



Chambers Global Practice Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Digital Healthcare 2021

Malaysia

Raja Eileen Soraya Raja Aman, Tong Lai Ling,
Joyce Teh and Charlaïne Adrienne Chin
Raja, Darryl & Loh

Law and Practice

Contributed by:

Raja Eileen Soraya Raja Aman, Tong Lai Ling, Joyce Teh
and Charlene Adrienne Chin
Raja, Darryl & Loh see p.16



CONTENTS

1. Digital Healthcare Overview	p.3	7. Internet of Medical Things	p.10
1.1 Difference between Digital Healthcare and Digital Medicine	p.3	7.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things	p.10
1.2 Regulatory Definition	p.3	8. 5G Networks	p.10
1.3 New Technologies	p.4	8.1 The Impact of 5G Networks on Digital Healthcare	p.10
1.4 Emerging Legal Issues	p.4	9. Data Use and Data Sharing	p.11
1.5 Impact of COVID-19	p.4	9.1 The Legal Relationship between Digital Healthcare and Personal Health Information	p.11
2. Digital Healthcare and Climate Change	p.5	10. AI and Machine Learning	p.12
2.1 Digital Healthcare and Public Health Dangers Related to Climate Change	p.5	10.1 The Utilisation of AI and Machine Learning in Digital Healthcare	p.12
3. Healthcare Regulatory Environment	p.5	11. Upgrading IT Infrastructure	p.12
3.1 Healthcare Regulatory Agencies	p.5	11.1 IT Upgrades for Digital Healthcare	p.12
3.2 Recent Regulatory Developments	p.6	11.2 Cloud Computing	p.13
3.3 Regulatory Enforcement	p.6	12. Intellectual Property	p.14
4. Non-healthcare Regulatory Agencies	p.7	12.1 Scope of Protection	p.14
4.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies	p.7	12.2 Research in Academic Institutions	p.14
5. Software as a Medical Device	p.7	12.3 Contracts and Collaborative Developments	p.14
5.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technology	p.7	13. Liability	p.14
6. Telehealth	p.8	13.1 Patient Care	p.14
6.1 Role of Telehealth in Healthcare	p.8	13.2 Commercial	p.15
6.2 Regulatory Environment	p.9	14. Hot Topics and Trends on the Horizon	p.15
6.3 Payment and Reimbursement	p.9	14.1 Hot Topics That May Impact Digital Healthcare in the Future	p.15

1. DIGITAL HEALTHCARE OVERVIEW

1.1 Difference between Digital Healthcare and Digital Medicine

Difference between Digital Healthcare and Digital Medicine

Unlike other jurisdictions which may distinguish between digital healthcare and digital medicine, whether from the perspective of the healthcare-provider, the patient or consumer, the regulatory framework or the technology, in Malaysia, the difference between digital healthcare and digital medicine is not clearly defined in any existing legislation.

Whether it is digital healthcare or digital medicine, the players in the digital healthcare industry will still have to navigate through the current Malaysian legislative and regulatory framework in undertaking such endeavours in Malaysia.

Technology Platforms That Collect and Store Data and Clinical Evidence Used in Patient Care

Jumping specifically into the interplay between technology platforms in healthcare or digital health systems that collect and store data for possible use as clinical evidence for the purposes of other future patient care, it should be borne in mind that consent of the individual patient will have to be obtained for any such data to be processed for this purpose, as there is no exception provided under the Personal Data Protection Act, 2010 and related regulations. (See **1.2 Regulatory Definition** for more details).

1.2 Regulatory Definition

Digital Health and Digital Medicine from a Regulatory Perspective

There is currently no specific legislative or regulatory framework in Malaysia that defines the terms “digital health” and “digital medicine”. In fact, Malaysia does not have specific legislation

for digital healthcare [including for telemedicine and artificial intelligence (AI)]. The Telemedicine Act, 1997, which was promulgated in 1997, never came into force. The lack of specific legislation should not, however, lead to the conclusion that digital healthcare products or solutions can be rolled out in Malaysia without the need to consider the impact of any current laws and regulations. The digital healthcare product, service or solution will need to be assessed to determine whether, depending on its form, contents and/or capabilities, among other features, existing legislative and regulatory requirements apply to that product, service or solution, as the case may be.

Aspects Subject to Existing Legislative and Regulatory Framework

In Malaysia, digital healthcare products or medical devices are primarily governed by the Malaysian Medical Device Act, 2012. Under this legislation, “medical device” means, among others, any instrument, apparatus, implement, machine, appliance, software, material or other similar or related article intended by the manufacturer to be used, alone or in combination, for human beings for the purpose of, among others, diagnosis, prevention, monitoring, treatment or alleviation of disease or injury or investigation, replacement or modification or support of the anatomy or of a physiological process.

Given the breadth of this definition, any software (and it can extend to similar or related technological offerings) that is capable of diagnosing, preventing, monitoring, treating or alleviating a disease or injury or investigating, replacing or modifying or supporting the anatomy or a physiological process would likely fall within the definition of “medical device” for the purpose of this legislation. If so, various provisions under this legislation relating to, among others, registration of the medical device will have to be adhered to prior to its roll-out into the Malaysian market.

