JOURNAL OF INTERNATIONAL STUDIES
https://e-journal.uum.edu.my/index.php/jis

How to cite this article:
Hadiyantina, S., Ayub, Z. A., Cahyandari, D., Paramitha, A. A., & Mohamed Yusoff, Z. (2022). Transborder data flows: Protection of medical tourist personal data in Malaysia and Indonesia. *Journal of International Studies, 18,* 269-291. https://doi.org/10.32890/jis2022.18.10

TRANSBORDER DATA FLOWS: PROTECTION OF MEDICAL TOURIST PERSONAL DATA IN MALAYSIA AND INDONESIA

[1]Shinta Hadiyantina, [2]Zainal Amin Ayub, [3]Dewi Cahyandari, [4]Amelia Ayu Paramitha & [5]Zuryati Mohamed Yusoff
[1,3&4]Department of Administrative Law, Faculty of Law, Universitas Brawijaya, Indonesia
[2]Legal & Justice Research Centre, School of Law, Universiti Utara Malaysia
[5]School of Law, Universiti Utara Malaysia

[1]Corresponding author: shinta_fh@ub.ac.id

Received: 27/4/2022 Revised: 5/7/2022 Accepted: 18/7/2022 Published: 17/10/2022

ABSTRACT

Medical tourism is popular within the Association of Southeast Asian Nations (ASEAN) region, especially in the Indonesian region. The economic prosperity, closer vicinity as compared to Jakarta, and the quality of medical services provided in the neighbouring countries lead to medical tourism prospering among the Indonesians. Malaysia is one of the most frequently visited countries by Indonesians as medical tourists. The growth of medical tourism triggers issues of the adequacy of the Indonesian and Malaysian laws to regulate cross-border medical records. It is the aim of this study to examine the adequacy of the current laws in handling cross-border medical

records. This study applied doctrinal legal research methodology, i.e., mainly library-based research, where the main legal materials were from Malaysia and Indonesia. It was found that the need for personal data protection is a necessity since boundaries among jurisdictions are becoming "borderless". The Malaysian law, although comprehensive, has yet to gazette any country as a "whitelisted country" to allow for cross-border data. The Indonesian law does not regulate cross-border medical records. The risk of personal data leakage has become imminent. The importance of cross-border medical records protection is important to create safe integrated medical records. While Malaysia has enacted a comprehensive legal framework on personal data protection (including medical data), Indonesia needs to enhance its legal framework in protecting the data. Regionally, the legal framework of cross-border personal data between Malaysia and Indonesia should be updated in accordance with the ASEAN Data Management Framework.

Keywords: Medical tourism, transborder data flows, medical record, cross-border healthcare, personal data protection, Indonesia and Malaysia.

INTRODUCTION

The importance of maintaining good health is undeniable and people are becoming more and more health conscious. They are willing to do all the necessaries in order to maintain good health, including to travel abroad for the purpose of obtaining medical treatment, which is also known as medical tourism. Medical tourism is experiencing an increase in growth every year. This is motivated by the economic growth and technological developments that make it easier for everyone to travel abroad. Apart from the economic growth and technological advances, medical tourism is also caused by several reasons, namely medical costs, the absence of domestic facilities and experts in the field, as well as availability of medical facilities. Medical tourism has a long history in accordance with medical development itself; this has been done since the days of Ancient Greece and Ancient Egypt until it continued in the 18th century when people sought treatment in various countries to treat tuberculosis (Pickert, 2008).

Indonesia is one of the countries whereby the majority of the middle- and upper-class population are consumers of medical tourism. Every

year, there are around 670,000 Indonesians who acquire treatment in Malaysia (Malaysia Healthcare Travel Council, 2018). This number occupies the highest percentage where 60 percent of the patients are Indonesian citizens. Since 2011–2019, the number of medical tourism patients continued to increase, where Indonesian citizens dominated this percentage. The growing number of Indonesian medical tourists reflect the growth of the nation's economy. Indonesia's economy in the last ten years, as measured by the gross domestic product at current prices and gross domestic product at constant prices, shows an increasing trend (Badan Pusat Statistik, 2020; 2015). Indonesia's economic growth from 2010–2020 was in the range of (4%–6%) annually. The top two countries that become medical tourism destinations for Indonesian citizens are Malaysia and Singapore. Both countries are the top medical tourism destinations because of their proximity to Indonesia. In addition, by overall medical quality, these two countries occupied the highest rank in Southeast Asia. The ranking of medical quality in the world's top 50 countries is filled by three members of the Association of Southeast Asian Nations (ASEAN), which are Singapore (27), Malaysia (29), and the Philippines (37), while Indonesia itself is in fact positioned at number 55 (Numbeo, 2021). The Healthcare Index or ranking is based on five variables: general statistical analysis, infrastructure, quality, availability of medicines, and competence of health workers. When compared between Malaysia and Singapore in terms of the number of patient visits from Indonesia, Malaysia ranks first. This is due to the affordable prices offered by Malaysia as compared to Singapore. With the same quality, Malaysia provides prices that are (30%–50%) cheaper than Singapore and (45%–80%) cheaper than the United States of America (USA) (Patients Beyond Borders, 2020). Higher medical care in Singapore is due to high medical inflation. Since 2015, the health system in Singapore has experienced inflation of (8%–9%) per year (Statista, 2020). The similarity of culture and language is also one of the reasons why many Indonesian citizens choose Malaysia.

