Akademika 95(1), 2025: 391-408
https://doi.org/10.17576/akad-2025-9501-22

To Share or Not to Share Patient Health Data Without Consent for Public Interest Purposes: A Critical Comparative Analysis of EU GDPR 2018 and Malaysia PDPA 2010

Berkongsi atau Tidak Berkongsi Data Kesihatan Pesakit Tanpa Keizinan untuk Tujuan Kepentingan Umum: Analisis Perbandingan Kritis antara EU GDPR 2018 dan PDPA Malaysia 2010

SITI FARAHIYAH AB RAHIM* & MUHAMAD FIRDAUS AB RAHMAN

Received: 7 November 2024 /Accepted: 27 March 2025

ABSTRACT

This paper aims to validate the use and sharing of patient health data for medical research without consent when it serves the public interest and is safeguarded appropriately. With healthcare increasingly driven by data, access to patient datasets allows researchers to identify trends, develop more effective treatments, and inform policy, thereby benefiting public health. However, ethical and legal legislation, particularly data protection laws, are perceived by some researchers as impediments to research advancement. This paper propounds how data protection law can be best structured to balance privacy protection with the needs of research. A qualitative and comparative methodology are employed to evaluate the effectiveness of two legal frameworks—the EU General Data Protection Regulation (GDPR) 2018 and Malaysia's Personal Data Protection Act (PDPA) 2010—in balancing privacy with research needs. Findings indicate significant limitations in Malaysia's PDPA, including its narrow scope (which excludes the public healthcare sector) and the absence of research-specific provisions, potentially reducing its effectiveness in protecting privacy while accommodating research. The paper recommends that Malaysia's PDPA adopt a framework similar to the GDPR to address these gaps. Key recommendations include extending the PDPA coverage to public healthcare data, establishing 'public interest' lawful basis for research use and implementing safeguards like data minimisation and Data Protection Impact Assessments (DPIAs). Aligning the PDPA more closely with international standards could foster public trust in data practices, support Malaysia's research infrastructure and promote the responsible and safe use of health data in scientific research.

Keywords: patient health data, privacy, medical research, Malaysia's Personal Data Protection Act (PDPA) 2010, EU General Data Protection Regulation (GDPR) 2018

ABSTRAK

Kajian ini bertujuan untuk mengesahkan keabsahan penggunaan dan perkongsian data kesihatan pesakit bagi tujuan penyelidikan perubatan tanpa keizinan apabila ia memenuhi kepentingan umum serta dilindungi dengan langkah-langkah keselamatan yang sewajarnya. Dalam era penjagaan kesihatan yang semakin berteraskan data, akses kepada set data pesakit membolehkan penyelidik mengenal pasti corak penyakit, membangunkan rawatan yang lebih berkesan, serta mempengaruhi dasar kesihatan untuk manfaat kesihatan awam. Namun demikian, undang-undang perlindungan data, sering dianggap oleh sebahagian penyelidik sebagai halangan kepada kemajuan penyelidikan. Justeru, kajian ini mengemukakan bagaimana undang-undang perlindungan data boleh distrukturkan dengan lebih baik bagi mengimbangi perlindungan privasi dengan keperluan penyelidikan. Kajian ini menggunakan pendekatan kualitatif dan perbandingan bagi menilai keberkesanan dua rangka kerja perundangan—Peraturan Perlindungan Data Umum Kesatuan Eropah (GDPR) 2018 dan Akta Perlindungan Data Peribadi Malaysia (PDPA) 2010—dalam mengimbangi perlindungan privasi dan keperluan penyelidikan. Hasil kajian menunjukkan terdapat kelemahan ketara dalam PDPA Malaysia, antaranya skop perlindungan yang terhad (tidak meliputi sektor penjagaan kesihatan awam) serta ketiadaan peruntukan khusus bagi penyelidikan, yang boleh menjejaskan keberkesanannya dalam melindungi privasi sambil menyokong penyelidikan perubatan. Kajian ini mencadangkan agar PDPA Malaysia diperluaskan dan diselaraskan dengan GDPR bagi mengatasi kelemahan ini. Antara cadangan utama ialah

memperluaskan skop PDPA kepada data kesihatan sektor awam, mewujudkan peruntukan berteraskan 'kepentingan awam' bagi penggunaan data dalam penyelidikan, serta melaksanakan langkah perlindungan seperti peminimuman data dan Penilaian Kesan Perlindungan Data (DPIA). Penyelarasan PDPA dengan piawaian antarabangsa dapat meningkatkan kepercayaan masyarakat terhadap pengurusan data, menyokong pembangunan penyelidikan di Malaysia, serta memastikan penggunaan data kesihatan dalam penyelidikan dilaksanakan secara bertanggungjawab dan selamat.

Kata kunci: data kesihatan pesakit, privasi, penyelidikan perubatan, Akta Perlindungan Data Peribadi Malaysia (PDPA) 2010, Peraturan Perlindungan Data Umum Kesatuan Eropah (GDPR) 2018

INTRODUCTION

Healthcare is increasingly data driven. A high volume of research conducted today reviews patient data rather than experimenting with human subjects (Quinn 2021; Cate 2010). Research focuses on health data allows review of patient's actual experience with treatments and drug therapies to detect any adverse drug reactions, to understand better how medicine operates and to develop new treatment. This growing use of research-based health data was found to have many advantages (Mohamed, 2013). In contrast with experimental studies that are costly and may require a longer time, research using health data is often faster and less expensive and able to analyse enormous sets of data as more data about medical experience becomes available in computerised analysis (Juntao 2024; Stauch 2013). More importantly, in contrast with traditional 'interventional research', it does not directly expose the patient to the risk of physical harm.

With the emergence of big data, patient health data holds immense potential for advancing scientific research and improving public health outcomes (Manap et al. 2024). Access to comprehensive health datasets enables researchers to identify health trends, develop treatments, and inform policy decisions (Batko & Slezak 2022; Quinn 2021). However, sharing health data for research introduces significant legal and ethical challenges particularly around privacy, data protection and public trust (Taylor et al. 2021; Mourby et al. 2019; Laurie et al. 2015). Data Protection Law (DPL) aims to safeguard individuals' personal data from unauthorised access, use and sharing, thereby safeguarding their right to privacy. To achieve this, DPL establishes a set of principles governing the use of personal data and grants individuals' specific rights regarding their personal information, which organisations that collect and use such data are required to uphold. Compliance with DPL is critical to ensure that the use of patient data is legally justified (Mondschein et al. 2019). However, researchers have expressed that the stringent requirements imposed by the DPL may hamper high-quality research, posing major barriers to making patient data available for various research purposes (Staunton 2019; Dove 2018; Chassang 2017; El Emam et al., 2015; Crook 2013). Therefore, this paper questions how data protection law can be best designed to achieve the dual aims of accommodating research activities while protecting patients' privacy interests? Reconciling these two aims is essential to ensure that the benefits of medical research for the public good are realised while minimising risks to patient privacy. To this end, the paper argues that the use of patient health data without consent for research purposes in the public interest can be ethically and legally justified, provided it complies with the data protection law, adheres to research governance and includes appropriate safeguards. This article does not have the space to extensively discuss the ethical and research governance frameworks governing the use of health data for research, as these will be addressed elsewhere.

