DIGITALIZATION OF HOSPITALS: A COMPARATIVE STUDY BETWEEN MALAYSIA AND UNITED KINGDOM

[i*]Angelina Anne Fernandez, [ii] Nurul Asyikeen Binti Abdul Jabar, [iii] I Wayan Edi Arsawan, [iv] Nadia Nabila binti Haji Mohd Saufi, [v] Azlanor bin Rahmad, [vi] Abd Shukor bin Mohd Yunus

[i*]Management and Science University, Malaysia

*Corresponding author: angelina_anne@msu.edu.my

Article history:
Submission date: 5 Dec 2025
Received in revised form: 30 Nov 2025
Acceptance date: 31 Dec 2025

Keywords:
Digitalization, hospitals, privacy, data protection, confidentiality, healthcare law

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Fernandez, A. A., Jabar, N. A. A., Arsawan, I. W. E., Saufi, N. N. M., Rahmad, A., & Yunus, A. S. M. (2025). Digitalization Of Hospitals: A Comparative Study Between Malaysia And United Kingdom. *Current Legal Issues*, *7*(2), 95-107.

ABSTRACT

The digitalization of hospitals represents a fundamental transformation in the healthcare sector, where information technology (IT) is integrated into all aspects of hospital management, from clinical care and administration to financial and operational systems. A digital hospital utilises electronic communication systems, artificial intelligence, and networked medical devices to enhance coordination among healthcare professionals and improve patient outcomes. However, the increasing reliance on digital systems introduces significant challenges, particularly data privacy and cybersecurity risks. For instance, cyberattacks targeting hospitals in Europe and Asia have revealed vulnerabilities that threaten both data integrity and patient safety.

This paper examines the legal and regulatory frameworks governing the digitalization of hospitals in Malaysia and the United Kingdom (UK). It adopts a doctrinal legal research methodology, supported by comparative, analytical, and jurisprudential approaches, to assess the adequacy of existing laws in protecting patient data and ensuring ethical digital healthcare practices. This study makes several significant contributions to healthcare law and digital governance scholarship. First, it provides a systematic comparative legal analysis of hospital digitalization frameworks in Malaysia and the United Kingdom, highlighting regulatory gaps, overlaps, and best practices in patient data protection and confidentiality. Second, it contributes doctrinal clarity by examining how existing healthcare and data protection laws—particularly Malaysia's Personal Data Protection Act 2010 and the UK GDPR—apply to digital hospitals, electronic medical records, and emerging e-health systems. Third, the study advances policy discourse by identifying structural and normative shortcomings in Malaysia's current legal regime and proposing reform-oriented recommendations informed by the UK model. Finally, this research contributes to the broader debate on digital health governance by integrating legal, technological, and ethical perspectives, offering a framework that may guide lawmakers,

regulators, and healthcare institutions in developing resilient, patient-centred digital hospital systems.

INTRODUCTION

What constitutes a digital hospital? According to Kilic (2016), a digital hospital contributes to personal productivity, it smoothens the process of hospital procedure or operation, it protects the patient safety by integrating cutting-edge technologies namely digital communication tools.

An example of digital hospital can be seen in 2016 whereby Malaysia's first hospital, Prince Court Medical Centre had received the acknowledgement by HIMSS Analytics to receive the honour of "Stage 6" digital hospital certificate.

Amongst the biggest problem that digital hospitals can face is that medical information is prone to be hacked. It is crucial to note that patient's medical information is worth 10 times more than a normal credit card number on the black market (Humer & Finkle, 2014). The hackers sell the medical information to the black market, and this information is subjected to fraud, identity theft and abuse (Why Medical Record, 2016). This only happens if there is low security in the digital hospital. Hackers will hack medical information and commit medical fraud.

According to BBC News (2018), in the United Kingdom it was shocking when 150,000 patients' confidential information was leaked due to a software coding error in the U.K organization. According to the *New Straits Times* (NST) report dated 21 September 2023, the Personal Data Protection Department (PDPD) had received reports of 130 cases up to June 2023, revealing a four-fold increase when only 30 such cases were recorded for the entire 2022 in Malaysia. (https://www.malaymail.com/news/malaysia/2023/09/21/report-malaysias-data-breach-cases-hit-all-time-high-with-four-fold-increase-recorded-in-2023/92075).