The high number of medical tourists from one country to another country causes new problems, i.e., the issue of protection of transborder or cross-border personal data. The data of patients who receive medical treatment abroad create concerns among medical tourists. The main problems are twofold, the protection of the outgoing data of the medical tourists from their country of origin, and the outgoing data from the visiting country to the home country. Both countries must have legal

protection to the transborder of personal data of the medical tourists. The importance of medical data protection as highlighted by Figg and Kam (2011, p. 24) is that "medical identity theft is the fastest-growing form of healthcare fraud". Besides, while the healthcare providers may suffer loss of reputation if there is any breach of their patients' medical data, the impact will also be detrimental against the patients because their identity can be used for identity fraud (Information Commissioner's Office, 2022). Other negative impacts of breach of medical data upon the patients inter alia are financial loss, alteration or false patients' entry record, harassment, etc. (Figg & Kam, 2011).

Nevertheless, the increased number of foreign patients has opened possibilities of Malaysian healthcare providers being subjected to malpractice claims and triggering a myriad of cross-border legal issues. Presently, there is no internationally accepted legal framework to regulate medical tourism and issues of legal redress in relation to unsatisfactory provision of treatment across international boundaries. The economic benefits of medical tourism must be based upon a solid legal regulatory framework and strong ethical standards as well as upon high-quality medical and healthcare services (Kassim, 2009). There is a dearth of studies on cross-border healthcare data flows in context within the ASEAN region. There are studies on data protection in Malaysia by Kassim (2009), on ASEAN by Tampubolon and Ramadan (2020), and security of health crisis in ASEAN by Azmi et al. (2021). The present study is important to give insights on the cross-border data flow of medical records regionally, in particular, between Indonesia and Malaysia. For this reason, the study aims to examine the adequacy of current legal framework in these two countries, i.e., Indonesia and Malaysia, in regulating and handling the cross-border medical data of patients.

METHODOLOGY

The setting up of this article is the transborder or cross-border of medical tourists' medical data between Indonesia and Malaysia, while ASEAN is referred to as a point of critique. Henceforth, it is the aim of this article to examine the legal protection given to the transborder of patients' personal data of medical records between Indonesia and Malaysia. To achieve the objective, this article employed doctrinal legal research, or also known as black-letter legal research, which is

mainly library-based legal research (Mohd et al., 2018; Hutchinson & Duncan, 2012). Doctrinal research methodology is largely documentary (Salter & Mason, 2007). Doctrinal research defines what the law in a particular area is. In doing so, the researcher collects and analyses the data from the primary and secondary sources. Primary sources are the statutes and decided cases, i.e., judgements from the court. Secondary sources are, inter alia, articles, books, commentaries, and online materials (Dobinson & John, 2017). As such, most of the legal materials are on Malaysia and Indonesia's positive laws, on medical records and data protection.

FINDINGS/RESULTS

In this section, the authors used primary and secondary data from the primary and secondary sources to evaluate the protection of transfer of medical tourists' data between Indonesia and Malaysia.

Medical Tourism and Transfer of Medical Data

Medical tourism is the practice of travelling to another country to obtain healthcare services. Among the healthcare services sought by patients in another country are organ transplant, reproductive treatment, and dental treatment (Smith et al., 2011). Travellers are defined as persons who stayed away, travelled for more than 24 hours from their home country, and used any form of accommodation facility, to which they are also considered as tourists (Douglas & Derrett, 2001). Medical tourism is not a new practice, but the trend of the practice is new (Eissler & Casken, 2013). In the past, medical tourism involved elites from developing and third-world countries who travelled to developed countries in search of sophisticated and high-quality medical treatments. The trend changed in recent years in that the practice of medical tourism now involves ordinary groups of people from developed countries searching for affordable treatments in developing countries because of the expensive healthcare procedures required in their home countries (Mutalib et al., 2017).

In 2022, medical tourism is popular among the people of the Republic of Indonesia. They seek treatment regionally, especially from Malaysia and Singapore. In Malaysia, medical tourism has been identified as

one of the main sectors to contribute to the growth of the nation's economy since 1998 (Ormond et al., 2014). One of the challenges identified in relation to medical tourism is the protection of medical records (Kassim, 2009).

A medical record is a document that describes the patient's history, clinical findings, diagnostic results, actions before and after treatment, patient development, and treatment (Bali et al., 2011). Before the word "medical record" was widely used, other terms used were "medical documents", and "medical recording systems". The oldest medical record documents that were found and well-documented are medical records that originated from the ancient Egyptian civilisation (Al-Awqati, 2006). Hippocrates, a well-known ancient Greek physician who lived about 2,400 years ago (Grammaticos & Diamantis, 2008), also documented the treatments he gave to the patients at the Temple of the God Asclepius. Hippocrates wrote a document about his patient containing the symptoms and the patient's arrival to determine the care and treatment that the patient would receive. Hippocrates also kept these documents that were used for further treatment (Cheng, 2001). Confidentiality between doctor and patient was also regulated and included as a standard code of ethics by Hippocrates. Furthermore, the principles it creates cover the actions that should and should not be performed on patients (Moskop et al., 2005).

In the digital era, these data are easily transferred cross-border since the data are now in digital form. Therefore, the protection of electronic medical record data from patients who are undergoing medical treatment in different jurisdictions is crucial. When undergoing medical treatment, there are two types of treatment undergone by Indonesian patients going abroad: the first-time treatment at the destination hospital, or follow-up treatment that has previously been carried out at Indonesian hospitals. For the first instance, the concern is seen from the perspective of Malaysian law, while for the second scenario, the concern involves both the applications of Indonesian and Malaysian laws. This is due to the difference of jurisdictions between Malaysia and Indonesia during the cross-border transfer of medical records. Every patient who receives medical treatment at a different hospital, either on their own will or the transfer is made by the hospital, has the right to get a copy of their medical record that will later be brought to the destination hospital. This is done in order to integrate a follow-up care to optimise the treatment that patients are given and as a form of

appreciation for the patients' autonomy. Therefore, medical tourism and medical records together with the cross-border transfer of data are intertwined, which have to be discussed to protect the privacy and personal data of the patients in every part of the world. The following sections or subtopics further discuss the matter.