Obtaining consent presents significant challenges for large-scale research, as will be discussed further. To address this, the European Union's General Data Protection Regulation (GDPR) provides a flexible model for balancing research needs with privacy protection by allowing health data processing without consent under strict safeguards, including data minimisation and pseudonymisation (Dove & Chen 2020; Mostert et al. 2016). The GDPR applies uniformly across both public and private sectors, thus, ensures consistent privacy standards that accommodates research using diverse health data sources.

In contrast, Malaysia's Personal Data Protection Act (PDPA) 2010 primarily applies to the private sector, excluding public healthcare institutions (Section 3 PDPA). This limited scope creates inconsistencies in privacy protection and leaves data processing within the public healthcare sector unprotected under data protection law (Ali & Abu Bakar 2020; Sidi and Sonny 2019). The launch of the Malaysian Health Data Warehouse (MyHDW) in 2017, which collates and streamlines health data from public and private healthcare facilities across Malaysia as a national health data repository may present significant privacy risks (Manap et al. 2024). The situation is particularly concerning as MyHDW links patient information with data from the National Registration Department (NRD), the Department of Statistics, and other relevant bodies. This warehouse functions as a one-stop centre aimed at supporting evidence-based decision-making, enabling data-driven research and improving healthcare management (Ministry of Health Malaysia 2024; HealthCareAsia Daily 2024). However, this lack of uniform protection may undermine public trust in the platform, as patients could be uncertain about the privacy and security of their sensitive health information within a fragmented regulatory framework. Public trust is crucial in research, as it encourages individuals to participate in studies. Without trust, people may be reluctant to share personal information, limiting the scope and quality of research and hindering research progress. When the public trusts that safeguards are in place, including data protection laws regulating the use of personal data, individuals are more willing to allow data use, enhancing the potential impact of research on public health advancements.

The Malaysian PDPA is currently under review for Amendment Bill 2024 to align with international data protection standards and to address new issues emerging from the evolving use of personal data. However, one of the major amendments- the PDPA's applicability to government bodies- did not transpire. It should be noted that regulation on data processing specifically in the public sector is crucial to forge public trust as Malaysia is one way forward towards healthcare-data driven (Department of Personal Data Protection Malaysia 2024; Farah Nabilah 2024)

This paper finds that the Malaysian PDPA has several unique limitations, raising questions about whether the law can effectively achieve the twin aims of facilitating medical research while protecting patient privacy. This paper suggests that the PDPA should have a more comprehensive framework similar to EU GDPR 2018 to close the gaps. The salient findings therefore as follows; the PDPA should extend its applicability to public healthcare sector to ensure consistent privacy standards across all data types and uses, supporting both the protection and the safe use of patient data in medical research. Further, it is recommended that the PDPA incorporate research-friendly provisions similar to those in the GDPR, such as lawful bases for public interest task and mandatory safeguards like DPIAs and data minimisation requirements. This approach could enhance public trust in data handling practices, benefiting Malaysia's research capabilities and aligning its practices with international data protection standards.

METHODOLOGY

The methodology employed in this study is a qualitative (Arif & Markom 2024; Shariff et al., 2018) and comparative legal analysis (Roslan et al., 2019), focusing on the EU General Data Protection Regulation (GDPR) 2018 and Malaysia's Personal Data Protection Act (PDPA) 2010. This approach enables an in-depth examination of both legal frameworks from a doctrinal perspective, assessing their related provisions, interpretations, and practical applications in advancing health data use for research purposes while safeguarding patient privacy (Taylor et al., 2016; Saldana, 2011; Zahir et al., 2019). Barbour et al. (2018) and Marhaban et al. (2022) noted that the qualitative aspect involves a critical analysis of primary legal texts; including relevant provisions from the GDPR and the PDPA, along with legal scholarly interpretations and commentaries. Besides, Neely and Ponshunmugam (2019) claimed that the comparative analysis identifies key similarities and differences between the two frameworks, highlighting areas where the PDPA might align with the GDPR's structured approach to public-interest research. This methodology is suited to assessing the effectiveness of legal principles and privacy safeguards, with findings aimed at addressing potential gaps in Malaysia's PDPA. Suggestions for reform are drawn directly from the comparative insights, offering targeted reforms that uphold privacy while accommodating data-driven research.

RESULTS AND DISCUSSION

JUSTIFYING THE USE AND SHARING OF PATIENT HEALTH DATA FOR MEDICAL RESEARCH IN THE PUBLIC INTEREST

The use and sharing of patient health data can be justified in the public interest when the use is necessary to advance medical research, improve public health and inform health policy. Evaluating whether such data sharing is in the public interest requires careful consideration of the public benefits, patient privacy rights, and the legal and ethical frameworks that govern data protection. The rationale for the use and sharing of patient health data in the public interest is analysed through few key aspects as will be discussed below.

Public health relies on the collection and analysis of data for medical researchers to monitor disease trends, control outbreaks, and implement preventative strategies. Sharing patient health data in this context serves a crucial public interest. Firstly, the sharing of health data is essential for disease control and prevention. For instance, during the COVID-19 pandemic, real-time sharing of patient data between governments, health organizations, and researchers allowed for the effective tracking of the virus, identification of hotspots, and development of public health interventions. Without the ability to share patient data on a global scale, the response to the pandemic would have been slower, leading to higher infection rates and deaths.

Further, sharing patient data is crucial for monitoring health trend. Aggregated health data allows public health authorities to monitor long-term trends, such as the increasing prevalence of chronic diseases like cancer, diabetes or cardiovascular disease. This data enables health authorities to allocate resources more effectively, design preventive health campaigns and identify areas where healthcare services need to be improved. For example, if a rise in obesity is detected in certain areas, targeted interventions such as promoting healthier lifestyles or investing in healthcare services, can be implemented.

Therefore, the benefits of medical research are substantial and crucial for the public good. It is essential for researchers to access, use, and link patient health data to fully realise these potential benefits of research. Using a broad range of patient health data enhances research validity and reliability by enabling comprehensive analysis of health patterns and treatment effectiveness. However, obtaining individual patient consent for each data use in large-scale studies is often impractical, costly, and impacts research viability. To address these challenges, permitting data use without consent for public-interest research, subject to strict safeguards, is essential to achieving the dual aims of facilitating research while minimising privacy risks (Duguet & Herveg 2021; Staunton et al. 2019). The following discussion will justify the use of health data without consent in achieving these twin aims.