According to a research done by Dr. Pranav Patil et al (2018), he mentioned that Digital Hospital help assist doctors, surgeons, nurses and more, in terms of check-up, diagnosis, treatment and medical observation through means of "E-Health".

Malaysia achieved a significant milestone in hospital digitalization in 2016 when Prince Court Medical Centre became the country's first hospital to be recognised by HIMSS Healthcare Information and Management Systems Society (HIMSS) AnalyticsAnalytics with a "Stage 6" digital hospital certification. This recognition was awarded based on the hospital's adoption of the HIMSS Analytics Electronic Medical Record Adoption Model (EMRAM), a globally recognised benchmarking framework that evaluates hospitals' electronic medical record (EMR) capabilities through an integrated methodological and algorithmic assessment of digital maturity..

According to a report by Deloitte, the global health care expenditure is expected to reach $10.059 trillion by the year 2022, this is due to the inefficiency in maintaining healthcare delivery through cost-containment efforts and rapid economic growth (Deloitte, 2019).

Against this backdrop, this study is guided by the central research question: *To what extent do the existing legal and regulatory frameworks in Malaysia and the United Kingdom adequately govern the digitalization of hospitals, particularly in relation to patient data protection, privacy, and confidentiality?* A related inquiry examines whether Malaysia's current healthcare and data protection laws are

sufficiently equipped to address emerging risks posed by electronic medical records, big data analytics, and e-health technologies when compared to the more mature regulatory framework of the United Kingdom. The contribution of this research lies in its comparative legal analysis of two common law jurisdictions at different stages of digital health governance. By examining statutory provisions, regulatory guidelines, and reported data breach incidents, this study identifies legal gaps and enforcement challenges within Malaysia's digital hospital ecosystem. It further contributes to scholarly and policy discourse by offering reform-oriented recommendations informed by the UK experience, with the aim of strengthening patient trust, enhancing cybersecurity resilience, and promoting ethically sound and legally robust digital hospital systems.

Amongst the most pressing challenges that digital hospitals face is the vulnerability of medical information to cyberattacks. Patient medical data is highly sensitive and, unlike a credit card number, contains a comprehensive record of a person's identity, medical history, prescriptions, and sometimes even genetic information. This makes it extremely valuable on the black market—estimated to be worth **ten times more than a credit card number** (Humer & Finkle, 2014). Hackers target such data not only for financial gain through medical fraud and identity theft but also because it can be exploited repeatedly over time, unlike a credit card number which can be cancelled once compromised (Why Medical Record, 2016). The intrinsic value and permanence of medical data make it uniquely precious, underscoring the ethical and legal responsibility of hospitals to safeguard it.

Real-world incidents illustrate the magnitude of this risk. For instance, in the United Kingdom, a software coding error led to the exposure of **150,000 patients' confidential medical records**, demonstrating how even small technical vulnerabilities can compromise massive amounts of sensitive information (BBC News, 2018). Similarly, in Malaysia, the Personal Data Protection Department (PDPD) reported **130 cases of data breaches up to June 2023**, a four-fold increase from the previous year, signaling rising vulnerabilities in local digital health infrastructure (New Straits Times, 2023).

Despite these risks, digital hospitals offer significant advantages. Research by Patil et al. (2018) highlights that digital hospitals enhance healthcare delivery by supporting doctors, surgeons, and nurses in check-ups, diagnoses, treatments, and continuous patient monitoring through **E-Health systems**. Malaysia's Prince Court Medical Centre exemplifies such advancement, having achieved the **HIMSS Analytics Stage 6 digital hospital certification in 2016**, which reflects the hospital's sophisticated integration of electronic medical records (EMR) to optimize patient care while maintaining security standards (HIMSS Analytics, 2016).

While the adoption of digital systems improves efficiency and quality of care, the high value of medical data amplifies the stakes. Hospitals must therefore implement robust cybersecurity measures to prevent breaches that could irreparably harm patients, both financially and personally. This tension between technological advancement and data security highlights the critical challenge facing digital hospitals today.