In addition to the Medical Device Act, 2012, the existing healthcare-related legislation which may have an impact on digital health and digital medicine products, solutions and services include the Medical Act, 1971, the Dental Act, 1971, the Sale of Drugs Act, 1952, the Medicines (Advertisement and Sale) Act, 1956, the Optical Act, 1991, the Private Healthcare Facilities and Services Act, 1998, to name a few, and newer legislation such as the Traditional and Complementary Medicine Act, 2016 and the Allied Health Professions Act, 2016 (together with all their related regulations). Any solution in healthcare using technology or digital platforms, whether it is a healthcare product, solution or service, a pharmaceutical dispensary/sale-related solution or a digital service or solution which measures or scans any part of the human anatomy for the purposes of delivering healthcare products, services or solutions to a patient or customer, will still have to comply with the existing legislative and regulatory framework in Malaysia. It will, therefore, be necessary to conduct a regulatory compliance check of various aspects of these healthcare technologies or digital platforms and what they are capable of doing (such as diagnostics, monitoring, measurement and/or treatment capabilities).

Aspects Not Subject to Existing Regulatory Framework

What is clearly not regulated, under the current legislative and regulatory framework in Malaysia, is the specific choice of technology and related aspects.

1.3 New Technologies

Key Technologies Enabling New Capabilities in Digital Healthcare and Digital Medicine

Big data analytics, artificial intelligence, geographical information systems (GIS) and block-chains are utilised to manage high volumes of structured and unstructured data in the Malaysia Health Data Warehouse, which is part of the

MyDIGITAL initiative (see **3.2 Recent Regulatory Developments** for more details).

The Malaysia Health Data Warehouse is a national healthcare information-gathering and reporting system which seeks to cover all Government and private healthcare facilities and services and which enables users to capture, store and analyse health data in a centralised manner. See also **7.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things** and **10.1 The Utilisation of AI and Machine Learning in Digital Healthcare** for a detailed discussion on artificial intelligence and the internet of medical things.

1.4 Emerging Legal Issues

Emerging Legal Issues

In Malaysia, the lack of a defined regulatory framework for digital healthcare has resulted in uncertainty over what is and is not permitted.

For example, telemedicine is currently subjected to the existing healthcare framework with Acts of Parliament that go as far back as 1952. Telemedicine, as a part of digital healthcare, appears to be gaining traction. With the gain in popularity of telemedicine, ancillary legal issues are emerging relating to online-platform governance and accountability, such as the prescription of certain medicine and the promotion of medical services. These issues are being driven by the current COVID-19 pandemic and the aggressive marketing of the telemedicine platforms, coupled with the increasing concern by the regulators who are still operating under archaic statutory regimes.

1.5 Impact of COVID-19

Impact of COVID-19 in the Acceleration of Digital Adoption and Transformation in Malaysia

COVID-19 has accelerated digital adoption and transformation. It is used in the pandemic for

Contributed by: Raja Eileen Soraya Raja Aman, Tong Lai Ling, Joyce Teh and Charlene Adrienne Chin, Raja, Darryl & Loh

the entire spectrum of public health measures, from contact tracing, disease surveillance, diagnostics, reports, dashboards, hospital surge capacity (beds, ventilators, labs, PPE), strategic communications, drugs' trials, vaccine management, forecasting and modelling, virtual clinics and webinars. Digital healthcare or healthcare technology has basically been used both at the community level as well as for operational and strategic purposes. The "MySejahtera" application was developed to assist in the monitoring of the COVID-19 outbreak, as well as to provide pandemic-related information to the public such as an outbreak tracker, COVID-19 health guidelines, vaccination registration/information and information on healthcare facilities available. With regard to clinical care, the Ministry of Health signed a Memorandum of Understanding with a digital healthcare platform to establish a Virtual Health Advisory to provide the public with access to free consultations regarding COVID-19. Various public and private healthcare facilities were also constrained to establish their own teleconsultation services, primarily to ensure continuity in clinical care. Some healthcare facilities have entered into partnerships with digital healthcare platforms to provide home-assessments and virtual consultations, with a view to reducing the congestion at healthcare facilities during the pandemic.

2. DIGITAL HEALTHCARE AND CLIMATE CHANGE

2.1 Digital Healthcare and Public Health Dangers Related to Climate Change

Digital Healthcare in Addressing the Public Health Dangers Driven by Climate Change

Changes in climate and climate variability, particularly changes in weather extremes, affect the provision of clean air, water, food, shelter and security. The public-health dangers caused as a result of climate change include air pollution,

the spread of vector-borne and waterborne diseases, floods, mental health disorders and temperature extremes. Digital healthcare has been utilised in addressing these dangers through the dissemination of information, provision of access to healthcare to those who have been displaced and distribution of basic medical and hygiene kits to those in need.