Protection of Privacy and Personal Data as Human Rights

After the Second World War, there are developments of the concept of individualism-based rights related to personal protection, such as freedom of religion, the right to live, and not being tortured. Human rights are an appreciation of the natural fundamental rights that every human being has. The concept of human rights continues to develop and change in line with changes in society itself and generally only centres on the right to freedom of thought, the right to believe, freedom of expression, the right to access free healthcare, and the right to an impartial trial (Woogara, 2001). In the recent research on data protection, human rights are also included as an umbrella of legitimacy for protecting individuals and collective data. The introduction of this concept is accepted because human rights are universal in nature, which is recognised regardless of boundaries and time. The concept of privacy, which is identified as part of human rights, is carried out so that there are no obstacles to the introduction of this concept throughout the world (Yusoff & Ayub, 2019). This is also done so that all individuals have the same understanding of the concepts of personal data protection that exist in the right to privacy. The recognition of privacy in human rights will also make it a new standard of morality that can be included in norms, both decency and legal norms. The recognition of the right to privacy, which is one of the important aspects of human rights, has long been accepted and articulated as "a right to be let alone" (Warren & Brandeis, 1890; Ayub & Yusoff, 2007). In their writings, Warren and Brandeis (1890) both intensified human rights into the right to enjoy life, then the right to live is extended to the right to enjoy life, and the right to enjoy life is extended to the right to be let alone and is now known as the right to privacy. This right to privacy and personal data protection is reflected in the Universal Declaration of Human Rights (Ayub & Yusoff, 2015), where the article reads,

> "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor

> to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Likewise, Indonesia recognises the right to privacy in its constitution, the 1945 Constitution of the Republic of Indonesia, through two articles contained therein. Article 28G Section (1) reads,

> "Every person shall have the right to protection of his/herself, family, honour, dignity, and property, and shall have the right to feel secure against and receive protection from the threat of fear to do or not do something that is a human right."

While Article 28F states that,

> "Every person shall have the right to communicate and to obtain information for the purpose of the development of his/herself and social environment, and shall have the right to seek, obtain, possess, store, process and convey information by employing all available types of channels."

Not surprisingly, the importance of privacy and personal data protection nowadays is also related to the activities of mass data collection. Mass data collection is a civilian data collection activity carried out by the private sector or the public sector. As long as the data collection involves a great deal of personal data, it will be referred as mass data collection. Several countries carry out this practice for various purposes. One of the objectives of mass data collection that is carried out both for citizens and non-citizens is aimed at preventing acts of terrorism (Taylor, 2017). Public and private legal entities carry out mass data collection in various sectors: the banking sector, government sector, and health sector that includes insurance, clinical data, and medical records. This collection method can be done traditionally or with modern methods, namely uploading data to large data stores. In the context of document modernisation and data storage, digitisation of data, which was previously in its physical form such as documents on paper, has now shifted to a cloud system where this mechanism centralises massive data into big data to be retrieved at any time by prioritising time and storage efficiency. This method is considered

better because it does not take up space such as physical storage on paper documents. This modern method based on big data also comes with risks: efficiency of space and ease of access that potentially permit high risks of leakage at the click of a button, and anonymity of users. Special attention to data security in cloud systems is one of the bases of research (Munn et al., 2019), which uses the term "privacy by design", whereby among the approaches or methods offered is to encrypt data with a certain password before uploading it to prevent the data from being read by unauthorised parties. Furthermore, the concept of interdependency of data protection also arises. This article argued that reflecting on the concept of interdependency (Kamleitner & Mitchell, 2019) in data protection is important to show that interdependency of privacy, personal data, and mass data collection are connected to one another, not something that stands alone. This is due to technological advances that have enlarged the scope of interdependency between parties. On the accessibility and protection of data, only two parties are involved, the data processor and data controller. This concept of interdependency, when viewed through interdependency in data protection, will be considered a simplification of complex problems. Interdependency in data protection recognises three parties: the owner of the data as the first party, the recipient or the party who can legally access the data as the second party, and the third party as the one who gets access from the second party. All parties related to data access are considered to have the potential to misuse the data. One such violation is the provision of data access to other parties without consent of the data owner. Kamleitner and Mitchell (2019) debated that the inadequacy of data control is seen from two aspects; first, the patients are consciously aware of the risks they will face in the future, but those risks are ruled out when it comes to their health. Second, medical data misuse has been happening for a long time on such a large scale that it is considered a common thing (Figg & Kam, 2011). As such, the privacy and personal data protection of medical records are loosely protected due to the imminent nature of the treatment needed by the patients. It is not unusual, or simply put, it is a "common thing" for the data to be misused.

The advancement of big data in the digital era also reflects the growth of electronic medical data and their flows without boundaries. The sensitive medical data of patients are stored digitally and are accessible from any parts of the world. However, the advancement also has its drawbacks. The vulnerability of software, human errors,

or securities issues, among others, cause leakages of medical data to unauthorised parties. It is reported that from 2005 to 2019, there are 249.09 individuals affected by healthcare data breaches. In 2019 alone, 41.2 million of healthcare records were either exposed, stolen, or illegally disclosed. The breach of healthcare medical records in 2019 as reported by IBM, cost the industry USD6.45million. It is also revealed that healthcare medical record breaches constitute the highest number of breaches as compared to other industries (Seh et al., 2020).

