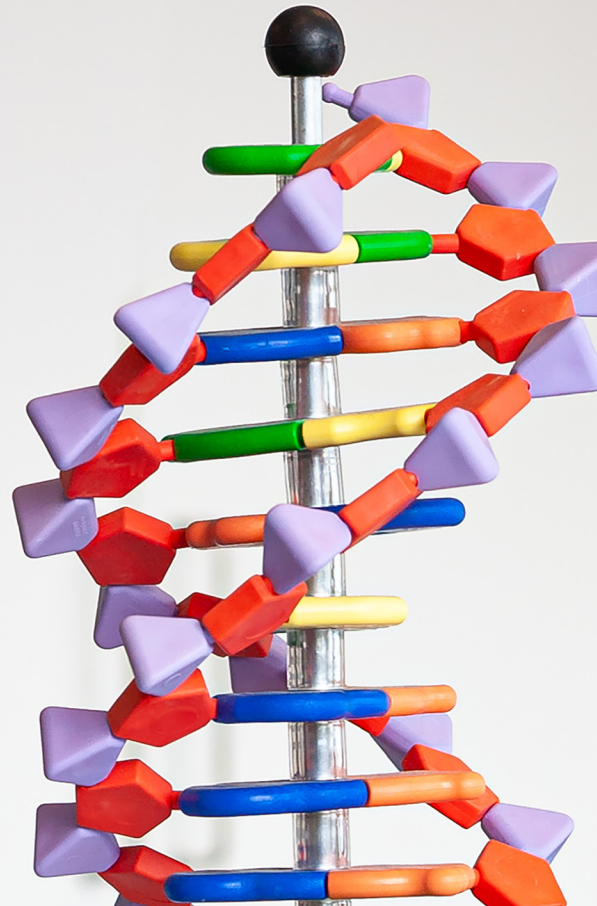

CHAMBERS GLOBAL PRACTICE GUIDES

Digital Healthcare 2023

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

Japan: Law & Practice

Junichi Kondo, Yasufumi Shiroyama,
Hiroshi Ishihara
and Masayuki Yamanouchi
Anderson Mori & Tomotsune



JAPAN

Law and Practice

Contributed by:

Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi

Anderson Mori & Tomotsune



Contents

1. Digital Healthcare Overview p.6

- 1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics p.6
- 1.2 Regulatory Definition p.6
- 1.3 New Technologies p.7
- 1.4 Emerging Legal Issues p.7
- 1.5 Impact of COVID-19 p.7

2. Healthcare Regulatory Environment p.7

- 2.1 Healthcare Regulatory Agencies p.7
- 2.2 Recent Regulatory Developments p.8
- 2.3 Regulatory Enforcement p.9

3. Non-healthcare Regulatory Agencies p.9

- 3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies p.9

4. Preventative Healthcare p.10

- 4.1 Preventative Versus Diagnostic Healthcare p.10
- 4.2 Increased Preventative Healthcare p.10
- 4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information p.11
- 4.4 Regulatory Developments p.11
- 4.5 Challenges Created by the Role of Non-healthcare Companies p.11

5. Wearables, Implantable and Digestibles Healthcare Technologies p.11

- 5.1 Internet of Medical Things and Connected Device Environment p.11
- 5.2 Legal Implications p.11
- 5.3 Cybersecurity and Data Protection p.12
- 5.4 Proposed Regulatory Developments p.13

6. Software as a Medical Device p.13

- 6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies p.13

7. Telehealth p.14

- 7.1 Role of Telehealth in Healthcare p.14
- 7.2 Regulatory Environment p.15
- 7.3 Payment and Reimbursement p.16