LITERATURE REVIEW

One of the biggest challenges that digital hospitals face is data and analytics challenge. This is due to the amount of useable patient health data that has increased drastically in the past decade. It is crucial to note that almost thirty percent of the data are from healthcare industry (Pramanik et al, 2019). This includes very sensitive personal details namely the patient's diagnosis,

pathology, operation, financial and insurance information, notes, documents and more. Imagine all this sensitive information falling into the hands of the cracker and hacker outside of the hospital wall. It is crucial for hospitals to have professional data governance to maintain the integrity of the hospitals. As professional governance will make the doctors make proper clinical decisions that directly affect their patients' lives (Gopal et al, 2019). It is crucial for hospitals to implement **professional data governance**, which refers to a structured framework of policies, procedures, and accountability mechanisms designed to ensure the proper collection, storage, access, and usage of sensitive medical information (Gopal et al., 2019). Professional data governance goes beyond merely maintaining electronic records; it establishes clear rules on **who can access patient data, under what circumstances, and with what level of authorization**, while ensuring compliance with national and international privacy standards. By instituting such governance, hospitals create an environment in which **clinical decisions are informed by accurate, timely, and secure data**, thereby directly impacting patient outcomes.

Critically, professional data governance serves as a proactive defense against cybersecurity threats. By implementing strict access controls, regular auditing, encryption of sensitive data, and staff training on security protocols, hospitals can significantly reduce the risk of medical information falling into the hands of hackers. Moreover, well-structured governance fosters accountability, so that any unauthorized access or data breach can be promptly identified and mitigated, limiting both the clinical and financial consequences of a breach. In essence, professional data governance not only **protects the integrity of patient information** but also **enhances trust between healthcare providers and patients**, while ensuring that digital hospitals can leverage technology for improved care without compromising privacy.

Amongst the advantage of digital hospitals are the fact that by utilizing Big Data technologies in the digital hospital, hospital staff will be more aware of their patients' need and treatment by reviewing their patient's history before administering treatment (Disch, 2016). Hospital staff will be more well informed on their patients' need and treatment by reviewing their patient's history.

Amongst the efforts by Malaysia is the Malaysian Health Data Warehouse (MyHDW) 2017 which was introduced and is currently an ongoing project under the Ministry of Health Malaysia (Ministry of Health, Malaysia, 2017). The whole purpose of the project is to develop a centralized database for health data in Malaysia. Another initiative is the MySejahtera app (Parliament Account Committee (PAC, 2021) that is to assist during the COVID-19 pandemic to facilitate contact tracing efforts.

The Ministry of Health's (MOH) record-breaking allocation of RM41.22 billion in Budget 2024 will include allocations to expand the use of digital health records and further promote preventive health care.

The Malaysian Prime Minister Anwar Ibrahim announced in Budget 2024 the allocation of RM150 million to maintain and expand information technology (IT) systems under the MOH, which includes the implementation of Clinic Management System Subscription (CCMS) in 100 *klinik kesihatan* (health clinics), covering rural and community clinics as well.

To quote the Prime Minister "Only three per cent of the nation's health clinics are equipped with digital health records. Digital records are crucial for quickly accessing patient data and can be shared across all government health care facilities," Anwar said when presenting Budget 2024. (Budget, 2024)

The Malaysian Health Minister Dr Zaliha Mustafa had emphasized that digital records are vital for quick patient data access and sharing among government health care facilities. This improves the work process for MOH frontline staff and reduces patient waiting times.

It is crucial to note that at Selayang Hospital, the electronic medical record (EMR) system—once the flagship digital system—was not upgraded, resulting in its deterioration and forcing many processes to revert to manual methods, which doctors reported has significantly delayed operations and compromised patient care (CodeBlue, 2023). So **while the EMR problem at Selayang Hospital has not yet been fully resolved**, the government has **expressed a commitment to upgrade and reinstate a robust digital records system**, and the broader national EMR expansion indicates ongoing engagement with digital health transformation.It is also crucial to note that Hospital Kuala Lumpur (HKL), one of the country's largest and busiest hospitals, handles up to 16,000 medical records manually every day.