Meanwhile, it is agreed that quick access to medical records could save lives. The quick flow of patients' medical data between healthcare providers is imminent to provide the best medical services to the patients. Nevertheless, the issue also concerns the possibility of the personal medical data of patients that are transferred that may be leaked to third parties or misused by the data controller (i.e., the healthcare provider). The leak may be due to many circumstances like the fault of the healthcare providers or their employees, who do not prepare adequate IT infrastructure to deal with online data, or the act of cybercrimes. Therefore, relevant law or regulation should be in place, not to obstruct the cross-border of medical data, but to make sure that the data is handled accordingly to protect the medical data of patients.

Cross-border Data Transfer and the Law

Medical records that contain personal data are used to improve the quality of medical services. The process of recording medical records starts from the inpatient registration desk, outpatient registration desk, or emergency room. Every action taken by a medical officer, both nurses and doctors, is required to be recorded in the medical record. Changes in medical record documents into electronic medical records have an implication on the storage method, and the same can be said for data that are transferred into a cloud-based data storage. The digital or electronic data storage of medical records make the transfer of data from one jurisdiction to another to become instantaneous, immediate, and at ease.

Data transfer is the transfer of data from one place to another either within the same or different jurisdictions as stated in the European Union General Data Protection Regulation 2018 (GDPR). In other

words, data transfer is the transfer of medical data carried out through two different jurisdictions, i.e., Indonesia and Malaysia. The ease of transferring medical record data brings advantages and disadvantages. The advantages are efficiency of time and storage, as well as the accessibility of data from anywhere in the world. However, the disadvantages are that the data are centralised in digital form, easily accessible by unauthorised parties (Seh et al., 2020), thus increasing the risk of data leakage and data misuse by the data processor or data controller, which ultimately leads to the interference with a person's right to privacy and protection of personal data.

In Indonesia, data protection of medical records is regulated in several separate regulations: Ministerial Regulations, laws, and other regulations scattered in the medical record code of ethics for health service providers. Laws regulating the protection of medical record data are Law Number 29 of 2004 concerning Medical Practice (*Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran*), Regulation of the Minister of Health Number 36 of 2012 concerning Medical Confidentiality (*Peraturan Menteri Kesehatan Nomor 36 Tahun 2012 tentang Rahasia Kedokteran*), and Regulation of the Minister of Health Number 269 of 2008 concerning Medical Records (*Peraturan Menteri Kesehatan Nomor 269 Tahun 2008 tentang Rekam Medis*). These three laws and regulations do not expressly protect the transfer or cross-border of medical records or data. For instance, Article 2 of the Regulation of Health Minister Number 36 of 2012 and Chapter IV, Article 10 of the Regulation of the Minister of Health Number 269 of 2008 only provide for the responsibility of medical practitioners to keep patients' medical records as confidential. The laws on medical records in Indonesia do not categorically cover the transfer of medical record data, retention rights, overcoming data leakage, and the authorised parties handling the data, namely the data controller and data processor. As provided under the GDPR, the data controller should have the authority to determine the purpose of data use and how to process the data, while the data processor working under the name of the data controller only has the authority to process data, who usually outsource the work.

In sum, the legal framework on personal data protection or privacy law in Indonesia is very limited. These inadequacies are also in relation to the protection of personal data of patients' medical records. Greenleaf (2014) highlighted that the substantial part of data

protection laws in Indonesia only covers e-commerce transactions. However, it is reported that Indonesia is in the process to replace, but not yet enacted, the "useless" and limited laws on data protection, by having elements of complying the GDPR in the new laws (Greenleaf, 2019, p. 17). At the time when this article is written, the Personal Data Protection (PDP) Bill of Indonesia, aimed to be introduced in 2020, was delayed due to the Covid-19 pandemic, and yet to be approved by the President (Wijaya, 2022). It is uncertain when this PDP Bill will be approved and enforced in Indonesia.

In Malaysia, the general and supreme law that protects the fundamental rights of the citizens is the Federal Constitution of Malaysia, while the protection of personal data is governed by the enactment of the Personal Data Protection Act 2010 (PDPA). The Federal Constitution of Malaysia only protects the "privacy-related" rights but do not include privacy as fundamental rights explicitly (Yusoff, 2011). The introduction of PDPA and the PDPA Code of Practice show Malaysia's commitment to adhere to the core principles of data protection, namely the personal data are processed fairly, lawfully, and transparent; limited to a particular purpose; and always accurate (World Health Organisation, 2021). Besides, Malaysia as the member of ASEAN adopted the ASEAN Framework on Personal Data Protection in November 2016 to regulate and promote the protection of personal data within the country and the region (Gan, 2018). In regard to medical records, the governing body of medical practice in Malaysia, the Malaysian Medical Council (MMC) has the rules on confidentiality and protection of a patient's data. The following subtopics discuss the PDPA and MMC's guideline and cases, which are related to the protection of patients' personal data or medical records and cross-border transfer of data.