THE ROLE OF CONSENT AND ITS PRACTICAL DIFFICULTIES IN LARGE-SCALE MEDICAL RESEARCH

In current privacy and data protection legislation, obtaining patients' (informed) consent is crucial and serve as one of the valid bases for processing personal data, including patient health-related data (Vedder & Spajić 2023; Staunton 2019; *Lee Ewe Poh v Dr Lim Teik Man & Anor, 2011*). The requirement of consent is fundamentally based on the theory of personal autonomy and privacy. In a health context, autonomy refers to a particular form of personal liberty that allows individuals to choose and implement their own decisions without deceit, duress, constraint and coercion (Mann et al. 2016; Puteri Nemie et al. 2014). Beauchamp and Childress propound that 'autonomous decision is those which are made with substantial understanding upon being properly informed (Beauchamp & Childress 1994). Therefore, to make a valid and autonomous choice, sufficient information must be afforded to the patient to enable them to make an informed consent.

Lawrence Gostin emphasises that personal autonomy- the right of individuals to govern themselves- is integral to privacy as it concerns with the idea of sovereignty over oneself (Gostin 2001). This idea is closely interrelated to the ideas of privacy. According to Alan Westin, often referred to as the "father of privacy theory" in his ground-breaking 1967 study on 'Privacy and Freedom', privacy is "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin 1968). Westin definition encapsulates the control patients should have over their information, including when and how it is accessed or shared, which is particularly relevant for health data.

Having said that, informed consent is a cornerstone of patient autonomy, allowing patients to control the use of their health data. Many data protection law enacted since then have followed suit, relying on individual choice and informed consent as the key tool for protecting privacy. Nevertheless, scholars have highlighted the insufficiencies of relying solely on patient consent for privacy protection in medical research, particularly in the context of large datasets and complex data-sharing practices (Taylor & Townend 2022; Dove & Chen 2020; Kasperbauer 2020; Cate 2010). This necessitates a re-evaluation of privacy approaches to better align with modern medical research realities.

The requirement of consent before research-use of health data presents significant difficulties that could limit the value and scope of data-driven studies (Dove & Chen 2020). Although asking consent is in line with ethical standards and ensures patients' control over their data, it is often impractical for research that relies on retrospective or extensive datasets. As the literature demonstrates, fulfilling consent requirements is particularly difficult for research involving vast amounts of health data, where tracking each participant or seeking re-consent for

every new research purpose can be costly, time-consuming and at times, impractical. For instance, developing targeted cancer therapies (e.g., for BRCA1 and BRCA2 mutations) relies on rapid access to genetic data to identify patient responses. The delay in getting consent from potentially thousands of patients can stall critical treatment developments, jeopardising the public health benefits of rapid innovation.

In addition to time, seeking consent for extensive patient datasets is expensive, involving costs for contacting patient participants, preparing necessary-complex information materials and managing records. These resources could be better utilised for further research and treatment development. Lawmakers acknowledge this issue and under the EU GDPR's public interest exemptions, research institutions can avoid costly consent procedures if they fulfil robust safeguards, thereby focusing resources on patient benefit.

Furthermore, many research projects require retrospective data or historical data which can be crucial in understanding long-term treatment effects or health outcomes. For example, research involving retrospective patient data from years ago are often critical in epidemiology and drug development. Contacting patients to obtain consent for the use of this historical data can be infeasible, especially if the data involves deceased patients or spans multiple health institutions.

Consent requirements may also inadvertently limit valuable research by reducing participant recruitment, leading to biased or incomplete datasets. This phenomenon, known as "consent bias," arises when only a specific group of patients agrees to participate in research while others do not. This selective participation can lead to a sample that does not accurately represent the entire population, potentially skewing research findings and weakening the project's validity. For example, a public health study aiming to analyse certain disease trends across populations might struggle to obtain a representative sample if only certain demographics consent to data use. Such biases can impact the validity of research findings and consequently, the medical interventions or policies derived from them, posing a risk to the public interest that these studies aim to serve.

Moreover, a strict reliance on consent can intrude into individuals' privacy, as repeated requests may lead to an unwarranted invasion into personal lives. This requirement for repeated engagement, which may involve notifying individuals each time their data is reused, can strain relationships between researchers and participants, leading to a climate of distrust that may discourage future research participation.

These challenges suggest that consent, while valuable, should not be a primary requirement for data sharing in public-interest health research. Instead, a framework that allows data use without consent, supported by rigorous safeguards like pseudonymisation and data minimisation, could balance privacy protection with research utility (Chico 2018). Furthermore, the integration of legal and ethical compliance, safeguards, alongside public trust on data privacy, is crucial to address the limitations of individual choice for research-use of health data. This multifaceted approach is vital to reconcile between the need for data utility with the imperative of protecting patient privacy.

AIMS OF DATA PROTECTION LAW: ENSURING APPLICABILITY ACROSS ALL SECTORS AND FOR ALL PURPOSES OF DATA PROCESSING

A vast number of individuals' personal data is held and used by various entities across both public and private sectors for numerous purposes. This data ranges from personal data to highly sensitive data, including health data collected by healthcare providers when individuals seek medical care.

Personal data refers to any information that relates to an identifiable individual, either directly or indirectly. This includes a person's name, address, emails, phone number or ID number as well as sensitive information such as data concerning health. Thus, Data Protection Law (DPL) plays a crucial role in safeguarding privacy, as unauthorised access or misuse of such data can lead to privacy breaches and identity theft that could potentially harms the individuals. Therefore, the institutions that processing personal must adhere to the rules specified by the DPL to ensure the individual right to privacy is safeguarded.

As a primary criterion, the DPL of a country should apply to all entities that process personal data, whether in the public or private sector, and to all types of processing, regardless of purpose. Therefore, this analysis aims to examine the objectives and applicability of both the EU GDPR and the PDPA 2010 in safeguarding the interests and rights of individuals concerning the processing of personal data.

The GDPR takes an 'omnibus' approach by having a comprehensive scope, applying to various data processing activities and entities across both the public and private sectors (Quinn 2021; Mondschein et al. 2019; Dove 2018). This broad applicability ensures that health data processed for research is consistently protected, regardless of the data handler's sector. In contrast, Malaysia's legal framework takes a sectoral approach as the Malaysian PDPA only applies to the private sector, excluding public authorities from its scope.

It is worthy of highlighting that the Malaysian healthcare context has a dual system of healthcare delivery in which public and private providers exist side by side and independent of one another (Kartina Aisha 2012). In the public sector, health and medical services are provided by the Ministry of Health (MoH), and policies and major decisions regarding resource allocation are made by the Minister of Health (Official Page Ministry of Health Malaysia). Hospitals in the public sector are run by the MoH and are called 'government hospitals'. These government hospitals are public authorities or data controller for the purposes of data protection law.