Thus, Malaysians have realized the need to maximize the latest technology in healthcare. Amongst the challenges is the privacy issue in which the patient's personal data should be protected under the law with the advancement of such technology in data processing and analytics. The implementation of these initiatives has caused many concerns namely on issues of data privacy and the readiness of the Malaysians for the Personal Data Protection Law 2010(Act 709)

In Malaysia, the Medical Act 1971 governs the registration and practice of medical practitioners and applies to both private and public healthcare settings. Additionally, professional standards are reinforced by the Malaysian Medical Council through instruments such as the Confidentiality Codes 2011.There are also other legislations that are important for digital hospitals namely the government circular on "Guidelines for Handling and Management of Patient Medical Records for Hospitals and Medical Institutions 2010" in which it clearly states that the hospital own the physical form and the medical report, but the patient's own the information. There are also other important Malaysian healthcare regulations and policy instruments governing the management of patient medical records, such as the **Pekeliling Ketua Pengarah Kesihatan Bil. 17/2010: Garis Panduan Pengendalian dan Pengurusan Rekod Perubatan Pesakit bagi Hospital-Hospital dan Institusi Perubatan** issued by the Ministry of Health, which clarifies that while the hospital holds the physical records, the information contained therein belongs to the patient; these principles are reinforced in updated **Ministry of Health medical records guidelines** that continue to govern the confidentiality, security, retrieval, storage, and disposal of both electronic and physical medical records in public health facilities.

According to the Guideline on Medical Records and Medical Reports 2006, all rights in regard to the ownership of a patient's medical record are held together by the medical practitioner, the healthcare institution, and the healthcare services. Therefore, it is crucial to note that medical records are the intellectual property of the physician who created them and the patient.

In Malaysia, it is important to note that there is no dedicated legislation specifically governing the protection of health data; instead, data protection in the healthcare sector is primarily regulated under the Personal Data Protection Act 2010 (Act 709), which serves as the closest applicable legal framework.According to Liddell (2021) he stated that GDPR covers the meaning processing of personal data, which suits the big data context, whether the data are in electronic or computerized records or on paper. Article 4 of GDPR defines personal data as any information

relating to an identified or identifiable natural person (data subject).

Amongst the challenges that Malaysia face is the GDPR has changed the rules pertaining to handling of data in the European Union. The GDPR attempts to clarify the roles and rights of both the people in which information is being collected namely (data subjects, article 4 (1) GDPR) and the people in charge of collecting that information (data controllers and data processors, article 4 (7), (8) GDPR. Therefore, it is crucial for Malaysia to develop a **comprehensive regulatory guideline on personal data protection in healthcare**, drawing inspiration from the **General Data Protection Regulation (GDPR)** of the European Union. Such a guideline should provide a **clear and legally binding definition of medical data**, including what constitutes sensitive health information, how it can be collected, stored, processed, and shared, and the obligations of healthcare providers in safeguarding this data. Additionally, the framework should establish **mandatory security standards, consent protocols, breach reporting mechanisms, and penalties for non-compliance**, ensuring accountability at every level of the healthcare system.

By implementing a GDPR-inspired regulatory framework, Malaysia can address existing gaps in legislation, **strengthen patient trust**, and provide hospitals with a structured approach to data governance. Moreover, clear definitions and standardized protocols would **reduce ambiguity for healthcare providers**, enabling them to adopt digital health systems confidently while minimizing the risk of data breaches, identity theft, and unauthorized access. In effect, such regulation would not only **protect patients' sensitive information** but also **enhance the credibility and safety of Malaysia's digital hospitals** in line with global best practices.

Therefore, it is crucial to note that based on the GDPR approach, Malaysia should develop a regulatory guideline specifically on the definition as we are still lacking.

As for the United Kingdom, there are two legislations on digital healthcare namely the UK Data Protection Act 2018 (DPA) which handles patient health data information and the system for telemedicine services which is still not yet fully updated with UK healthcare regulatory regime.

The UK General Data Protection Regulation has grave restrictions on the use of health data without providing notice of that use and demonstrating an appropriate legal basis for processing the special-category data. Amongst the issues on digital hospitals are in regard to patient confidentiality and misuse of private information (MoPI). It is crucial to note that the UK GDPR also imposes additional requirements namely to keep data secure, maintain its availability and accuracy, report data incidents, appoint a Data Protection Officer and/or a "Representative", conduct DPIAs, and generally ensure that usage of personal data is fair, lawful and does not involve excessive amounts of data.