Certain private digital healthcare platforms have provided medical and humanitarian assistance to Malaysians who have been affected by torrential rains and floods, particularly in areas with weaker health infrastructure. Through collaborations with pharmaceutical partners and healthcare practitioners, these digital platforms were able to provide virtual complimentary consultations to those who were affected as a result of waterborne diseases such as typhoid fever and cholera, as well as those with chronic medical conditions such as diabetes, hypertension and cardiac-related problems.

3. HEALTHCARE REGULATORY ENVIRONMENT

3.1 Healthcare Regulatory Agencies

Key Regulatory Agencies

The key regulatory agencies which play a role in digital healthcare and digital medicine include the Ministry of Health, the Medical Device Authority, the Medicine Advertisements Board of Malaysia and the National Pharmaceutical Regulatory Authority of Malaysia. From the perspective of digital healthcare and digital medicine:

- the Ministry of Health has an overall supervisory regulatory role with specific divisions dealing with the practice of medicine/dental, advertisements of medical services and products and the sale of pharmaceutical products

- that monitor digital healthcare platforms to ensure compliance with existing legislation;
- the Medical Device Authority is empowered under the Medical Device Act, 2012, to license and approve any digital health or digital medicine solutions and technologies (including technologies or devices which have diagnostics, consultancy and treatment capabilities, among others); and
 - the Medicine Advertisements Board of Malaysia is empowered under the Medicines (Advertisement and Sale) Act, 1956, to approve any advertisement that relates to the sale of medicine, among others, and which includes any online display.

The Ministry of Health, the Medical Device Authority and the Medicine Advertisements Board all have within their remit the regulation of various aspects of a digital healthcare, digital medicine or an e-wellness product, service or solution (depending on its form, contents and/or capabilities, among others), as discussed in **1. Digital Healthcare Overview.**

3.2 Recent Regulatory Developments

Regulatory Development in the Digital Space

The Economic Planning Unit of the Prime Minister's Department in Malaysia, on 19 February 2021, published the Malaysia Digital Economy Blueprint (Blueprint). The Blueprint sets out the Malaysian Government's MyDIGITAL initiative, which is a national initiative symbolising the aspirations of the Government to transform Malaysia successfully into a digitally driven, high-income nation and a regional leader in a digital economy. The Blueprint discusses the digital economy's contribution to the Malaysian economy and builds the foundation to drive digitalisation across Malaysia in many sectors, including, but not limited to, the healthcare services' sector. The MyDIGITAL initiative by the Government spans across three phases of implementation up to the year 2030. In terms of healthcare, the

initiative includes the development of a framework for rapid-growth adoption of technology for healthcare-related products and the acceleration of usage of the Malaysia Health Data Warehouse (MyHDW) with the inclusion of blockchain.

There has been, however, no new specific legislative or regulatory development introduced to date that has impacted digital healthcare or digital medicine.

3.3 Regulatory Enforcement

Regulatory Enforcement

Regulatory enforcement may take different approaches, depending on the alleged offence being committed and the applicable legislation. One key area is to ensure that activities undertaken by anyone in the digital healthcare industry in Malaysia, which can be said to be within the realms of the practice of medicine are not delegated to non-medical practitioners using these digital healthcare platforms or devices. Other areas for compliance include activities related to the prescription or dispensation/sale of certain pharmaceutical products through the digital platforms. These examples are not exhaustive and, as previously explained, much will depend on the digital healthcare product, solution or service being delivered.

The Private Healthcare Facilities and Services Act, 1998 gives extensive powers to officers from the Ministry of Health to investigate, raid, seize items and order facilities to stop operations if they are found to be acting contrary to the provisions of the Act. These acts of enforcement can be undertaken without notice. Sanctions include substantial fines and imprisonment.

It is recommended that each digital healthcare-provider keeps a checklist of compliance with all relevant Acts and regulations. If ever prosecution is threatened, representations can be made to the Ministry of Health or such other relevant min-

Contributed by: Raja Eileen Soraya Raja Aman, Tong Lai Ling, Joyce Teh and Charlene Adrienne Chin, Raja, Darryl & Loh

ister or regulatory authority and/or the Attorney General's Chambers; and if charges are professed, a defence will then need to be mounted in court.

4. NON-HEALTHCARE REGULATORY AGENCIES

4.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

Non-healthcare Regulatory Agencies

There are several non-healthcare regulatory agencies which may play a role in the development of medical technologies in the Malaysian landscape, including the Ministry of Science, Technology and Innovation (MOSTI), the Malaysian Communications and Multimedia Commission (MCMC) and the Malaysian Investment Development Authority (MIDA). From the perspective of digital healthcare and digital medicine:

- the Malaysian Communications and Multimedia Commission, created pursuant to the Malaysian Communications and Multimedia Commission Act, 1998, has extensive powers to regulate the communications and media industry, including powers to order internet service-providers to block websites to prevent the commission of an offence or the attempted commission of an offence; and
- the Ministry of Science, Technology and Innovation introduced the National Technology and Innovation Sandbox, which is a co-ordination centre that attempts to enable innovators and start-ups to stress-test their products, services, business models and delivery mechanisms with some relaxation from all or selected regulatory requirements and/or processes. Medical and Healthcare technology is an identified prioritised sector.