The Malaysian PDPA 2010, despite being modelled on international data protection laws, has notable limitations that affects the use of patient data for medical research. Its two primary limitations are its exclusion of public sector and its restriction to commercial transactions, which together significantly narrow its scope (Ali & Abu Bakar 2020; Abu Bakar & Siti Hajar 2010). The first limitation of the PDPA 2010 is that it 'shall not apply to Federal and State Governments' (Section 3 PDPA). According to Malaysia Interpretation Act, the federal government of Malaysia consists of the public authorities who work on public tasks at the federal level, including all ministries and the Prime Minister's department (Section 3 Malaysian Interpretation Acts 1948 and 1967). The term government in the Act could include ministries, universities and government hospitals (Sidi and Sonny 2019; Noriswadi & Cieh 2013).

The second limitation of PDPA 2010 is its applicability to only on commercial transactions. The preamble of the PDPA 2010 explicitly mentions that it is an Act 'to regulate the processing of personal data in commercial transactions and matters relating thereto'. Thus, the PDPA 2010 aims only to protect privacy in the processing of personal data in commercial transactions (Section 2 PDPA). A commercial transaction is defined in the PDPA as 'any transaction of a commercial nature, regardless of whether it is contractual or non-contractual including the supply or exchange of goods or services, agency, investments, finance, banking and insurance' (Section 4 PDPA). 'Commercial' is defined as business, trading or other activities that are profit-oriented (Black's Law Dictionary). Based on this definition, a commercial transaction must have an element of profit-making, or at least involve some form of monetary value. Thus, in effect, only private-sector transactions fall within the ambit of this act (Greenleaf 2012; Zuryati 2011).

The Malaysian PDPA 2010's limitations, namely its non-applicability to the public sector and its restriction to commercial transactions, significantly narrow its scope and create gaps in data protection (Ali & Abu Bakar 2020; Sidi and Sonny 2019). By excluding public healthcare sector such as government hospitals from its regulatory framework, the PDPA leaves a substantial amount of sensitive health data unprotected. This limitation means that government-held health data, which is widely used for research and public health initiatives, is not subject to the same data protection standards that apply to private sector. This would raise privacy concerns and shaken public trust in using their health data for research purposes. Additionally, the PDPA's focus on commercial transactions confines its applicability to profit-oriented activities, further excluding non-commercial uses of data such as medical research conducted by public healthcare sectors.

These combined limitations impede the PDPA's ability to offer comprehensive protection for patient data used in research, especially within public healthcare facilities. Public healthcare sector like the Ministry of Health (MoH) can process and share patient data for research without adhering to the PDPA's principles, as this data falls outside the scope of "commercial" processing. As Malaysia advances digital health initiatives such as the Malaysian Health Data Warehouse (MyHDW) which integrates public and private sector health data, the lack of consistent regulatory standards may erode public trust and compromise patient privacy (MyHDW Official Web; Joseph 2017). Aligning the PDPA framework with broader international standards such as the EU GDPR's universal applicability would better protect health data across sectors and foster a more trusted and secure environment for health research.

The GDPR's comprehensive scope promotes an environment where both privacy and research needs are balanced, with consistent protections across all data types and processing contexts. The GDPR's sector-neutral approach aims to create a unified data protection landscape across the EU, reducing fragmentation and ensuring the same high standards of data protection regardless of the organisational context.

DEROGATION FROM CONSENT AND SCIENTIFIC RESEARCH IN THE PUBLIC INTEREST AS A LAWFUL BASIS FOR HEALTH DATA PROCESSING

Data protection law empowers an organisation to use personal data if they have a legal reason to do so i.e if they have a lawful basis. The law demands that the organisations (the data controllers) specify the lawful basis to process personal data. Such lawful bases are necessary to ensure that only authorised organisations can hold and process personal data (Medical Research Council 2018).

The GDPR requires the data controller to identify the lawful basis before processing. In the GDPR, there are six available lawful bases for processing, which basis is the most suitable to use depends on the purpose of the processing and the relationship between the controller and the individual (UK Information Commissioners Office). They include, among others, that the data subject has given consent, that processing is necessary for performance of a contract, the processing is necessary for a task in the public interest or that processing is necessary for legitimate interests pursued by the data controller (Article 6(1) GDPR). Consent is one option for legitimising the use of health data, but it is not superior to other legal bases for use (Chico 2018). The GDPR defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by a clear affirmative action that signifies agreement to the processing of personal data' (Article 4(1) GDPR). As this requires an affirmative action, consent presumed by failure to opt-out or by changing the option of pre-ticked boxes is not consent for the purposes of the GDPR (Article 4 GDPR). Furthermore, the consent form must contain an attachment providing

information on the intended use of the data and the purpose of processing. However, during negotiations while drafting the GDPR, the scientific research community raised concerns that the strict definition of consent in the provision is somewhat challenging for scientific research, as some research may not be able to determine the purpose of processing at the time of data collection. After prolonged negotiation and lobbying by research communities, the final version of GDPR recognised that it would not be practical to use consent and adopted a more research-friendly position by including an exemption for scientific research (Recital 33 GDPR). This is in line with the earlier discussion above that consent requirements present significant challenges and may hinder data-driven research.

Of these legal bases, the processing is necessary for 'the performance of a task carried out in the public interest' is most likely to be appropriate for public sectors processing personal data without individual consent (Bell et al. 2019). While the term 'public authorities' is not defined in the GDPR, Section 7 of the UK DPA 2018, in accordance with the Freedom of Information Act (FoIA) 2000, defines public authorities as including research organisations such as the National Health Service (NHS), research universities and research councils. These institutions are funded by the public purse to conduct tasks that are in the public interest (Medical Research Council (MRC)). Thus, these public healthcare sectors processes health data for research purposes can use the 'public task' clause as a lawful basis for data processing ((Medical Research Council (MRC)). The lawful basis of the public task is applicable to these organisations, which carry out research based on the official authority vested in them. Further, together with Article 6(1)(e), Article 9(2)(j) of the GDPR permits the processing of sensitive health data without consent if it is necessary for public-interest research, provided appropriate safeguards are in place such as pseudonymisation or data minimisation which will be discussed further in the next discussion. This flexibility facilitates the advancement of medical research while balancing privacy rights.

Private sectors such as commercial entities and charitable research organisation may rely on 'legitimate interest' as the lawful basis for data processing as stipulated in Article 6(1)(f) of the GDPR (Quinn 2021; Dove & Chen 2020). In essence, the applicability and suitability of this lawful basis is determined by the purpose of processing, the true nature of the relationship with the individual and the type of organisation that is conducting the research (Information Commissioner Office (ICO); Medical Research Council (MRC)).