Law on Personal Data in Malaysia

The Malaysian Personal Data Protection Act 2010 (PDPA) was enforced on 15 November 2013, regulating the processing of personal data in commercial transactions. Briefly, the relevant personal data in the context of this article are the medical records of patients. The medical records of patients are classified as "sensitive personal data" as defined under Section 4 of the PDPA, stating that "any personal data consisting of information as to the physical or mental health or condition of a data subject". Due to the classification of personal

data on health condition as sensitive data, the data user is subjected to comply with the requirement of Section 40 of the PDPA when processing the data. Section 40 of the PDPA sets the conditions that any processing of sensitive data of patients must get explicit consent by the data subject/patient. Furthermore, Section 40 allows the processing of personal sensitive data if it is necessary for medical purposes, but it must be performed by healthcare professionals or the staff of healthcare professionals, and whoever owes a duty of confidentiality under the law (Section 40(1)(a) & (b)(iv) of PDPA 2010). In the case of *Oh See Wei v Teddric Jon Mohr & Anor* [2017] 11 MLJ 67, the High Court ruled that,

> "The right to privacy is a multi-dimensional concept. In this modern society, right to privacy has been recognised both in the eye of law and in common parlance. The right to privacy refers to the specific right of an individual to control the collection, use, and disclosure of personal information. Personal information could be in the form of personal interests, habits and activities, family records, education records, communication (including mail and telephone) records, medical records, to name a few. An individual could easily be harmed by the existence of computerised data about him/her which is inaccurate or misleading and which could be transferred for an unauthorised third party at high speed at very little cost. Innovative technologies make personal data easily accessible and communicable and there is inherent conflict between right to privacy and data protection."

With regard to the cross-border or transfer of data abroad, Section 3(2) of the PDPA states that the PDPA does not apply to any data processed outside Malaysia. However, before any outbound personal data including sensitive personal data are transferred, certain legal requirements must be fulfilled as provided under Section 129 of the PDPA. Without the explicit consent from the patient (the data subject), it is a legal requirement for any cross-border of personal data to the place outside Malaysia's jurisdiction, that the place must have similar laws or regulations that serve the same purpose as PDPA, or that the protection given to the personal data transferred to the outside jurisdiction provides adequate protection similar to the protection in Malaysia. It is for the Commissioner to determine whether the outside

jurisdiction has the legal personal data protection in place, similar or better than the protection given in Malaysia (Section 48(e), PDPA 2010), and the outside jurisdiction to be gazetted as "whitelisted" countries. As such, when an Indonesian medical tourist who has been receiving treatment in Malaysia wants to continue the treatment in Indonesia, the data user (i.e., the hospital) has to make sure that the requirement under Section 129 of the PDPA is fulfilled before transferring the data to their counterpart in Indonesia. Any breach of this provision, upon conviction, is subject to a fine not exceeding RM3,000 or to imprisonment for a term not exceeding two years or to both. However, it is found that Malaysia has never gazetted any country outside its jurisdiction as "whitelisted countries" for the purpose of Section 129 of the PDPA. There are suggestions for the requirement of "whitelisted countries" to replace with "blacklisted countries", i.e., the countries that are gazetted as blacklisted countries are considered as unsafe for cross-border data transfer (Pillai et al., 2022).

The question is, does Indonesia have the same protection to sensitive personal data, in this context, the patients' medical records, as in Malaysia? As mentioned above, Indonesia does not have a comprehensive personal data protection law yet.

The Codes and Guidelines of the Malaysian Medical Council

The Malaysian Medical Council (MMC) is the governing body established under the Medical Act 1971 to regulate the registration and the practice of medical practitioners in Malaysia. The MMC has issued several codes of conduct and guidelines regarding the protection of personal data of the patient, which is the guideline on confidentiality, namely the Confidentiality 2011 (hereinafter referred to as the Guideline), and is an extension of MMC's Code of Professional Conduct. In other words, the Guideline is part of the Code of Professional Conduct. Therefore, even though it is a "guideline", any breach or incompliance against the Guideline may result in disciplinary action taken against the medical practitioners. For instance, in the 2019 case of Dr. Isaac Siow Hee Chieh (Malaysian Medical Council, 2020), who was charged with conduct derogatory to the reputation of the profession whereby he had improperly disclosed the identity of his patient's confidential information by posting the patient's photographs on Facebook without the patient's consent. He

also posted the patient's photograph on Facebook, which was edited to give the appearance of a better outcome of the treatment than in reality. He was found guilty and had been suspended from medical practice for two years.

It is commendable that the Confidentiality 2011, i.e., the Guideline, outlines comprehensive provisions on the protection of information including physical or electronic medical records of the patients. It also provides circumstances in which disclosure of patients' information is allowed. However, there are few issues on the application of this Guideline regarding medical tourism.

Firstly, in regard to medical tourism, there is no clear definition of "patient", whether it includes the medical tourist or foreign patient in the Confidentiality 2011 guideline. Consequently, the question is whether the foreign patients, i.e., medical tourist data, foreign personal data, or medical records are also protected under the Guideline. It is argued that the data or medical records of the patients of medical tourism are always protected, the same as the protection given to Malaysian patients. The same protection of patients' data, either Malaysians or medical tourists, is protected because the term used in the guideline is "patient' without specifying or differentiating between Malaysian of foreign patients. Referring to Article 1 of the Guideline, it states that the "patients have the right to expect that there will be no disclosure of any personal information, which is obtained during the course of a practitioner's professional duties, unless they give consent". Therefore, a patient is a patient notwithstanding whether they are local or foreign. However, for the purpose of clarity, it is suggested that the definition of patient under the Guideline to be amended so as to include foreign patients.