With regard to wellness, fitness and self-care, depending on the contents and capabilities of the solution through technology or various digital platforms, these may still be regulated by the current healthcare statutory framework. For example, any wellness, fitness and/or self-care platforms that relate to the provision of traditional and complementary medicine will also need to comply with the provisions of the Traditional and Complementary Medicine Act, 2016, and platforms that involve any allied healthcare worker will need to ensure compliance with the Allied Health Professions Act, 2016.

In addition, ministries such as the Ministry of Domestic Trade, Co-operatives and Consumerism have also issued guidelines which will have to be complied with by anyone undertaking a beauty centre which provides various beauty, wellness and/or aesthetics services (including slimming and laser treatments).

5. SOFTWARE AS A MEDICAL DEVICE

5.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technology

Regulatory Definition of Software as a Medical Device

As previously stated, under the Medical Device Act, 2012, the term "medical device" for the purposes of the legislation includes a software or other similar or related article intended by the manufacturer to be used, alone or in combination, for human beings for the purpose of, among others, diagnosis, prevention, monitoring, treatment or alleviation of disease or injury or investigation, replacement or modification or support of the anatomy or of a physiological process. Given the breadth of this definition, any software or application that is capable of any of

the foregoing would likely be a “medical device” for the purpose of the aforementioned Act.

Medical Device Authority

The regulatory authority is the Medical Device Authority, which is a federal statutory agency under the Ministry of Health to implement and enforce the Medical Device Act, 2012.

Categorisation of a Medical Device by Risk

Medical devices are generally categorised by risk associated with:

- the vulnerability of the human body;
- the technical design of the medical device; and
- the manufacture of the medical device.

The rules of classification are based on:

- the intended use;
- the duration of use (transient, short-term and long-term); and
- the part of the human body (non-invasive or invasive with respect to body orifices, surgically invasive interventions, central circulatory system, central nervous system).

A manufacturer is responsible for classifying its medical device - the classes of medical device range from Class A (low risk) to Class D (high risk).

Software Improvements on a Continuous Basis

The Medical Device Authority does not currently separately address the fact that software improvements are made on a continuous basis; thus, at the time of writing, it is not clear if conventional timeframes for approving a medical device could hold back device improvement and patient care.

Artificial Intelligence and Machine Learning

In light of the broad definition of “medical device”, as set out above, products that use artificial intelligence and machine learning are not more likely to meet the regulatory definition of medical device compared with another type of software. This will have to be assessed on a case-by-case basis.

There does not appear to be a difference in regulation between software that uses adaptive or continuous learning from artificial learning and machine learning compared with “locked” algorithms and software in software-based or software-enhanced devices, as both are treated in the same manner.

A challenge which companies from outside the healthcare industry face when offering software as a medical device technology is the potential gap in the knowledge and experience relating to the provision of healthcare. Such companies may have the technological ability and expertise to produce the medical device; however, the device may not include certain features which are considered indispensable by a healthcare service-provider or healthcare practitioner. It would, therefore, be prudent to explore collaborations between such companies and healthcare service-providers or healthcare practitioners.

6. TELEHEALTH

6.1 Role of Telehealth in Healthcare

Role of Telehealth in Healthcare

Telehealth may potentially serve as a primary care modality that provides access to healthcare to those who prefer not to have in-person consultations or are not able to do so. There is not, however, sufficient data to demonstrate the rate of conversion and hence, to confirm if telehealth is indeed playing this role in any significant manner.

Contributed by: Raja Eileen Soraya Raja Aman, Tong Lai Ling, Joyce Teh and Charlene Adrienne Chin, Raja, Darryl & Loh

In Malaysia, telehealth primarily encompasses digital healthcare monitoring, virtual consultations and dispensation/sale of medication. Based on the growth reported by certain digital platforms, virtual consultations, in particular, have seen a steep rise since the start of the Covid-19 pandemic. Anecdotal reports suggest that, during the lockdown in Malaysia in March 2020, private medical practitioners saw a drop in patient in-person visits by about 70%-80%. Patients, however, appear to have delayed their consultations and may not necessarily have chosen virtual consultation as an alternative. Internet connectivity, which is a pre-requisite to an established national telehealth network, is a main hindrance to patients embracing telehealth and remote healthcare, particularly in rural Malaysia. As the licensing of practitioners is tied to their place of practice, telehealth which crosses provincial, state and national borders would challenge the concept of where the “practice of medicine” occurs. There is, however, no guideline nor judicial precedent in Malaysia that would assist with this concern at this stage. Virtual hospitals, however, do not appear to have gained any traction in Malaysia at the time of writing.

6.2 Regulatory Environment

Acceleration of Telemedicine by the COVID-19 Pandemic

Malaysia passed the Telemedicine Act, 1997, in June 1997, but it never came into force and as such, has no force of law.