The separate addition of lawful bases for 'tasks in the public interest' and 'legitimate interest' for the data controller is important, as it demonstrates that only the organisations that hold personal data can process it legitimately. These two bases, which are to be applied by public bodies and private entities, respectively, clearly distinguish between the processing of health data for the public interest and for commercial purposes. The alternative lawful bases for processing personal data for research signifies the GDPR's positive step towards welcoming scientific research and step away from requirement for consent, which may hamper scientific research.

In contrast, there is no provision in the Malaysian PDPA that explicitly provides a lawful basis for such tasks. In Malaysia, according to the PDPA, the processing of sensitive personal data, including health data, requires 'explicit consent', subject to certain derogations such as when such use is required by law (Section 42 PDPA). Sections 6(2)(a)–(f) highlight that a data user may process personal data if it is necessary for the performance of a contract (Section 6(2)(a)), if it is at the request of the data subject (Section 6(2)(b)), if it is done to comply with legal obligations (Section 6(2)(c)), if it is to protect the vital interests of data subjects (Section 6(2)(d)), if it is for the administration of justice (Section 6(2)(e)) or, lastly, if doing so exercises the functions conferred by law (Section 6(2)(f)). Remarkably, none of the mentioned legal bases explicitly

related to the two bases mentioned in the GDPR. However, in another provision, which does not concern lawful bases for research use, Section 39(e) of PDPA states that 'personal data may be disclosed for any purpose other than the purpose where it was originally collected if the disclosure was justified in the public interest in circumstances as determined by the Minister' (Section 39(e) PDPA). This demonstrates that the PDPA lacks a clear public-interest lawful basis for processing health data without consent. Further, although Section 39(e) of the PDPA provides public interest as a condition for data sharing, it does not specify a broad lawful basis for processing health data for research without consent. Consequently, Malaysian researchers face greater challenges under the PDPA in accessing health data for research when asking consent from individuals is impractical.

ADHERENCE TO DATA PROTECTION PRINCIPLES AND DEROGATIONS WHEN NECESSARY TO ACCOMMODATE RESEARCH IN THE PUBLIC INTEREST

DPL governs the processing of personal data by reference to a set of principles that ensure, *inter alia,* that data is only processed when it is fair and lawful to do so, that data is retained for no longer than is necessary for the purposes for which they were obtained, that data is processed only in a manner that ensures appropriate security. Compliance with these principles is overseen by an independent body commonly termed 'data protection authorities which is designed to enforce data protection obligations on the controllers and protect the privacy rights of individuals (Laurie et al 2019; Mondschein et al. 2019). Failure to comply with the law can result in significant fines and civil claims from data individuals (data subject) who have suffered as a result (Raul 2021).

The first principle to data processing in the GDPR deals with 'lawfulness, fairness and transparency' principle (Article 5 GDPR). The **lawfulness** principle requires the processing be based on a lawful basis, such as consent or another legitimate reason. **Fairness** requires that data be used in ways that individuals would reasonably expect without causing them undue harm. The **transparency** component is fundamentally linked to fairness; ensures that individuals are informed from the outset about who is processing their data, why it is used and how. This transparency is crucial for informing the public about the use of their data, helping them recognise the benefits of research, and reducing objections to data processing. Healthcare registration forms could include a privacy notice explaining that personal data may be used for research, so by signing, individuals acknowledge and consent to potential research use. This "privacy notice" can appear as a leaflet, poster, or website statement, notifying individuals about the possible research use of their data, reinforcing transparency, and fostering public trust.

Likewise, the fairness and transparency principles are called the Notice and Choice Principle in the PDPA 2010. This principle requires the data user to inform the data subject via written notice about various information, including the purpose of data collection (Section 7(1) PDPA). In essence, the Fairness and Transparency Principles in the GDPR and the Notice and Choice Principle in the PDPA both intended to notify individuals about the intended purpose of processing and details about the activity. They are important for fostering trust and transparency in processing activities by making the data subject aware of the possible uses of their information. Practically, most organisations comply with the principles by providing a privacy notice that incorporate all the above information. When the notice includes the purpose of processing, individuals are given an opportunity to understand how their data is used, have a greater control over it and effectively exercise their rights.

Another core principles of the GDPR are like data minimisation, purpose limitation, storage limitation and integrity and confidentiality stipulating that personal data should only be processed when necessary and secured. When research aims to serve public interest and safeguards are in place, the GDPR offers derogations, such as exemptions from the purpose and storage limitation principles permitting further processing and longer retention periods. Another principle, the accountability principle requires the healthcare authorities processing the data demonstrate that they have complies with the GDPR requirements by consolidating necessary safeguards or security measures to protect personal data. Nevertheless, Malaysia's PDPA lacks a similar provision, leaving these authorities with fewer formal responsibilities to prove their commitment to protecting personal data.

PROCESSING HEALTH DATA FOR SCIENTIFIC RESEARCH IN THE PUBLIC INTEREST WITH ROBUST SAFEGUARDS

To safeguard privacy and support research activities, data protection law (DPL) must enforces robust safeguards. These measures are crucial for protecting individual rights, ensuring data security, and building public trust. Public trust is essential for the viability of research involving health data. By implementing robust safeguards, research institutions demonstrate their commitment to respecting individuals' rights which can alleviate public concerns about privacy. These safeguards also play pivotal roles for security purposes to prevent unauthorised access and mitigates risks associated with data breaches. Avoiding these risks are crucial in healthcare as breaches can damage institutional reputations and discourage public engagement (Staunton 2019). The EU GDPR and Malaysia's PDPA unfold significant approaches to handling patient health data, with critical disparities that impact their support for medical research. Under the GDPR, health data processing is strictly regulated, particularly when used in the public interest for scientific research (Staunton 2019). Article 9(2)(j) of the GDPR provides a specific derogation that allows the processing of health data for scientific research without individual consent, but only if the healthcare sector and researcher implements sufficient safeguards to protect individuals right to privacy. This legal structure allows public healthcare sectors, such as research universities and healthcare facilities, to conduct research-use of health data under a well-defined legal framework that balances research utility with privacy protection.