Also, the UK GDPR grants individuals substantial personal data rights, e.g. to access or delete their data. The DPA also has certain additional rules, which includes criminal offences for re-identifying personal data, or selling it after it has been improperly obtained.

The UK GDPR makes it a requirement that controllers ensure that data is accurate, up to date and processed fairly. It also makes it a requirement for controllers to notify individuals about how their data may be processed, including the logic used in automated decisions made about them. ICLG. (n.d.). *Digital health laws and regulations: United Kingdom.* International Comparative Legal Guides. Retrieved December 30, 2025, from

https://iclg.com/practice-areas/digital-health-laws-and-regulations/united-kingdom)

If the personal data of users/patients is processed using digital health software, such processing must comply with the data protection laws in force in the UK, in particular with:

- The UK General Data Protection Regulation ("GDPR");
- The Data Protection Act 2018 (the "DPA") and
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), to the extent relevant.

It is also important to note that the UK GDPR is in regards the processing of personal data and it requires that any processing undertaken is done (amongst other things) lawfully, fairly and in a transparent manner namely Articles 5(1)(a), and 6.

According to Article 5 of GDPR:

1. "Personal data shall be:

    a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

    b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

    c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

    d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

    e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

According to Article 6 of GDPR,

Processing shall be lawful only if and to the extent that at least one of the following applies:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The UK GDPR also imposes other conditions namely on the processing of "special category data" which includes health data. This is embodied in Article 9 GDPR.

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

The Consumer Rights Directive (2011/83/EC) applies when a person purchases an application relating to lifestyle or wellbeing therefore any data that is transferred via the app is likely to be considered personal data.

A structured comparison between Malaysia and the United Kingdom demonstrates significant divergence in the regulation of digital hospitals across several key dimensions. In terms of legal basis, Malaysia relies on a fragmented framework comprising the Personal Data Protection Act 2010, the Medical Act 1971, professional confidentiality codes, and administrative guidelines, none of which are specifically designed to regulate digital hospitals or large-scale health data processing (Personal Data Protection Act 2010; Medical Act 1971; Malaysian Medical Council, 2011). In contrast, the United Kingdom operates under a comprehensive statutory regime through the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, which expressly recognise health data

as "special category data" warranting enhanced protection (UK GDPR, art. 9; Data Protection Act 2018). With respect to regulatory scope and clarity, Malaysia's approach remains largely general and reactive, whereas the UK framework provides detailed obligations governing lawful processing, transparency, data minimisation, data security, and accountability, including mandatory breach notification and Data Protection Impact Assessments (Articles 5, 6, and 35 UK GDPR; Liddell, 2021). In relation to patient rights, Malaysian law affords limited and less clearly articulated rights of access and control over personal health data, while UK patients enjoy extensive data subject rights such as access, rectification, erasure, restriction of processing, and safeguards against automated decision-making (Articles 15–22 UK GDPR). Enforcement mechanisms further distinguish the two jurisdictions, as Malaysia continues to face challenges in sector-specific guidance and consistent enforcement, whereas the UK benefits from strong institutional oversight by the Information Commissioner's Office, supported by administrative penalties and criminal sanctions for data misuse (Data Protection Act 2018; ICLG, n.d.). Finally, in terms of digital hospital readiness, Malaysia has demonstrated strong policy commitment and investment in digital health initiatives but continues to experience uneven implementation and infrastructural constraints (Ministry of Health Malaysia, 2017; Budget 2024), while the United Kingdom reflects a higher level of regulatory maturity with clearer compliance standards that better support secure and trustworthy digital hospital systems.

RESULTS AND FINDINGS

Findings 1

Research Methodology

To ensure alignment with the study's focus on hospital digitalisation and data protection, this research adopts a hybrid methodology combining **doctrinal legal analysis** and **socio-legal inquiry**, with a comparative perspective focused specifically on healthcare law. The doctrinal analysis examines statutory provisions, regulations, and judicial precedents relevant to digital health, electronic medical records, and data protection in Malaysia and the United Kingdom, clarifying legislative intent and identifying gaps in legal safeguards. The socio-legal approach contextualizes these laws within the practical realities of hospital digitalisation, including privacy, security, and ethical issues, while comparative analysis evaluates Malaysia's legal frameworks against international benchmarks, particularly the UK GDPR, to propose targeted reforms in digital health governance.