During the COVID-19 pandemic, and amidst calls for regulatory guidance for the provision of telehealth, the Malaysian Medical Council issued an Advisory on Virtual Consultations which was expressed as being applicable only during the COVID-19 pandemic.

There is a push for the Malaysian Medical Council to provide even clearer guidance to healthcare practitioners who have commenced tel-

emedicine consultations. The Ministry of Health has, in the meantime, been engaging with the relevant stakeholders to develop an Online Healthcare Services Regulatory Framework, with a view to rationalising the existing legal framework and providing clarity. It cannot, however, be said that regulatory barriers have been relaxed or removed, as the Ministry of Health has been actively monitoring digital healthcare-providers and active enforcement has been taken against some. Online platforms such as Zoom or Microsoft Teams are not specifically regulated, and there is no restriction on the use of platforms for telehealth at the time of writing. The appropriateness of the technology used is to be determined by the healthcare practitioners, as stated in the Advisory of the Malaysian Medical Council.

6.3 Payment and Reimbursement

Rules and Regulations on Payments for Telehealth Services

There are no express rules that regulate the fees for telehealth services in Malaysia. Section 108 and the Seventh Schedule of the Private Healthcare Facilities and Services (Private Hospitals and Other Private Healthcare Facilities) Regulations, 2006 regulate the fees for various procedures undertaken at private healthcare facilities. Consultation fees are provided under the Schedule. Arguably, the same consultation fee range would apply to telehealth consultations, whether it is the prescribed fee for general practitioners, the fee for initial specialist consultations and the fee for specialist follow-up consultations.

Further to this, paragraph 1.12 of the Malaysian Medical Council’s Code of Professional Conduct states that it would be improper or unreasonable or an unjustified demand or acceptance of professional fees from patients if the fees are contrary to the relevant schedules and provisions. Paragraph 4.10.3 of the Malaysian Medical Council’s Good Medical Practice states that

a doctor must charge reasonably. These general rules should apply to telehealth services.

7. INTERNET OF MEDICAL THINGS

7.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

Internet of Medical Things

The internet of medical things refers to a connected infrastructure consisting of medical devices which use embedded sensors, micro-processors and communication hardware to collect, process and send data acquired from patients. Specific applications include wearables, which monitor heart rates and blood pressure of patients and which send the monitored data to the patients' doctors.

Some of the technological developments that have enabled the internet of medical things include machine learning and artificial intelligence. For example, medical devices which are AI-enabled may be able to measure and analyse patient data remotely on a real-time basis.

The regulatory issues to look out for which may be relevant to connected and smart devices (such as hospital beds), wearables, implantable and data exchange with other devices and hospital networks will depend on the form they take and their contents and capabilities. See **1. Digital Healthcare Overview** for more details.

Security Risks

Potential security risks which arise with regard to the internet of medical things include situations where a device/wearable/implantable (Device) is hacked, resulting in the potential loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction of patient data residing in a Device.

When Devices are updated, it is crucial that the software/firmware update be encrypted (possibly in packets) to prevent hacking and interception. It is therefore important that the software/firmware update is secure and encrypted before it is uploaded on to the Device.

If the software/firmware update fails to be properly installed in a Device as a result of a hacking or interception event, there may be severe consequences, for example in a pacemaker. Issues of liability will need to be analysed primarily from the perspective of the party at fault and whether the alleged fault caused the harm alleged.

8. 5G NETWORKS

8.1 The Impact of 5G Networks on Digital Healthcare

5G Network and Digital Healthcare

5G is expected to transform the existing mobile network in Malaysia as more data is transferred via 5G at much faster speeds, reduced congestion and lower latency (ie, the delay before a transfer of data begins following an instruction).

As telehealth is the provision of healthcare services remotely by utilising telecommunication technologies, it is likely that 5G networks will increase the use of telehealth in Malaysia in light of the exponential increase in data-transfer speed. For example, in the case of telemedicine, 5G will enable better transmission of video/audio between doctors and patients, leading to a more efficient consultation, diagnosis and treatment experience.

With regard to the internet of things (IoT), it is expected that the much higher data-transfer speed will enable more IoT devices to be connected and share data amongst one another much faster than before. In the context of healthcare, this will mean, for example, that wearables

Contributed by: Raja Eileen Soraya Raja Aman, Tong Lai Ling, Joyce Teh and Charlene Adrienne Chin, Raja, Darryl & Loh

will be able to transmit data to a healthcare professional faster than before. The same applies to medical treatment in disaster areas and by first responders as the high data-transfer speed will translate to emergency services being provided much more quickly.

One of the commercial and contractual considerations healthcare institutions face in entering into arrangements with telecoms-providers to deploy and manage the 5G network is ensuring that such arrangements will enable them to make full use of the 5G network at a capped cost, instead of being charged on the basis of the amount of data downloaded or uploaded. Such healthcare institutions should also ensure that the telecoms-providers adhere to strict service levels in terms of 5G network availability to enable uninterrupted data transfer.