There are six key safeguards required by the GDPR to protect personal data in research. Article 89(1) mandates that health data used for scientific research include safeguards such as data minimisation and pseudonymisation, which are essential for maintaining data privacy and research integrity. Data minimisation requires that only the minimum amount of personal data necessary to achieve the purpose should be used. In the research context, this means using the least amount of health data needed to achieve the research's objectives, which limits the exposure of sensitive data and mitigates the risk of privacy breaches. The GDPR also strongly requires pseudonymisation as a technical and organisational measures to protect patient's data (Article 4(4) GDPR). Pseudonymisation of personal data refers to the act of altering personal data to the extent the that the data subject (the patient) cannot be directly identified without having further information (Mondschein et al. 2019). It involves replacing patient's identifiable information with codes or identifiers, which makes it more difficult to link data back to patient directly. This technique allows researchers to work with health data in a way that limits the possibility of re-identification, protecting privacy while still permitting meaningful data linkage and analysis (*R v. Department of Health ex parte Source Informatics Ltd*, *2000*).

Additionally, the GDPR introduces proactive security principles like Data Protection by Design (DPbD) and Data Protection by Default (DPbDf) which requiring that data processing systems be designed with privacy settings enabled from the outset, ensuring that privacy risks are minimised automatically (Article 25 GDPR). DPbD requires data controllers to design systems with built-in privacy measures such as default settings that enforce the highest level of data security. For example, data systems or software used in research should automatically enable privacy settings without requiring users to opt in. The principles of DPbD and DPbDf may help average users ensure that by default, the system used to process health data is designed and embedded with safeguards. This approach is crucial to promote a culture of privacy by default within research institutions (Jasmontaite et al. 2018).

In the event that processing is highly-likely to have a high risk to patient participants despite the implemented safeguards, the GDPR requires data controllers to conduct a preventive data protection impact assessment (DPIAs) (Article 35 GDPR). A DPIAs is a systematic process conducted to assess the potential risks of a study, particularly those involving sensitive data or a high-scale research data. It helps the organisations identify and address privacy risks early by implementing safeguards and security measures to ensure the protection of personal data and demonstrate compliance with the GDPR. (Kingston 2017).

The GDPR requires a combination of technical and organisational safeguards to safeguard data throughout its lifecycle. Technical measures may include secure data storage, encrypted data use and sharing, and limiting data access to only authorised personnel. Organisational measures, on the other hand, involve policies, training, and protocols that ensure all personnel involved in data sharing are informed of and adhere to data protection requirements. For medical research, these safeguards help establish a secure environment that upholds data confidentiality and integrity and is particularly important when consent of the patient is impractical to obtain (Staunton et al. 2019; Jasmontaite et al. 2018).

In contrast, the PDPA lacks specific provisions to accommodate health data processing for research in the public interest. While the PDPA includes conditions allowing health data processing for "medical purposes," these are primarily limited to clinical contexts rather than broader scientific research. The PDPA's limited scope further narrows its applicability to private sectors, thereby excluding public sector bodies, such as government hospitals, from its data protection framework. This restriction leaves health data handled by public institutions without regulatory oversight under the PDPA, creating gaps in data protection for public sector research. Sections 39(5) and 6(2) of the PDPA mention health data processing for public interest, but these provisions are neither specific to research nor robust enough to support structured health research on par with the GDPR. This gap hinders Malaysia's ability to leverage public health data effectively for scientific research, posing a stark contrast to the GDPR's comprehensive approach that actively supports research through clear legal bases.

The PDPA also lacks these proactive and specific safeguard measures. While it includes a general security obligation, it does not mandate technical or organisational safeguards comparable to the GDPR's specific requirements. Without explicit guidance on implementing measures like DPbD, DPbDf, or DPIAs, the Malaysian PDPA security framework remains reactive, primarily addressing data protection after potential risks or breaches have occurred. This limitation may erode public confidence in Malaysia's data privacy framework, especially since public sector institutions, which handle large volumes of health data, are exempt from the PDPA. The absence of pre-processing safeguards restricts Malaysia's capacity to protect data subjects in research contexts comprehensively. Adopting proactive safeguards, similar to those in the GDPR, would

enable Malaysia to better balance data protection with the benefits of health research, enhancing both privacy and research viability.

In summary, the GDPR's structured approach, with its clear lawful basis and robust safeguards for health data processing in scientific research, supports a balanced model that advances research while safeguarding privacy. The GDPR's structured safeguards such as DPbD, DPbDf, and DPIAs are crucial for research viability without compromising privacy. These safeguards allow researchers to access necessary patient data while maintaining compliance with privacy laws. This detailed requirements for safeguards provide a clear framework for responsible data use, ensuring that research-use of health data are legally sound and aligned with best practices in data protection.

Conversely, the PDPA's limited scope and absence of explicit research-friendly provisions and safeguards hinder Malaysia's capacity to fully support privacy-health research, especially within public healthcare sectors. To strengthen health data use for research and align with international standards, the PDPA could benefit from integrating proactive data protection measures, ensuring that both private and public research initiatives are conducted within a secure, privacy-compliant framework.

CONCLUSION

An ideal data protection law should reconcile the protection of patient privacy with the facilitation of medical research that serves the public interest. Such a law would safeguard personal data at every stage from its collection, use and sharing while ensuring that research activities are not unduly restricted. To achieve this, the law should establish a specific "public interest" lawful basis that permits the processing of health data for research purposes without requiring individual patient consent, provided it is subject to robust safeguards. This approach would protect patients' rights while allowing valuable research to advance, supporting both privacy and public health outcomes. The comparative analysis of the EU GDPR 2018 and Malaysia's PDPA 2010 uncovers significant differences in their approach to sharing patient health data for research, particularly regarding informed consent, public interest provisions and the requirement of safeguards measures. The GDPR demonstrates flexibility by allowing health data use without consent for public-interest research under specific lawful bases (i.e public task) and mandates robust safeguards like data minimisation, pseudonymisation and Data Protection Impact Assessments (DPIAs). This framework empowers researchers to access health data for essential medical research while prioritising patient privacy rights, thus achieving the twin aims of facilitating medical research while safeguarding patient interests to privacy.

In contrast, Malaysia's PDPA lacks similar breadth and flexibility. Its application is limited to the private healthcare sector which excludes public healthcare institutions—the largest repositories of patient health data from its scope. Additionally, the PDPA lacks 'public-interest lawful basis' for research without consent and does not stipulate specific safeguards, thereby restricting the availability of patient data for research in Malaysia. These limitations create a fragmented and less supportive environment for data-driven medical research, which can deter the country's ability to conduct large-scale, impactful studies and reduce its alignment with international data protection standards.

To enhance the PDPA's support for public-interest research, several key reforms are recommended. Expanding the PDPA's scope to include public healthcare data would address existing inconsistencies and establish a unified framework for privacy protection. Additionally, establishing a lawful basis for research in the public interest, would allow data use without patient consent in specific cases when seeking consent is impractical. Finally, incorporating mandatory safeguards like Data Protection Impact Assessments (DPIAs,) data minimisation and pseudonymisation would strengthen privacy protections, bolster public trust and create a more research-friendly regulatory environment. Together, these reforms would align Malaysia's PDPA more closely with international best practices, supporting ethically robust medical research.