8. Internet of Medical Things p.17

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things p.17

9. 5G Networks p.17

9.1 The Impact of 5G Networks on Digital Healthcare p.17

10. Data Use and Data Sharing p.18

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information p.18

11. AI and Machine Learning p.19

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare p.19

11.2 AI and Machine Learning Data Under Privacy Regulations p.20

12. Healthcare Companies p.21

12.1 Legal Issues Facing Healthcare Companies p.21

13. Upgrading IT Infrastructure p.21

13.1 IT Upgrades for Digital Healthcare p.21

13.2 Data Management and Regulatory Impact p.22

14. Intellectual Property p.23

14.1 Scope of Protection p.23

14.2 Advantages and Disadvantages of Protections p.23

14.3 Licensing Structures p.24

14.4 Research in Academic Institutions p.24

14.5 Contracts and Collaborative Developments p.24

15. Liability p.24

15.1 Patient Care p.24

15.2 Commercial p.25

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

Anderson Mori & Tomotsune is a large, international Japanese law firm. The firm is known for its long history of advising overseas companies doing business in Japan and in cross-border transactions. The main office in Tokyo is supported by offices across Japan, China and the South-East Asian region. Anderson Mori & Tomotsune has considerable experience in matters relating to the life sciences field, including expertise in licensing, regulatory, intellectual property and corporate transactions such as

M&A and venture investments. The firm works with increasingly diversified international and Japanese-based healthcare companies, including pharmaceutical manufacturers, medical device manufacturers, distributors and e-health providers. The team, which consists of about ten partners and 20 associates, provides comprehensive advice from the set-up of a Japanese entity to all stages of the product life cycle and helps clients to navigate a broad range of regulatory matters.

Authors



Junichi Kondo is a partner at Anderson Mori & Tomotsune. His practice focuses on corporate, M&A and regulatory affairs involving the pharmaceutical and medical

devices industries. He regularly advises both local and foreign clients on M&A of listed and unlisted businesses and joint ventures. He also regularly provides advice on general corporate and commercial matters and regulatory affairs, including licensing, dealings with healthcare professionals, labelling and promotion, off-label use and adverse event reporting. He is a member of the Dai-ni Tokyo Bar Association (Japan) and admitted to the New York Bar. He is widely published in the field of life sciences.



Yasufumi Shiroyama is a partner at Anderson Mori & Tomotsune. He has focused on global and domestic dispute resolution of intellectual properties in various forms, including patent and

trade secrets, as well as having advised on transaction and regulatory matters in relation to life sciences and other technologies. In addition, he has taught at the University of Tokyo, School of Law since 2004 and was a chairperson of the JFBA Committee on Intellectual Property Rights in 2017–18.

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune



Hiroshi Ishihara is a co-head of the healthcare, pharmaceutical and life sciences department at Anderson Mori & Tomotsune. In his practice in the life sciences area, he handles commercial transactions, such as M&A of pharmaceutical companies and licence agreements. He also advises clients on regulations related to drugs, medical devices and regenerative medicine. He is an adviser of the Medical Affairs Study Group of the Japan Pharmaceutical Industry Legal Affairs Association. Hiroshi is a qualified Japanese lawyer (bengoshi) as well as a qualified lawyer in New York and California.



Masayuki Yamanouchi is a partner at Anderson Mori & Tomotsune. He holds a Master's degree in science and has been engaged in various matters involving technology issues. His main focus is on the pharmaceutical industry, and he has advised both domestic and foreign clients on pharmaceutical regulations and has represented clients in patent-infringement actions, as well as licensing negotiations, joint-development projects and technology-transfer projects. He also has expertise in AI and big data-related technologies applied in medical services and products. Masayuki is a member of the Dai-ni Tokyo Bar Association (Japan) and admitted to the New York Bar.

Anderson Mori & Tomotsune

Otemachi Park Building
1-1-1 Otemachi
Chiyoda-ku
Tokyo 100-8136
Japan

Tel: +81 3 6775 1000
Email: inquiry@amt-law.com
Web: www.amt-law.com/en

**ANDERSON
MŌRI &
TOMOTSUNE**

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Definitions of Digital Healthcare and Digital Medicine

While Japanese law does not provide formal definitions of digital healthcare and digital medicine, there is a difference in those terms based on whether a product constitutes a “pharmaceutical” or a “medical device” under the Securing Quality, Efficacy and Safety of Products including Pharmaceuticals and Medical Devices Act (the “Pharmaceuticals Act”). Digital medicine may be viewed as relating to products that have been approved by the relevant authorities in Japan, such as the Ministry of Health, Labour and Welfare (MHLW), as a pharmaceutical or medical device, while digital healthcare may be viewed more broadly as relating to those products and services that do not constitute pharmaceuticals or medical devices and, therefore, do not require approval from the MHLW.