9. DATA USE AND DATA SHARING

9.1 The Legal Relationship between Digital Healthcare and Personal Health Information

Data Use and Data Sharing

Data protection is a key legal issue with regard to the sharing of personal health information in research and clinical settings, unless that personal health information is processed for research purposes and the results of the research are not made available in a form which identifies the data subject. The same legal framework, ie, the Personal Data Protection Act, 2010 regulates both data use and data sharing in Malaysia.

De-identification will alleviate, although not entirely remove, the risk of identifying the individual, as identifiers such as alphanumeric tags may still be present after de-identification. Data aggregation will also lessen the risk of certain personal health information being considered

personal health information if individuals are not identifiable following the data aggregation exercise.

When a wearable healthcare device sends data to healthcare and non-health entities, consent must be obtained upfront, by checking a box consenting to the processing of personal data in the manner described in a personal data protection notice.

The Private Healthcare Facilities and Services Act, 1998, makes it mandatory for written consent to be obtained for any invasive procedure. If such procedures are contemplated during a virtual consultation held with a view of securing consent, consent may be confirmed after a discussion by checking a consent box in a mobile application rather than obtaining a wet signature.

The essence of informed consent, however, remains. Any patient using digital healthcare solutions must be made aware of any added material risks that may be involved, including any risk or shortfall in the technology and any limitation related to virtual consults.

The obligation to ensure the protection of patients' personal data lies primarily with the healthcare practitioner. However, if there is a breach or unauthorised use or access to personal health information, one cannot discount liability being imposed on digital healthcare platforms as well.

10. AI AND MACHINE LEARNING

10.1 The Utilisation of AI and Machine Learning in Digital Healthcare

The Utilisation of AI and Machine Learning in Digital Healthcare

AI is both “artificial intelligence” and “augmented intelligence”, depending on which aspect of healthcare is in discussion. For example, it is more likely to be augmented intelligence in the case of precision surgical tools (which combine both human skills and augment machine intelligence for precision) and artificial intelligence when a healthcare mobile application is involved.

An aspect of data use and data sharing of personal health information which is relevant to providing training data for machine-learning algorithms is the requirement that such use and sharing is:

- for a lawful purpose directly related to an activity of a data user that is the entity which uses or has control over or authorises the use of the personal health information;
- necessary for or directly related to that purpose; and
- adequate but not excessive in relation to that purpose.

Some of the key roles that machine learning plays in digital healthcare are the analysis of medical records and medical images for diagnostic purposes and streamlining electronic record-keeping by storing records in a more organised manner. It is likely that the analysis of medical records and medical images poses the most risk to misuse or leak of sensitive data and cybersecurity attacks due to the storage of such data, unless regular penetration testing is carried out on the server to ensure the security of that data.

The strength of using a centralised electronic health record computer system is accessibility and convenience for a patient and a doctor. The weakness would, of course, be that if the centralised system is hacked, all of a patient’s records would be in jeopardy, hence, placing a considerable amount of pressure on the owner or operator of such a system to ensure that the security systems are robust. The Personal Data Protection Act, 2010 applies in the case of data use and data sharing in the machine-learning context. Under the Private Healthcare Facilities and Services (Private Hospitals and Other Private Healthcare Facilities) Regulations, 2006, the licensed holder and the person in charge of the private healthcare facilities shall be responsible to safeguard information in the patient’s medical record against loss, tampering or use by unauthorised persons.

Natural language processing, or NLP, is a segment of AI in which the machine seeks to understand and derive meaning from human language. NLP aims to simplify our lives by managing and automating smaller tasks first. Common-use scenarios are smart assistants such as Apple’s Siri, email filters, predictive text, and even urgency detection. Although no specific regulatory scheme is implicated, the product liability scheme set out in the Consumer Protection Act, 1999, may be relevant in the event of a failure in a common-use scenario except where that scenario relates to healthcare services provided or to be provided by healthcare professionals or healthcare facilities.

11. UPGRADING IT INFRASTRUCTURE

11.1 IT Upgrades for Digital Healthcare IT Upgrade for Digital Healthcare

Other than cloud servers, on-premises state of the art servers which are able to process infor-

Contributed by: Raja Eileen Soraya Raja Aman, Tong Lai Ling, Joyce Teh and Charlene Adrienne Chin, Raja, Darryl & Loh

mation at a much faster speed are required to support digital healthcare, especially in the fields of telehealth, machine learning, the internet of medical things and data transmission. Network security should also be upgraded, to support in particular the internet of things and data transmission. This goes hand in hand with enhanced encryption which facilitates data protection in the context of the internet of medical things where data is uploaded and downloaded between wearables and servers residing in healthcare institutions.

Healthcare institutions should also explore procuring AI-driven platforms with the capacity to analyse massive amounts of data which accelerates machine learning and which in turn encourages automation.

In addition, the IT infrastructure of healthcare institutions should be upgraded in relation to its internet connectivity to improve the audio and video quality of telehealth consultations. Virtual private networks could also be explored.