Secondly, the issue is that there is no specific provision on cross-border or transfer of personal data outside Malaysia in the Guideline. Once again, due to the lack of implicit provision on this matter, the question is whether the Guideline allows outbound cross-border of patients' data. Referring to Part IV of the Guideline on "sharing information within the healthcare team or with others providing care", Article 22 allows the sharing of information of the patient between healthcare team members on the "need-to-know basis" to provide the best possible care to the patient. The exchange of information is allowed even to a third party outside the healthcare profession. Articles 23 to 27

of the Guideline continue to use the term "sharing between healthcare team members", "transferred between healthcare providers", and "other team members understand and observe confidentiality". Based on the articles under Part IV of the Guideline, the authors submitted that, the Guideline does not cover the outbound transfer of personal data or medical records of patients abroad. This is due to the wording of article 27 under Part IV which states that "Anyone receiving personal information in order to provide or support care is bound by a legal duty of confidence, whether or not they have contractual or professional obligations to protect confidentiality". This provision can only be enforced on the Malaysian healthcare team, Malaysian healthcare providers, or Malaysian "third parties". The preamble of the Guideline also states that this Guideline is an extension of MMC's Code of Professional Conduct, whereby it is imposed and applied to medical practitioners who are practising in Malaysia.

Thirdly, the issue is about who owns the medical records of the patients containing 'sensitive personal data' under the PDPA. The MMC Guideline 002/2006 provides that a "...patient's medical record is the property of the medical practitioner and the healthcare facility and services, who hold all rights associated with ownership". Similarly, Private Healthcare Facilities and Services (Private Medical Clinics or Private Dental Clinics) Regulations 2006, under Regulation 30 (1) provides that, "A patient's medical record is the property of a private medical clinic or private dental clinic". Due to this issue of ownership of patients' medical records, the problem arises especially when there is a civil claim against the healthcare provider, where the patient (the claimant) has to apply to court to gain access to their medical records. In the case of *Nurul Husna Muhammad Hafiz & Anor v Kerajaan Malaysia & Ors*. [2015] 1 CLJ 825, the High Court judge laid down a new principle in obtaining the medical records as such,

> "Based on the legal duties and rights that arise from the physician-patient fiducial relationship, and further having regard to the provisions in the guideline and the common law principles, the legal position in Malaysia vis-à-vis the patient's right of access to medical records can be summarised as follows:
>
> a. The ownership of a patient's medical record vests with the physician or hospital as the case may be. However, the physician or hospital must deal with the medical records in the best interest of the patient;

b. The patient has an innominate and qualified right of access to his medical records and there is a corresponding general duty on the part of the physician or hospital to disclose the patient's medical records to the patient, his agents, medical advisers, or legal advisers;"

Could the healthcare service providers in Malaysia be reluctant or refuse to disclose the medical records of the medical tourists or foreign patients, involving the patients' sensitive personal data, to be transferred outside Malaysia when requested by the patient, fearing civil action taken against them, i.e., the healthcare service provider? Perhaps data subjects must be given more control over personal data that are processed automatically and be granted the "right to portability" and "right to erasure" as provided under Articles 17 and 18 of the GDPR. The answer to this is yet to be seen.

DISCUSSION AND CONCLUSION

In conclusion, there are few main findings that have been highlighted on the protection of cross-border personal data amidst the growth of medical tourism between Indonesia and Malaysia. Firstly, it is highlighted that the legal framework in Indonesia on personal data protection, in particular the transborder of patients' data, is inadequate. It is unknown when the Personal Data Protection Act will be introduced in Indonesia. While for Malaysia, the protection is already emplaced by the enactment and enforcement of PDPA and related regulations. Consequently, the inflow of personal data including medical data of medical tourists from Indonesia to Malaysia is a non-issue since the data are adequately protected by the Malaysian law. However, the outflow of the said data of medical tourists are hindered to be transferred cross-border (to Indonesia) due to inadequacy of the protection. The inadequacy of Indonesian law on this matter hinders Indonesian medical tourists to obtain their follow-up treatment in Indonesia after getting their treatment abroad. The only way for the outflow transfer of the patients' data is by explicit consent given by the patients themselves.

Secondly, the Malaysia's PDPA 2010 never gazetted any countries as "whitelist" as provided under Section 48(e) and 129 of the Act. It is proposed that the "whitelist" approach to be replaced with the

"blacklist" approach. However, the amendment to this effect is yet to be tabled in the Parliament. Consequently, Malaysia needs to improve certain areas of protection, especially on the minor ambiguity of the MMC's Codes and the Guideline involving transfer of data abroad. Even though the cross-border of personal data is clearly stipulated under the PDPA, the MMC's Codes and Guidelines are suggested to insert provisions on transborder of personal data flow, in harmony with the PDPA. Moreover, the issue of "ownership" of patients' medical records as highlighted in the case of *Nurul Husna Muhammad Hafiz & Anor* should be resolved by amending the MMC Guideline 002/2006 and Regulation 30(1) of the Private Healthcare Facilities and Services (Private Medical Clinics or Private Dental Clinics) Regulations 2006. The amendment on this matter is important to illuminate the question of ownership of medical data/records of the medical tourists or foreign patients.