Difference From the Regulatory Perspective

The aforementioned differences are important because if a certain product constitutes a pharmaceutical or medical device under the Pharmaceuticals Act, the provider of that product must obtain the relevant licence, such as a marketing licence, a manufacturing licence and/or a distribution licence, and must also obtain marketing authorisation, certification or notification for the product in question.

Difference From the Patient’s/Consumer’s Perspective

From a patient’s perspective, if a doctor prescribes a pharmaceutical item at a medical institution, the patient’s cost for that pharmaceutical will be covered by national health insurance, and the patient will be required to pay only a portion

of the cost of that pharmaceutical. By contrast, if a digital healthcare product does not constitute a pharmaceutical item, the consumer must pay the full price of the product to the provider.

Determination of a Medical Device

Sometimes, it can be difficult to determine whether a certain product, such as a medical-device program, may be categorised as a medical device; as such, the MHLW issued the Guideline Concerning the Determination of Software as a Medical Device on 31 March 2021 (amended on 31 March 2023; the “SaMD Guideline”).

The SaMD Guideline clarified that a program that records, stores and displays personal health data for the purpose of a user (ie, a patient) monitoring their own health information does not constitute a medical-device program. By contrast, a program that is intended to diagnose, treat or prevent a disease is a medical-device program.

1.2 Regulatory Definition

Definitions and Regulations Under the Pharmaceuticals Act

As previously stated, Japanese law, including the Pharmaceuticals Act, does not provide formal definitions of digital healthcare and digital medicine.

However, the Pharmaceuticals Act contains definitions of “pharmaceutical” and “medical device,” which include medical-device programs.

In general, a product or instrument (including a computer program) that is intended for use in the diagnosis, treatment or prevention of disease in humans would constitute a “pharmaceutical” or “medical device” under Article 2, Items 1 and 4 of the Pharmaceuticals Act.

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

Thus, if a digital medicine product is classified as a pharmaceutical or medical device under the Pharmaceuticals Act, that product would be subject to the relevant regulations under that Act. However, if a digital medicine product or a digital healthcare product is not classified as a pharmaceutical or medical device under the Pharmaceuticals Act, that product would not be subject to that Act and only the general regulations relating to a general consumer product would apply.

1.3 New Technologies Use of Internet and Artificial Intelligence

Technologies using the internet and artificial intelligence (AI) have been adopted in digital healthcare products and medical device programs.

There are many digital healthcare products, such as applications for smartphones, that use the internet to transmit healthcare information among users.

Also, some medical device programs adopt AI for their functions to enhance their effects, such as diagnosis of a certain disease.

1.4 Emerging Legal Issues From Face-to-Face to Online

Due to new technologies, medical treatment and medication counselling may be conducted remotely by using information communications equipment. However, medical treatment and medication counselling have traditionally been conducted on a face-to-face basis, so the existing regulations had to be amended to regulate remote medical treatment and remote medication counselling appropriately. In this regard, the MHLW issued Guidelines for Appropriate Performance of Online Medical Treatment, dated March 2018 (amended in March 2023). Also, the

Pharmaceuticals Act was amended as of September 2020 to allow online medication counselling under certain conditions.

1.5 Impact of COVID-19 Online Medical Treatment and Medication Counselling

Due to the spread of COVID-19, the MHLW temporarily relaxed regulations regarding online medical treatment and online medication counselling on 10 April 2020.

Accordingly, under certain circumstances, a doctor may conduct a patient's first medical examination remotely and provide online medical treatment to that patient using information communications equipment.

Also, under certain circumstances, a pharmacist may conduct online medication counselling by telephone or through information communications equipment.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies Business Licences and Marketing Authorisation

As a general rule under the Pharmaceuticals Act, any person intending to market a medicinal product must have a business licence and obtain a marketing authorisation, certification or notification, depending on the risk classification for the product.

The MHLW has primary jurisdiction over matters concerning pharmaceuticals, medical devices, medical treatment, health insurance and other healthcare matters, including matters in the digital health sector. Authority over matters concern-

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

ing clinical trials, authorisations, registrations and post-marketing safety measures of pharmaceuticals and medical devices is delegated from the MHLW to the Pharmaceuticals and Medical Devices Agency (PMDA), an organisation established under the Law for the Pharmaceuticals and Medical Devices Agency. Furthermore, the granting of business licences that are required for the manufacture, marketing or sales of pharmaceuticals and medical devices, and the monitoring activities in relation to those licences, including violation of advertising regulations, is partially delegated to local governments.