11.2 Cloud Computing

Cloud Computing

The increase of cloud computing in healthcare is generally driven by factors such as low capital investment costs (especially when compared with on-premise infrastructure) and consequently a reduced total cost of ownership, scalability (which results in high flexibility) and also high availability. A key legal concern in the context of healthcare is privacy and the protection of personal health information, as such information is stored off premises and likely to be in a location which is not under the control of the healthcare service-provider. Security is another key legal concern and the cloud service-provider must adhere to strict service levels in order to protect the personal health information from loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction

pursuant to the Personal Data Protection Act, 2010.

The best practices for green data centre use in Malaysia are encapsulated in the Technical Code for the Specification for Green Data Centres developed by the Malaysian Technical Standards Forum Berhad via its Technical Experts Group on Green Data Centres, under the supervision of the Green ICT Working Group, which outlines the best practices that data centres should adopt to achieve a sustainable industry. The aforementioned Technical Code was developed to provide the minimum requirements for green data centres for the purpose of establishing policies, systems and processes to improve the energy efficiency of data centres, at the same time reducing the carbon footprint of the industry.

When IT vendors outside the healthcare industry provide technology upgrades, there is a possibility of a gap between the understanding of those IT vendors and the needs of the healthcare industry. As such, IT vendors may only be able to provide generic technology upgrades instead of specific customised solutions.

When multiple IT vendors are involved in upgrade programmes, the best practices for vendor management would be to have one system integrator, who will be primarily contractually responsible for those upgrade programmes. That system integrator would then be responsible to manage and contract with the rest of the IT vendors. In the event that it is not possible to have such a system integrator, there will need to be a robust governing structure for the management of those vendors, such as putting in place a project steering committee.

12. INTELLECTUAL PROPERTY

12.1 Scope of Protection

Scope of Protection of the Intellectual Property

The scope of protection under patent and copyright in so far as it relates to digital health is the same as that afforded to inventions and works in any other field. There is no specific legislation for the protection of trade secrets in Malaysia, so it is possible to try to protect certain information as confidential information under common law and/or by way of a contract using non-disclosure agreements.

Compilation of data and databases may be eligible for protection under copyright by reason of the selection and arrangements of their contents, but not for the data or database per se. If the data or databases are under confidentiality obligations, the rules under trade secrets may apply.

Based on current legislation (and in the absence of any case law or judicial decisions to the contrary, as is currently the case) protection of patents and copyright in Malaysia appears to relate only to inventions or works that are human-made or at least human-directed. If the invention or work was created purely by AI without any human intervention or contribution, the current legislation does not recognise the AI as a valid or legal “inventor” or “author” of the invention or work and, as such, may not by that reason accord protection to the invention or work in question under the relevant existing intellectual property laws.

12.2 Research in Academic Institutions

Research Work in Academic Institutions

Generally, intellectual property rights can be allocated in any manner as may be agreed amongst the parties involved. In the absence of any such

agreement to the contrary, the following general rules would apply.

Based on current patent legislation in Malaysia, inventions that are created during the course of employment would belong to the employer and, therefore, if the physician/inventor is an employee of the university or healthcare institution, the rights to that invention would be deemed accrued to the university or healthcare institution, unless the employment agreement states otherwise. The same principle applies to private-sector technology companies; if the invention was created by an employee in the course of employment, it would belong to the employer. If a third-party contractor was engaged by the company to be involved in the development of a device or medical innovation, the rights to the invention will be deemed accrued to the company unless the agreement states otherwise. Similar principles apply for works protectable under copyright and industrial designs.

12.3 Contracts and Collaborative Developments

Contracts and Collaborative Developments

Given the deeming provisions relating to ownership of inventions or works made during the course of employment or under commission, if the inventor/author wishes to retain ownership or be recognised as a co-owner of the invention or work, clear provisions on ownership must be set out in the contractual agreement or collaborative arrangement.

13. LIABILITY

13.1 Patient Care

Liability in Patient Care

Hitherto, healthcare practitioners, healthcare providers and their employees would be primary defendants in civil suits which are premised upon medical negligence. However, data analytics, AI

Contributed by: Raja Eileen Soraya Raja Aman, Tong Lai Ling, Joyce Teh and Charlene Adrienne Chin, Raja, Darryl & Loh

and machine learning may challenge the existing convention and impose liability on various other parties in addition to healthcare practitioners, healthcare-providers and their employees.

The determination of liability is likely to be heavily dependent on the cause of the injury that is suffered and if the cause can be traced to the use of the data analytics, AI, machine learning and software. Any medical device used in the treatment of patients will need to be coupled with documented training and, possibly, accreditation of all potential users. Liability will depend largely on the reasonableness of the conduct and the sufficiency of the training. Bias in AI is not, however, an issue that can be easily addressed at this stage as there is insufficient applicable case law to assist.

13.2 Commercial

Third-Party Vendors

Third-party vendors' products or services could be a vector for cybersecurity attacks if those products are not encrypted or have not been properly virus-checked, making them more vulnerable to such attacks. In such an event, it is imperative to obtain the requisite product warranties and indemnities from those third-party vendors.