This research adopts a hybrid methodological framework combining doctrinal legal analysis and socio-legal inquiry, complemented by comparative and interdisciplinary perspectives. The doctrinal component involves an in-depth examination of statutory provisions, subsidiary legislation, and judicial precedents to interpret how the law operates within specific domains data protection (Personal Data Protection Act 2010 This method is fundamental in clarifying legislative intent, identifying interpretive inconsistencies, and analyzing the evolving judicial attitudes that shape Malaysian jurisprudence (Chynoweth, 2008; Hutchinson, 2018).

The socio-legal method complements doctrinal analysis by contextualizing legal frameworks within social, technological, and economic realities. . Empirical data, secondary reports, and policy papers are examined to provide insight into how the law functions in practice — bridging the gap between *law in books* and *law in action* (Banakar & Travers, 2005).

The comparative legal dimension draws parallels with other common law jurisdictions such as the United Kingdom, to evaluate Malaysia's legal responses against international benchmarks.

Finally, the interdisciplinary method integrates perspectives from economics, sociology, information technology, and environmental science. This ensures a holistic analysis that goes beyond black-letter law and reflects the multifaceted challenges of modern regulation.

The analysis of digital hospitals and data protection in Malaysia and the United Kingdom can be illuminated through several jurisprudential theories. **Legal positivism** emphasizes the authority of enacted laws, as seen in Malaysia's *Medical Act 1971* and *Personal Data Protection Act 2010* (Act 611, 2010), and the UK's GDPR and Data Protection Act 2018, which provide formal frameworks for patient data protection and hospital operations (ICLG, n.d.). Complementing this, **natural law theory** highlights the ethical obligation to protect patient confidentiality, ensure safety, and promote equitable access to digital health technologies, guiding legislators to align laws with societal welfare (Fuller, 1964). **Legal realism** illustrates that practical outcomes of these laws depend on social and technological factors, such as the manual handling of 16,000 medical records daily at Hospital Kuala Lumpur or data breaches at Selayang Hospital, emphasizing the need for adaptable and context-sensitive regulations (Llewellyn, 1931; Humer & Finkle, 2014). **Critical Legal Studies (CLS)** offers a lens to examine structural inequalities, including how marginalized groups might face barriers in accessing digital healthcare (Unger, 1983), while **feminist jurisprudence** focuses on gendered dimensions, ensuring policies protect sensitive health information and provide equitable access to telemedicine services for women (Watson, 2022). Finally, **socio-legal theory** integrates social realities, demonstrating how public awareness, hospital workflows, and cultural factors affect compliance with laws like the PDPA and UK GDPR, bridging the gap between "law in books" and "law in action" (Banakar & Travers, 2005). Together, these theories provide a holistic framework to assess, refine, and advance the legal and ethical governance of digital hospitals in both Malaysia and the UK.

By linking doctrinal analysis to jurisprudential reflection, the research contributes to understanding not only *what the law is* but also *what the law ought to be* in a developing regulatory ecosystem like Malaysia's.

DISCUSSION

The advent of digital hospitals has significantly transformed healthcare delivery, improving efficiency, accuracy, and patient outcomes through the integration of electronic health records (EHRs), telemedicine, and automated clinical decision-making systems. Malaysia's first recognized digital hospital, **Prince Court Medical Centre**, achieved the **HIMSS Analytics Stage 6 certification** in 2016, demonstrating advanced adoption of electronic medical record systems (HIMSS Analytics, 2016). Such recognition highlights Malaysia's commitment to digital health innovation, aligning with global trends where hospitals increasingly rely on digital technologies to manage patient care and streamline operations.