In brief, the procedure for obtaining marketing authorisations for medicinal products is as follows.

Clinical trials must be performed to collect data that is necessary for the application. In essence, clinical trials performed prior to the application include:

- Phase I (for a small number of healthy adults);
- Phase II (for a small number of patients); and
- Phase III (for a large number of patients).

After clinical trials, any person intending to market a medicinal product must file an application with the PMDA for approval to market that product. The PMDA reviews and examines the application and reports the results of its review to the Minister. The Minister then decides whether to grant the approval to market the product, based on the report of the PMDA.

Reimbursements Under the National Health Insurance System

The National Health Insurance System (NHIS) is a public healthcare system that covers the entire country. Under the NHIS, everyone in the country is, in principle, entitled to all types of medical

care services (including medical treatments and drugs) provided by medical institutions. Patients receive treatment at a medical institution and pay a portion (10% to 30%) of the cost of treatment at that medical institution. The remaining cost is billed to the assessment and payment agency, which reimburses the medical institution from the insurance premiums collected from the insured by the health insurance association, with the government covering any deficit.

The MHLW Welfare Ordinance prescribes the coverage by the NHIS for medical examinations, diagnoses or treatment and usage of pharmaceuticals and medical devices, including digital health products or services. Insurance reimbursement for medical devices varies, depending on the category of the device. For example, the cost of certain products, primarily disposable products, is specifically reimbursed as for pharmaceuticals. More commonly, however, the cost of the medical device is included in the medical diagnosis or treatment fee. For example, the use of software that processes image data of the human body taken by an imaging device is assessed as a technical fee in connection with a medical diagnosis. In other words, insurance reimbursement is provided for the act of diagnosis using specific software, not for the purchase or payment of a service fee for the software. Insurance reimbursement is also available for online medical treatment.

2.2 Recent Regulatory Developments Software as a Medical Device (SaMD)

Whether certain software is regulated as a medical device under the Pharmaceuticals Act is often a nuanced question. The SaMD Guideline is the latest guideline on whether certain software should be regulated as a medical device under the Pharmaceuticals Act, and indicates how to determine whether a software is deemed

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi, Anderson Mori & Tomotsune

a medical device. See **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies** for details.

Telemedicine

The provision of medical diagnoses over the telephone, by video or using other online tools (online medical treatment) is becoming more common in Japan. However, the Medical Practitioners' Act prohibits doctors from providing a diagnosis without examining a patient. Thus, the issues of whether an online examination may be construed as the examination required under the Medical Practitioners' Act, and of the extent to which an online examination is permitted, are controversial. The MHLW has been accepting online medical treatment, but with certain requirements, such as that the initial medical examination be held face to face.

In 2020, however, the MHLW issued Temporary and Exceptional Measures for Medical Treatment Using Telephones and Other Communication Tools Under the Spread of the COVID-19 Infection, which temporarily permitted the online performance of a patient's initial medical examination. Now, a patient may receive medical treatment online even if they have never been examined at a hospital for the specific disease or symptom. See **7.2 Regulatory Environment** for details.

2.3 Regulatory Enforcement

The MHLW, and prefectural governments as delegated by the MHLW, have vast authority in enforcing the regulations. That authority includes the ability to issue various administrative orders against regulatory violations, such as:

- a revocation of a marketing authorisation and/or business licence;
- a business suspension order;

- a temporary suspension of sales and disposal of stocks; or
- a recall order.

Certain violations of the Pharmaceuticals Act – such as violation of administrative orders, the sale of unauthorised drugs or medical devices and off-label promotion – are also subject to criminal penalties.

Regulators use these administrative orders and criminal penalties, but sometimes only administrative guidance, based on the severity of the violation and the risk to national health. There is no other significant trend or tendency in regulatory enforcement.

3. Non-healthcare Regulatory Agencies

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

Whether a certain digital health product or service is regulated by the Pharmaceuticals Act, the Medical Practitioners' Act or the Medical Care Act makes a substantial difference. Once the relevant product or service is determined as falling outside the healthcare regime, the applicable regulations are significantly less stringent than the laws described above, though there are still some notable regulations.

