabt/vol5/iss1/3

Perera, Harsha & Hussain, Waqar & Mougouei, Davoud & Shams, Rifat & Nurwidyantoro, Arif & Whittle, Jon. (2019). Towards Integrating Human Values into Software: Mapping Principles and Rights of GDPR to Values. 404-409. 10.1109/RE.2019.00053.

Paal BP. Artificial Intelligence as a Challenge for Data Protection Law: And Vice Versa. In: ; :290-308.

Rouse, "2022 Indonesian Data Protection Law", accessed from <https://rouse.com/media/vfjiy0ac/rouse-2022-indonesian-data-protection-law-guide.pdf>

Sareen, S., Saltelli, A. & Rommetveit, K. Ethics of quantification: illumination, obfuscation and performative legitimation. *Palgrave Commun* 6, 20 (2020). https://doi.org/10.1057/s41599-020-0396-5

Scherer, Matthew U. (2015). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, Vol. 29, No. 2, Spring 2016, Available at SSRN: https://ssrn.com/abstract=2609777 or http://dx.doi.org/10.2139/ssrn.2609777

Sharma P, Sethi MIS, Liem A, Bhatti HBS, Pandey V, Nair A (2023) A review of telemedicine guidelines in the South-East Asia Region, Telemedicine Reports 4:1, 271–278, DOI: 10.1089/tmr.2023.0040.

Stephenson J. (2021). WHO Offers Guidance on Use of Artificial Intelligence in Medicine. *JAMA health forum*, *2*(7), e212467. https://doi.org/10.1001/jamahealthforum.2021.2467.

Sun, Chen & Shrivastava, Abhinav & Singh, Saurabh & Gupta, Abhinav. (2017). Revisiting Unreasonable Effectiveness of Data in Deep Learning Era.

T Zarsky. (2017). Incompatible: The GDPR in the Age of Big Data. 47 *Seton Hall Law Review* 995, 1005 et seq.