However, the digitization of healthcare presents serious challenges, particularly regarding the **security and integrity of medical data**. Patient medical information is considered **highly valuable and sensitive**, often cited as being worth up to ten times more than a credit card number on the black market (Humer & Finkle, 2014). Unlike financial data, medical information contains immutable personal identifiers, medical histories, and genetic information that cannot be easily changed once exposed. Breaches of such data can

result in identity theft, fraudulent insurance claims, and other forms of abuse, which not only harm patients but also undermine trust in healthcare institutions (Why Medical Record, 2016). Reports in Malaysia show a **four-fold increase in personal data breach cases** in 2023 compared to the previous year, highlighting the urgent need for stronger regulatory frameworks (MalayMail, 2023). Similar incidents abroad, such as the 150,000-patient data breach in the United Kingdom caused by a software error, demonstrate that even developed healthcare systems are vulnerable to cyber threats (BBC News, 2018).

To mitigate these risks, **professional data governance** is indispensable. Professional data governance encompasses the implementation of policies, standards, and practices that ensure the **accuracy, security, and ethical use of medical data**. This includes structured protocols for data access, encryption, audit trails, employee training, and incident response strategies. By instituting governance frameworks, hospitals can **prevent unauthorized access, reduce the likelihood of data breaches, and ensure compliance with national and international data protection standards** (Gopal et al., 2019). Furthermore, proper governance empowers healthcare professionals to make informed clinical decisions, as reliable and secure data forms the backbone of effective medical judgment.

Malaysia currently lacks a **comprehensive regulatory framework** that explicitly defines sensitive health data and establishes standards for digital hospital operations. Drawing from the **General Data Protection Regulation (GDPR)**, Malaysia could develop legislation that specifies the definition of medical data, sets out clear consent procedures, mandates breach reporting, and enforces strict penalties for violations. Such regulation would ensure that hospitals adopt a standardized approach to **data privacy, patient autonomy, and cybersecurity**, enhancing both patient safety and institutional accountability.

Finally, while digital hospitals facilitate **E-health solutions, telemedicine, and automated diagnostics** (Patil et al., 2018), their full potential depends on a **robust combination of technology, professional governance, and regulatory oversight**. Hospitals that integrate these elements effectively can leverage digital systems not only for improved healthcare delivery but also to safeguard sensitive patient information in an increasingly interconnected and digital world.

CONCLUSION

It is evident that the healthcare legislation in Malaysia has gone through a passage of in which it has grown from through its legislation and regulations on basic human and the new technology development namely digital hospitals.

It is evident through the concerns of our Malaysian Health Minister Dr Zaliha Mustafa that digital records are vital for quick patient data access and sharing among government health care facilities as it reduces waiting and saves many lives.

The fact that our Hospital Kuala Lumpur (HKL), one of the country's largest and busiest hospitals, handles up to 16,000 medical records manually every day is shocking.

Although digitalization in hospital and healthcare services is not a panacea, but it provides important opportunities to increase access to care, cut costs, and enhance quality.

Digital health systems are emerging rapidly and involving a wide variety of stakeholders. For example, game and app developers with creative digital health ideas can face challenges in implementing digital health services at the interface between health care and individuals. In certain situations, indistinct legislation would be a concern.

It is evident that healthcare legislation in Malaysia has evolved significantly, reflecting the country's

progress from foundational medical laws to regulations accommodating emerging technologies, particularly digital hospitals. The emphasis by Malaysian Health Minister Dr. Zaliha Mustafa on digital records underscores their critical role in enabling rapid patient data access and secure sharing across government healthcare facilities, ultimately reducing waiting times and saving lives. The current manual handling of up to 16,000 medical records daily at Hospital Kuala Lumpur (HKL), one of Malaysia's largest hospitals, highlights the urgent need for broader digitalization.

Although digitalization in healthcare is not a complete solution, it offers substantial opportunities to enhance access to care, reduce costs, and improve the overall quality of services. The rapid emergence of digital health systems involves multiple stakeholders, including app and software developers, who face challenges in navigating the intersection of healthcare provision, patient rights, and regulatory compliance. Ambiguities in legislation may hinder the effective implementation of innovative digital health solutions, making it essential to develop clear, robust, and harmonized legal frameworks that protect patient data while fostering innovation.

Moving forward, Malaysia's healthcare system can benefit from continued legislative refinement, adoption of international best practices such as the UK GDPR, and targeted investments in digital infrastructure. By addressing both technological and legal challenges, Malaysia can establish a secure, efficient, and patient-centered digital health ecosystem that supports clinical decision-making, enhances operational efficiency, and strengthens public trust in healthcare services.