The Act Against Unjustifiable Premiums and Misleading Representations, administered by the Consumers Affairs Agency, governs all consumer products, including digital health products and services marketed towards consumers. The Act prohibits any representation in which the quality of a product or service is portrayed as being significantly superior to the quality of the

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi, Anderson Mori & Tomotsune

actual product or service, and any representation regarding price or any other term of a product or service that could be misunderstood to be significantly more advantageous than the term of the actual product or service. Medical devices and other products governed by the Pharmaceuticals Act are also governed by this Act, but in most cases the promotion and advertising rules under the Pharmaceuticals Act are stricter than the corresponding rules under the Act Against Unjustifiable Premiums and Misleading Representations.

Further, a health-related product or service that would, by its nature, not be regulated as a medical device or a medical service may be regulated as such if an advertisement, sales promotion or other communication portrays the product or service as applicable for use in diagnosis, treatment or prevention of diseases. In this respect, the Pharmaceuticals Act, the Medical Practitioners' Act and the Medical Care Act limit advertisements and other communications regarding non-medical devices and services.

The Electric Appliances Safety Act may apply to some categories of electrical appliances. Manufacturing or importing those electric appliances requires notification to the Ministry of Economy, Trade and Industry, and the products must conform to designated technical standards.

Privacy is one of the most crucial issues relating to digital health-related services. The Consumer Affairs Agency also plays an administrative role in the privacy regime. See **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information** for details.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

The Pharmaceuticals Act defines a medical device as an instrument that is intended for use in the “diagnosis”, “treatment” or “prevention” of disease. Similarly, an item that is intended for use in the “diagnosis”, “treatment” or “prevention” of disease can be categorised as a pharmaceutical under the Act. Therefore, when developing an instrument or an item that can be used to prevent disease, it should be carefully determined whether the instrument or item falls within the category of a medical device or a pharmaceutical, which are subject to the Pharmaceuticals Act.

Also, only a medical practitioner may engage in medical practices under the Medical Practitioners' Act. Thus, if a certain act involves a medical intervention, such as surgery, it cannot be performed via a computer or by a layperson – only by a medical practitioner.

4.2 Increased Preventative Healthcare

Due to the increasing cost of medical care in Japan, the Japanese government, as well as private enterprises, are focusing more on measures to help people live healthy lives and prevent early onset of serious diseases. While developing pharmaceuticals requires enormous amounts of money and time, developing an instrument or software that can promote better health requires fewer resources. Therefore, many start-up companies and traditional companies, whose core business is not healthcare, are now entering the healthcare sector by developing instruments or software that can be used for preventative medicine.

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Under the Act on the Protection of Personal Information (APPI), medical information is classified as “special care-required personal information”, and care must be taken when handling such information. In order to acquire special care-required personal information, it is necessary to obtain the prior consent of the individual concerned, except for certain exceptions. Fitness and wellness information not classified as special care-required personal information can be acquired without the prior consent of the individual concerned. If the information is a combination of medical information and fitness and wellness information, the entire information would be classified as special care-required personal information. There have been no court precedents that have explicitly ruled on the handling of such combined information.

4.4 Regulatory Developments

As it is often difficult to differentiate between a software program that should be categorised as a medical device and one that is not a medical device, the authorities are developing a guideline and a list of examples to help a company that develops such a program determine whether its software program should be categorised as a medical device or not.

For example, a program to be used personally at home to record an individual’s healthcare status for fitness purposes is not categorised as a medical device, so it is not subject to the Pharmaceuticals Act.

4.5 Challenges Created by the Role of Non-healthcare Companies

As pharmaceutical and medical devices are highly regulated by the Pharmaceuticals Act and

other relevant regulations, it is often a challenge for a company that is new to the healthcare business. Such companies tend to join forces with a traditional healthcare company that has already obtained the necessary licences and approvals. Alternatively, a new entrant first develops a device or product that is not categorised as a medical device or a pharmaceutical so that they do not have to obtain and maintain the requisite licences or approvals, which tend to incur substantial costs and time.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

The internet of medical things (IoMT) and connected devices have completely changed the medical scene. They are extremely useful for in-hospital use. Radio frequency identification attached to specimens such as blood or urine samples are now indispensable for preventing mix-ups. A recently developed bed can monitor the patient’s vital signs and transmit the data to the hospital’s central computer system. These devices are, however, most notable for in-home use. Wearable devices enable continuous and real-time monitoring of outpatients. One Japanese pharmaceutical company has developed a drug with a microsensor to enable monitoring of the patient’s compliance with dosing instructions.