Medical tourism and personal data protection are interrelated. To boost medical tourism industry, the law on data protection needs to be emplaced to facilitate the growth of the industry. Indonesia and Malaysia must have a comprehensive legal framework on personal and medical data protection. At the regional level among ASEAN members, the ASEAN Framework on Personal Data Protection was adopted in 2016 while the ASEAN Data Management Framework was endorsed by the 1st ASEAN Digital Senior Officials' Meeting in January 2021. The ASEAN Framework on Personal Data Protection and the Data Management Framework acknowledge the importance of the members of ASEAN to remove unnecessary legal restrictions on cross border data flows within ASEAN (Association of Southeast Asian Nations, 2021), yet the laws should be comprehensive to protect the data. Only three out of ten ASEAN countries have enacted comprehensive data protection legislation, namely Malaysia, Singapore, and the Philippines. According to a report, there is yet a complete law or only piecemeal legislation on data protection available in Cambodia, Indonesia, Brunei Darussalam, Lao PDR, Vietnam, Myanmar, and Thailand (Gan, 2018). As for the three countries that already have the laws, there is always room for improvement. Minor issues on data protection in the three countries should be addressed, and lesson learnt for the members that are yet to enact or amend their laws. For example, the Commissioner under the Singapore Personal Data Protection Act is not independent, and the appointment of the Commissioner may be revoked at any time without having to give any

reasons (Greenleaf, 2014). The non-independent and revocation of appointment without any reason may disrupt the Commissioner from exercising his power "without fear or favour". Similarly, Malaysia and Singapore's PDPA do not cover the public sector (Yusoff, 2011) and thus, the protection is only "partial protection" as the Acts do not cover the public sector. Besides, the awareness among private companies in Malaysia on data protection is said to be lacking (Greenleaf, 2014). The non-uniformity of the laws on data protection among ASEAN members should be resolved, at least to the extent that every member provides the same level of protection of data or "commonalities" to a regulatory approach (Casalini et al., 2021), and in the context of this article, to the cross-border of personal data of medical tourists. This study may be enhanced in future, by focusing on ASEAN initiatives and framework on cross-border medical data protection. Besides, the universal data protection may be introduced in the future as propounded by Schneble et al. (2020), and for future research within the ASEAN context.

ACKNOWLEDGMENT

This work is funded by the Fakultas Hukum, Universitas Brawijaya, Republic of Indonesia through a grant of Dana Program Penelitian Joint Research Tahun 2021 (3/JR/FHUB/PEN/2021, 2021) and also registered under Legal and Justice Research Centre, School of Law, Universiti Utara Malaysia (SO Code 444309).

REFERENCES

Abd Mutalib, N. S., Soh, Y. C., Wong, T. W., Yee, S. M., Yang, Q., Murugiah, M. K., & Ming, L. C. (2017). Online narratives about medical tourism in Malaysia and Thailand: A qualitative content analysis. *Journal of Travel & Tourism Marketing*, *34*(6), 821–832.

Al-Awqati, Q. (2006). How to write a case report: Lessons from 1600 BC. *Kidney International*, *69*(12), 2113–2114.

Association of Southeast Asian Nations. (2021). *ASEAN data management framework*. https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf.

Ayub, Z. A., & Yusoff, Z. M. (2007). Leave me alone! Syariah v civil law. *Malayan Law Journal*, *6*, xcix.

Ayub, Z. A., & Yusoff, Z. M. (2015). Search and seizure of digital evidence and privacy issues in Malaysia. *Current Law Journal*, 1 LNS(A), lviii.

Azmi, N. M., Hamzah, I. S., & Hussin, N. I. (2021). The implications of securitising health crises: The case of Southeast Asia. *Journal of International Studies*, *17*, 53–79.

Badan Pusat Statistik. (2015). Pertumbuhan ekonomi Indonesia tahun 2014. *Berita Resmi Statistik*. https://www.bps.go.id/pressrelease/2015/02/05/1114/pertumbuhan-ekonomi-indonesia-tahun-2014-tumbuh-5-02-persen--melambat-sejak-lima-tahun-terakhir.html.

Badan Pusat Statistik. (2020). *Produk domestik Bruto Indonesia Triwulanan 2016-2020*. Badan Pusat Statistik. https://www.bps.go.id/publication/2020/10/16/54be7f82b7d3aa22f5e2c144/pdb-indonesia-triwulanan-2016-2020.html.

Bali, A., Bali, D., Iyer, N., & Iyer, M. (2011). Management of medical records: Facts and figures for surgeons. *Journal of Maxillofacial and Oral Surgery*, *10*(3), 199–202.

Casalini, F., González, J. L., & Nemoto, T. (2021). *Mapping commonalities in regulatory approaches to cross-border data transfers*. OECD Trade Policy Papers No. 248. https://doi.org/10.1787/ca9f974e-en.

Cheng, T. O. (2001). Hippocrates and cardiology. *American Heart Journal*, *141*(2), 173–183.

Dobinson, I., & Johns, F. (2017). Legal research as qualitative research. In McConville, M., & Chui, W.H. (Eds.), *Research methods for law* (2nd ed., pp.18–47). Edinburg University Press.

Douglas, N., Douglas, N., & Derrett, R. (2001). *Special interest tourism*. John Wiley and Sons Australia Ltd.

Eissler, L. A., & Casken, J. (2013). Seeking health care through international medical tourism. *Journal of Nursing Scholarship*, *45*(2), 177–184.

Figg, W. C., & Kam, H. J. (2011). Medical information security. *International Journal of Security*, *5*(1), 22.

Gan, T. T. (2018). *Data and privacy protection in ASEAN – What does it mean for businesses in the region?* Deloitte. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf.

Grammaticos P. C., Diamantis A. (2008). Useful known and unknown views of the father of modern medicine, Hippocrates and his teacher Democritus. *Hellenic Journal of Nuclear Medicine*, *11*(1), 2–4.

Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade & human rights perspectives*. Oxford University Press.