ACKNOWLEDGMENT

The authors gratefully acknowledge Universitas 17 Agustus 1945 Semarang for funding this research project (Reference Code: UU-2024-005).

AUTHOR'S CONTRIBUTION

Introduction, Result and Discussion & Conclusion: Siti Farahiyah Ab Rahim; Methodology: Muhamad Firdaus Ab Rahman.

REFERENCES

Abu Bakar Munir and Siti Hajar Mohd Yasin. (2010). *Personal Data Protection in Malaysia: Law and Practice.* Malaysia: Sweet & Maxwell Asia.

Alibeigi, A., & Abu Bakar Munir. (2020). Malaysian personal data protection act, a mysterious application. *U. Bologna L. Rev.*, *5*, 362.

Arif, M. I. A. M., Markom, R., Adenan, F., & Rosei, M. S. D. A. (2024). Analyzing Social Viability of the Commercial Real Estate Waqf in Malaysia. Akademika, 94(2), 280-297.

Barbour, R.S., Kingdom, U., Buscatto, M., Chamberlain, K., Zealand, N., Coetzee, J.K. and Sun, J. (2018), *The SAGE Handbook of Qualitative Data Collection*, Los Angeles: SAGE Publications Inc.

Batko, K., Ślęzak, A. The use of Big Data Analytics in healthcare. *J Big Data* 9, 3 (2022). https://doi.org/10.1186/s40537-021-00553-4

Beauchamp, T. L., & Childress, J. F. (1994). *Principles of biomedical ethics*. Edicoes Loyola.

Bell, J., Aidinlis, S., Smith, H., Mourby, M., Gowans, H., Wallace, S. E., & Kaye, J. (2019). Balancing data subjects' rights and public interest research: Examining the interplay between UK law, EU human rights law and the GDPR. *Eur. Data Prot. L. Rev.*, *5*, 43.

Cate, F. H. (2010). Protecting privacy in health research: the limits of individual choice. *Calif. L. Rev.*, *98*, 1765.

Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. *ecancermedicalscience*, *11*.

Chico, V. (2018). The impact of the general data protection regulation on health research. *British medical bulletin*, *128*(1), 109-118.

Department of Personal Data Protection Malaysia. 2024. Personal Data Protection Act (Amendment) 2024. https://www.pdp.gov.my/ppdpv1/pindaan-akta-perlindungan-data-peribadi-2024/. Retrieved on: 6 November 2024.

Dove, E. S. (2018). The EU general data protection regulation: implications for international scientific research in the digital era. Journal of Law, *Medicine & Ethics*, 46(4), 1013-1030.

Dove, E. S., & Chen, J. (2020). Should consent for data processing be privileged in health research? A comparative legal analysis. *International Data Privacy Law*, *10*(2), 117-131.

Duguet, A. M., & Herveg, J. (2021). Safeguards and derogations relating to processing for scientific purposes: Article 89 analysis for biobank research. In *GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe*, 105-120..

Farah Nabilah. 2024. PDPA amendments missing key details. Institute of Strategic & International Studies (ISIS) Malaysia. 30 July. https://www.isis.org.my/2024/07/30/pdpa-amendments-missing-key-details/. Retrieved on: 6 November 2024.

Gostin, L. O. (2001). Health information: reconciling personal privacy with the public good of human health. *Health Care Analysis*, *9*, 321-335.

Greenleaf, G. (2010). Limitations of Malaysia's data protection Bill. *Privacy Laws & Business International Newsletter*, *104*(1), 5-7.

Greenleaf, G. (2012). ASEAN's 'New'Data Privacy Laws: Malaysia, the Philippines and Singapore. *Privacy Laws & Business International Report*, (116), 22-24.

Herring J. (2018). *Medical Law and Ethics*. 7th edn, Oxford University Press.

Information Commissioners Office. n.d. Overview- Data Protection and the EU. https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/. Retrieved on: 6 November 2024.

Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., & Leucci, S. (2018). Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *Eur. Data Prot. L. Rev.*, *4*, 168.

Joseph Kaos Jr. (2017). Health Ministry launches Malaysian Health Data Warehouse. *The Star,* 18 Apr. https://www.thestar.com.my/news/nation/2017/04/18/health-ministry-launches-malaysian-health-data-warehouse/. Retrieved on: 6 November 2024.

Juntao, Fang. (2024). Research on the application of data mining in the field of healthcare. doi: 10.62051/4pdg6558.

Kartina Aisha Choong (2016) 'Malaysia' in Herman Nys (eds) *International Encyclopaedia of Laws: Medical Law* (Kluwer Law International)

Kasperbauer, T. J. (2020). Protecting health privacy even when privacy is lost. *Journal of medical ethics*, *46*(11), 768-772.

Kassim, P. N. J., & Ramli, N. (2016). The Inviolability of medical confidentiality in Malaysia: An analysis of the rules and exceptions. *IIUMLJ,* 24, 335.

Kassim, P. N. J., Alias, F., & Muhammad, R. W. (2014). The Growth of Patient Autonomy in Modern Medical Practice and the Defined Limitations under the Shari'ah. *IIUMLJ*, 22, 213.

Kingston, J. (2017). Using artificial intelligence to support compliance with the general data protection regulation. *Artificial Intelligence and Law*, *25*(4), 429-443.

Laurie, G. H., & Dove, E. (2019). *Mason and McCall Smith's law and medical ethics*. Oxford University Press.

Laurie, G., & Postan, E. (2013). Rhetoric or reality: what is the legal status of the consent form in health-related research?. *Medical Law Review*, 21(3), 371-414.

Laurie, G., & Sethi, N. (2011). Information governance of use of health-related data in medical research in Scotland: Current practices and future scenarios. *U. of Edinburgh School of Law Working Paper,* (2011/26).

Laurie, G., Ainsworth, J., Cunningham, J., Dobbs, C., Jones, K. H., Kalra, D. & Sethi, N. (2015). On moving targets and magic bullets: Can the UK lead the way with responsible data linkage for health research?. *International journal of medical informatics*, 84(11), 933-940.

Laws of Malaysia [Act 388], Interpretation Acts 1948 and 1967

Lee Ewe Poh v Dr Lim Teik Man & Anor [2011] 1 MLJ 835

Manap, N. A., Ab Rahman, M. R., & Salleh, S. N. F. A. (2024). Big Data and The Deterioration of Consent Principle To Protect Health Data Privacy In Malaysia. *Malaysian Journal of Syariah and Law*, 12(3), 550-561.

Marhaban, S. M., & Shukri, M. H. M. (2022). Gerakan Antivaksin dan Keperluan Penyelesaian Menurut Perspektif Undang-Undang di Malaysia: Suatu Analisis. *Akademika*, *92*(2), 97-112.