Acknowledgement

The authors would like to express their sincere gratitude to Management and Science University (MSU) for the continuous support, guidance, and resources provided throughout the course of this research. The encouragement and academic environment at MSU have been invaluable in the completion of this study.

REFERENCES*

Banakar, R., & Travers, M. (2005). *Theory and method in socio-legal research*. Hart Publishing.

BBC News. (2018, July 2). NHS data breach affects 150,000 patients in England. https://www.bbc.com/news/technology-44682369

Budget 2024. (2024). *Budget 2024 speech*. Ministry of Finance Malaysia. https://belanjawan.mof.gov.my/pdf/belanjawan2024/ucapan/ub24-BI.pdf

Chynoweth, P. (2008). Legal research. In *Advanced research methods in the built environment* (pp. 28–38). Wiley-Blackwell.

CodeBlue. (2023). Selayang Hospital EMR system not upgraded, manual processes causing delays. *CodeBlue*.

Data Protection Act 2018 (United Kingdom).

Deloitte. (2019). *2019 global health care outlook*. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-hc-outlook-2019.pdf

Digital health laws and regulations: United Kingdom. (n.d.). *International Comparative Legal Guides*. https://iclg.com/practice-areas/digital-health-laws-and-regulations/united-kingdom

Disch, W. (2016, August 11). How to use big data to improve patient engagement. http://data-informed.com/how-to-use-big-data-to-improve-patient-engagement/

Fuller, L. L. (1964). *The morality of law*.

Yale University Press.

Gopal, G., Suter-Crazzolara, C., Toldo, L., & Eberhardt, W. (2019). Digital transformation in healthcare – architectures of present and future information technologies. *Clinical Chemistry and Laboratory Medicine, 57*(3), 328–335. https://doi.org/10.1515/cclm-2018-0685

Hart, H. L. A. (1961). *The concept of law*. Oxford University Press.

HIMSS Analytics. (2016). *Stage 6 recognition: Prince Court Medical Centre*. Healthcare Information and Management Systems Society.

Humer, C., & Finkle, J. (2014, September 23). Your medical record is worth more to hackers than your credit card. *Reuters*. https://www.reuters.com/article/cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSL2N0RN13320140924

Hutchinson, T. (2018). *Researching and writing in law* (4th ed.). Thomson Reuters.

Kiliç, T. (2016). Digital hospital: An example of best practice. *International Journal of Health Services Research and Policy, 1*(2), 52–58. https://doi.org/10.23884/ijhsrp.2016.1.2.04

Liddell, K. (2021). Patient data ownership: Who owns your health? *Journal of Law and the Biosciences, 8*(2). https://pubmed.ncbi.nlm.nih.gov/34611493/

Malaysian Medical Council. (2011). *Confidentiality codes*.

Malaysia Ministry of Health. (2017). *Malaysian Health Data Warehouse (MyHDW) initiative*.

MalayMail. (2023, September 21). Report: Malaysia's data breach cases hit all-time high with four-fold increase recorded in 2023. https://www.malaymail.com/news/malaysia/2023/09/21/report-malaysias-data-breach-cases-hit-all-time-high-with-four-fold-increase-recorded-in-2023/92075

Patil, P., et al. (2018). International for digitalization in hospital. *International Journal of Computer Science and Mobile Applications, 6*(10), 13–16.

Personal Data Protection Act 2010 (Act 709, Malaysia).

Pramanik, P. K., Pal, S., & Mukhopadhyay, M. (2019). Healthcare big data. In *Advances in healthcare information systems and administration: Intelligent systems for healthcare management and delivery* (pp. 72–100). IGI Global. https://doi.org/10.4018/978-1-5225-7071-4.ch004

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (United Kingdom).

UK General Data Protection Regulation (UK GDPR).

Unger, R. M. (1983). The critical legal studies movement. *Harvard Law Review, 96*(3), 561–675.

Watson, A. (2022). *Legal transplants and comparative law: Theory and practice*. Routledge.

Why medical records are 10 times more valuable than credit card info. (2016). *CyberPolicy*. https://www.cyberpolicy.com/cybersecurity-education/why-medical-records-are-10-times-more-valuable-than-credit-card-info