Consumer Protection

The Consumer Protection Act, 1999, is of general application to goods and services that are offered or supplied to one or more consumers, subject to the proviso provided in Section 2(2) which stipulates, among others, that the Act does not apply to healthcare services provided or to be provided by healthcare professionals or healthcare facilities.

Whilst the provision of healthcare services is precluded from its ambit, arguably, the Act may apply to producers and/or developers of digital health technologies which do not involve the services of a healthcare practitioner or healthcare facility. Such scenarios may include complex and innovative AI systems, particularly those which use software based on self-learning algorithms.

Ultimately, the exposure to liability under the Act is product-dependent and, to date, has yet to be tested in the Malaysian Courts. Understanding the applicable digital health technology-based risks, how they are likely to be assessed under the current legal and regulatory framework and how this might change, is therefore key to any organisation thinking of implementing digital health technology.

14. HOT TOPICS AND TRENDS ON THE HORIZON

14.1 Hot Topics That May Impact Digital Healthcare in the Future

Artificial intelligence and predictive healthcare appear to be a given in the near future. Digital platforms are shifting towards predictive healthcare solutions, such as wearables with tracking functions and mental health predictive platforms. Legal issues that may arise would likely revolve around liability of practitioners monitoring data in the event of missed diagnoses, data security and the establishment of doctor-patient relationships.

Contributed by: Raja Eileen Soraya Raja Aman, Tong Lai Ling, Joyce Teh and Charlene Adrienne Chin, Raja, Darryl & Loh

Raja, Darryl & Loh has a sizeable and dedicated medical and healthcare law practice group, which started more than 25 years ago. The firm's courtroom experience is extensive and the firm's lawyers are regularly involved in trials and appeals involving healthcare practitioners and hospitals. The numerous cases that the firm has handled, both in the courts and before tribunals, include cases involving allegations of misdiagnosis, surgical mishaps, delayed treatment, the alleged use of defective equipment/devices and the use of controversial drugs. Raja, Darryl & Loh is also constantly involved in matters pertaining to professional ethics, representing healthcare practitioners in disciplinary

inquiries held by the Malaysian Medical Council and the Malaysian Dental Council, established under the Ministry of Health. The firm's practice includes advising clients on legal developments as well as compliance with legislation relating to this industry (this includes representations to regulators and support and representation if enforcement proceedings are initiated or contemplated by the regulators). The commercial aspects of healthcare practice are not ignored. The firm reviews and drafts documents such as by-laws, forms relating to the various operations of a hospital and the practice of healthcare practitioners and various agreements relating to healthcare services and supplies.

AUTHORS



Raja Eileen Soraya Raja Aman was admitted to the Malaysian Bar in 1997 and, currently focusing on medico-legal cases, has a formidable reputation for her considerable knowledge of

medical law, having acted for medical and dental practitioners for over 20 years, and leads the firm's healthcare practice. Eileen's long-standing court experience and dealings with healthcare practitioners and regulators have enabled her to provide strategic advice on innovation and the digitalisation of healthcare services. She is the immediate past president of the Medico-Legal Society of Malaysia and is currently on the Executive Committee of the Medico-Legal Society of Malaysia.



Tong Lai Ling has almost 30 years' practice in Malaysia and New Zealand, and spearheads the firm's technology, multi-media and telecommunications (TMT) practice. Her capabilities

in this sector have led to her being recognised in industry-related publications. Lai Ling advises on wide-ranging present-day technology subjects, including software development, maintenance/support services, outsourcing, cloud services, cyberlaws, personal data protection, privacy policies, artificial intelligence and the internet of things. She recently advised an artificial intelligence company on Malaysian data protection issues.

Contributed by: Raja Eileen Soraya Raja Aman, Tong Lai Ling, Joyce Teh and Charlene Adrienne Chin, Raja, Darryl & Loh



Joyce Teh was called to the Malaysian Bar in 1999 and has extensive experience in corporate, commercial and regulatory matters affecting the healthcare and pharmaceutical

industries. Her work involves negotiation, documentation and advice. Aspects of these matters that she has handled and advised on include the management and operations of healthcare facilities, the practice of tele-medicine and tele-nursing, healthcare solutions and the regulatory requirements affecting medical devices, to name a few.



Charlene Adrienne Chin was called to the Malaysian Bar in 2012 and since then her practice has focused on medico-legal cases, representing medical and dental practitioners in the

courts, as well as in disciplinary inquiries before the Malaysian Medical Council. She regularly conducts seminars on issues of interest relating to healthcare, such as the role of artificial intelligence in healthcare. Charlene is currently on the Executive Committee of the Medico-Legal Society of Malaysia.

Raja, Darryl & Loh

Level 25 and 26 Menara Hong Leong
No 6 Jalan Damanlela
Bukit Damansara
50490
Kuala Lumpur
MALAYSIA

Tel: +3 2632 9999
Fax: +3 2632 9850
Email: joyceteh@rdl.com.my
Web: www.rajadarrylloh.com



RAJA, DARRYL & LOH
advocates and solicitors