Medical Research Council (MRC). (2018). MRC Ethics Series: Using information about people in health research. https://www.ukri.org/wp-content/uploads/2021/08/MRC-0208212-Using-information-about-people-in-health-research-2018.pdf. Retrieved on: 6 November 2024.

Ministry of Health Malaysia. https://www.moh.gov.my/. Retrieved on: 6 November 2024

Mohamed, A. E., (2013). Social Change, Health and Quality of Life in the Klang Valley Metropolitan Region-Langat). *Akademika*, *83*(1), 11-24.

Mondschein, C. F., & Monda, C. (2019). The EU's General Data Protection Regulation (GDPR) in a research context. *Fundamentals of clinical data science*, 55-71.

Mostert, M., Bredenoord, A. L., Biesaart, M. C., & Van Delden, J. J. (2016). Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. *European Journal of Human Genetics*, *24*(7), 956-960.

Mostert, M., Bredenoord, A. L., Van Der Slootb, B., & Van Delden, J. J. (2018). From privacy to data protection in the EU: Implications for big data health research. *European Journal of health law*, *25*(1), 43-55.

Mourby, M. J., Doidge, J., Jones, K. H., Aidinlis, S., Smith, H., Bell, J. & Kaye, J. (2019). Health data linkage for UK public interest research: key obstacles and solutions. *International Journal of Population Data Science*, *4*(1).

n.a. 2024. From Data to Action: GIS Technology in Malaysian Healthcare. *HealthCareAsia Daily*, 6 April. https://www.healthcareasia.org/2024/from-data-to-action-gis-technology-in-malaysian-healthcare/> Retrieved on: 29 October 2024.

n.a. n.d. Malaysian Health Data Warehouse. *Ministry of Health Malaysia.* https://myhdw.moh.gov.my/public/home. Retrieved on: 6 November 2024.

Neely, A.H. and Ponshunmugam, A. (2019), "A qualitative approach to examining health care access in rural South Africa", *Social Science and Medicine*, Vol. 230, pp. 214-221, doi: 10.1016/j.socscimed.2019.04.025.

Noriswadi Ismail & Cieh, E. L. Y. (2013). Limitations of the Personal Data Protection Act 2010 and Personal Data Protection in Selected Sectors. *Beyond Data Protection: Strategic Case Studies and Practical Guidance*, 65-98.

Nuffield Council on Bioethics. (2015). Biological and health data. http:// nuffieldbioethics.org/wp-content/uploads/DataEthics_Chapter5.pdf. Retrieved on: 3 November 2023.

Porsdam Mann, S., Savulescu, J., & Sahakian, B. J. (2016). Facilitating the ethical use of health data for the benefit of society: electronic health records, consent and the duty of easy rescue. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160130.

Quinn, P. (2021). Research under the GDPR–a level playing field for public and private sector research?. *Life Sciences, Society and Policy*, *17*(1), 4.

R v. Department of Health ex parte Source Informatics Ltd. [2000] 1 All ER 786 (CA).

Raul, A. C. (Ed.). (2021). *The privacy, data protection and cybersecurity law review*. Law Business Research Limited.

Raul, A. C. (Ed.). (2021). *The privacy, data protection and cybersecurity law review*. Law Business Research Limited.

Roslan, W. S. A. W., Hassim, J. Z., (2019). Kestabilan Kewangan Liga Sukan Profesional: Analisis Perundangan terhadap Peraturan dan Amalan Liga Sukan Profesional. *Akademika*, *89* (SI2), 129-142.

Rumbold, J. M. M., & Pierscionek, B. (2017). The effect of the general data protection regulation on medical research. *Journal of medical Internet research*, *19*(2), e47.

Saldana, J. (2011), *Fundamentals of Qualitative Research*, in Beretvas, N., (Ed.), Oxford University Press, New York, NY.

Shariff, A. A. M., & Rahman, M. A. (2018). Syariah Principles Regarding Investigation and Prosecution Procedures: A Wealth of Knowledge Propeling Towards Legal Development in the Society. *Akademika*, *88*(3), 127-135.

Shazwan Mustafa Kamal. 2017. Big data in healthcare: What we (need to) know. Malaymail, 21 April. https://www.malaymail.com/news/malaysia/2017/04/21/big-data-in-healthcare-what-we-need-to-know/1360925. Retrieved on: 6 November 2024.

Sidi Ahmed, S. M., & Sonny Zulhuda. (2019). Data protection challenges in the internet of things era: an assessment of protection offered by PDPA 2010. *International Journal of Law, Government and Communication (IJLGC)*, *4*(17).

Snyder, J. E., & Gauthier, C. C. (2008). *Evidence-based medical ethics:: cases for practice-based learning*. Springer Science & Business Media.

Staunton, C., Slokenberga, S., & Mascalzoni, D. (2019). The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. *European Journal of Human Genetics,* 27(8), 1159-1167.

Taylor, J. A., Crowe, S., Pujol, F. E., Franklin, R. C., Feltbower, R. G., Norman, L. J. & Pagel, C. (2021). The road to hell is paved with good intentions: the experience of applying for national data for linkage and suggestions for improvement. *Bmj Open*, *11*(8), e047575.

Taylor, M., & Townend, D. (2022). Towards a new privacy: informed consent as an encumbrance to group interests? In *Law and legacy in medical jurisprudence: essays in honour of Graeme Laurie* edited by G. T. Laurie, E. S. Dove & Niamh Nic Shuibhne (eds.). New York, NY: Cambridge University Press.

Taylor, S.J., Bogdan, R. and DeVault, M.L. (2016), *Introduction to Qualitative Research Method*, John Wiley and Sons, NJ.

Vedder, A., & Spajić, D. (2023). Moral autonomy of patients and legal barriers to a possible duty of health-related data sharing. *Ethics and Information Technology*, *25*(1), 23.

Westin A.F. (1968). Privacy and Freedom. *Washington and Lee Law Review* 166.

Zahir, M. Z. M., Zainudin, T. N. A. T., Raja-Manickam, R., & Abd Rahman, Z. (2019). Arahan Do Not Resuscitate (DNR) dalam Sektor Kesihatan dari Perspektif Undang-undang. *Akademika*, *89*, 143-154.

Zuryati Mohamed Yusoff. (2011). 'The Malaysian Personal Data Protection Act 2010: A Legislation Note' 9 *NZJPIL* 119.

Siti Farahiyah Ab Rahim (Corresponding author)
Faculty of Law,
Universiti Kebangsaan Malaysia, Malaysia
Email: farahiyahrahim@ukm.edu.my

Muhamad Firdaus Ab Rahman
Faculty of Syariah and Law,
Universiti Sains Islam Malaysia, Malaysia
Email: mfirdaus.rahman@usim.edu.my