Greenleaf, G. (2019). Global Data Privacy Laws 2019: 132 National Laws & Many Bills. 157 *Privacy Laws & Business International Report*, 14–18.

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review*, *17*(1), 83. https://doi.org/10.21153/dlr2012vol17no1art70

Information Commissioner's Office. (2022). *Personal data breaches*. Information Commissioner's Office. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Kamleitner, B., & Mitchell, V. (2019). Your data is my data: A framework for addressing interdependent privacy infringements. *Journal of Public Policy & Marketing*, *38*(4), 433–450.

Kassim, P. N. J. (2009). Cross-border issues in the development of medical tourism in Malaysia: Legal challenges and opportunities. *Journal of Law and Medicine*, *17*(1), 59–73.

Malaysia Health Care Travel Council. (2019). *Inaugural Malaysia Healthcare Expo 2019 in Jakarta aims to attract 15,000 visitors*. https://www.mhtc.org.my/2019/02/14/inaugural-malaysia-healthcare-expo-2019-in-jakarta-aims-to-attract-15000-visitors/.

Malaysian Medical Council. (2020). *Disciplinary punishment 2020*. https://mmc.gov.my/wp-content/uploads/2022/02/DISCIPLINARY-PUNISHMENT-2020.pdf.

Mohd Azmi, N., Hamzah, I. S., & Hussin, N. I. (2021). The implications of securitising health crises: The case of Southeast Asia. *Journal of International Studies*, *17*, 53–79. https://doi.org/10.32890/jis2021.17.3

Mohd, E., Ayub, Z. A., & Mohd Anuar, H. (2018). Regulatory barriers in collecting assessment rates arrears of local authorities in Malaysia. *The Journal of Social Sciences Research*, *6*(1), 1049–1055.

Moskop, J. C., Marco, C. A., Larkin, G. L., Geiderman, J. M., & Derse, A. R. (2005). From Hippocrates to HIPAA: Privacy and confidentiality in emergency medicine--Part I: Conceptual, moral, and legal foundations. *Annals of Emergency Medicine*, *45*(1), 53–59. https://doi.org/10.1016/j.annemergmed.2004.08.008

Munn, L., Hristova, T., & Magee, L. (2019). Clouded data: Privacy and the promise of encryption. *Big Data & Society*, *6*(1), 1-16. https://doi.org/10.1177/2053951719848781

Numbeo. (2021). *Health care index by country*. Numbeo. https://www.numbeo.com/health-care/rankings_by_country.jsp?title=2021.

Ormond, M., Mun, W. K., & Khoon, C. C. (2014). Medical tourism in Malaysia: How can we better identify and manage its advantages and disadvantages? *Global Health Action*, *7*(1), 25201.

Patients Beyond Borders. (2020, January 21). Patients beyond borders announces top 10 cities for medical tourists in 2020. *News Wise*. https://www.newswise.com/articles/patients-beyond-borders-announces-top-10-best-cities-for-medical-tourists-in-2020. Accessed March 9, 2022.

Pickert, K. (2008, November 25). A brief history of medical tourism. *TIME*. http://content.time.com/time/health/article/0,8599,1861919,00.html.

Pillai, D., Zulkifli, I. H., Anis, A. M., & Han, Y. S. (2022). *Proposed amendments to the Personal Data Protection Act 2010 (PDPA): Latest updates*. Rajah & Tann Asia. https://www.rajahtannasia.com/media/4724/220211_client_update_on_the_pdpa.pdf

Salter, M., & Mason, J. (2007). *Writing law dissertations: An introduction and guide to the conduct of legal research*. Pearson Education Ltd.

Schneble C. O., Elger B. S., & Shaw D. M. (2020). All our data will be health data one day: The need for universal data protection and comprehensive consent. *Journal of Medical Internet Research*, *22*(5), e16879. https://doi.org/: 10.2196/16879

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare (Basel, Switzerland)*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

Smith, R., Álvarez, M. M., & Chanda, R. (2011). Medical tourism: A review of the literature and analysis of a role for bi-lateral trade. *Health Policy*, *103*(2-3), 276–282.

Statista. (2020). *Consumer Price Index (CPI) of health care in Singapore 1990-2020*. Statista. https://www.statista.com/statistics/932798/singapore-cpi-health-care/.

Taylor, I. (2017). Data collection, counterterrorism and the right to privacy. *Politics, Philosophy & Economics*, *16*(3), 326–346. https://doi.org/10.1177/1470594X17715249

Warren, S. D., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*, 193–220.

Wijaya, G. (February 10, 2022). Global legislative predictions 2022: Indonesia's Personal Data Protection Bill. *International Association of Privacy Professionals (IAPP) Privacy Tracker*. https://iapp.org/news/a/global-legislative-predictions-2022-indonesias-personal-data-protection-bill/

Woogara, J. (2001). Human rights and patients' privacy in UK hospitals. *Nursing Ethics*, *8*(3), 234–246. https://doi.org/10.1177/096973300100800308

World Health Organization. (2021). *The protection of personal data in health information systems-principles and processes for public health* (No. WHO/EURO: 2021-1994-41749-57154). World Health Organization. Regional Office for Europe.

Yusoff, Z. M. (2011). The Malaysian Personal Data Protection Act 2010: A legislation note. *New Zealand Journal of Public and International Law*, *9*, 119.

Yusoff, Z. M., & Ayub, Z. A. (2019). Privasi di tempat kerja: Tinjauan sudut perundangan di Malaysia [Workplace privacy: The legal point of view in Malaysia]. *Kanun: Jurnal Undang-undang Malaysia*, *31*(1), 55–84.