5.2 Legal Implications

There is no specific legislation or other rules governing liability in the case of health injury arising from IoMT or connected devices malfunctions. There has been no case law establishing any specific rule for such liability, either.

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

The Product Liability Act (PLA) governs product liability litigation, along with the Civil Code. The liability under the PLA can be regarded as “strict” liability as, by replacing “negligence” with the existence of a “defect,” victims are not required to prove the negligence of the manufacturer. Nevertheless, victims still have to prove the defect and the other conditions for tortious liability (namely, the existence of damage and the causation between defects in the product and the damage) to claim the damage under the PLA.

A defect is defined as a lack of safety that the product should ordinarily provide, taking the following into account:

- the nature of the product;
- the ordinarily foreseeable manner of use of the product;
- the time when the manufacturer delivered the product; and
- other circumstances concerning the product.

The claimant bears the burden of this proof under the PLA. However, a court may lower the burden of proof regarding the existence of a defect, depending on the parties involved (eg, in the instance of a consumer acting against a large corporation), the nature of the product (such as the complex operational functions of a product) and the ordinarily foreseeable manner of use of a product.

Under the PLA, the manufacturer will be exempted from product liability if it proves that the defect in the product could not have been discovered given the state of scientific or technical knowledge at the time the manufacturer delivered the product (PLA Article 4).

5.3 Cybersecurity and Data Protection

The number of cyber-attacks against the healthcare industry has increased significantly. The Japanese government has designated the healthcare industry as one of the 14 important sectors that require elaborate countermeasures to combat cyber-attacks swiftly and efficiently.

There is no specific legislation or rules governing cybersecurity issues concerning IoT or connected devices malfunctions. However, the MHLW, the Ministry of Economy, Trade and Industry and the Ministry of Internal Affairs and Communications have introduced two guidelines on health information at large, namely:

- the Safety Management Guideline for Providers of Information Systems and Services that Handle Medical Information; and
- the Guideline on Safety Management of Medical Information Systems.

The latter provides guidance for medical institutions and applies to information created or recorded by healthcare providers.

The Guideline requires the preparation of the following:

- internal standard operating procedures for safety management;
- the establishment of committees for management and incident response;
- the implementation of staff training and incident reporting and responding standards; and
- measures to prevent eavesdropping, falsification or security breaches when exchanging information with outside parties via the network.

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

The Guideline also contains a specific checklist of cybersecurity measures that should be employed by medical institutions.

The Safety Management Guideline for Providers of Information Systems and Services that Handle Medical Information contains guidance for providers that supply medical information systems and resources and the services necessary for those medical information systems, and for providers that receive medical information from medical institutions based on the instructions of patients, including:

- providers of applications (“application service providers/service as software”);
- platforms;
- infrastructure (“infrastructure as a service”); and
- communication lines (“Providers”).

The Guideline sets out specific and detailed guidance on the recommended practices to be adopted by the Providers, such as measures against ransomware, and also requires Providers to obtain a privacy mark or an information security management system certificate. In addition, the Guideline provides detailed requirements regarding the risk management process (ie, risk assessment, risk analysis, risk management and risk communication) to be followed by the Providers.

5.4 Proposed Regulatory Developments

The Guideline on Safety Management of Medical Information Systems was updated in January 2021, and the Safety Management Guideline for Providers of Information Systems and Services that Handle Medical Information was updated in August 2020. Since then, there has been no notable change or proposed change in the regulations or guidance.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Legislation Framework

There is no specific legislation for the digital health sector, including software as a medical device (SaMD). Rather, existing legislative schemes apply to digital health products.

A product, which may be either a device or software, that constitutes a medical device is governed by the Pharmaceuticals Act. That Act defines a medical device as an instrument (including a computer program) that is intended for use in the diagnosis, treatment or prevention of disease in humans or animals, or is intended to affect the structure or function of human or animal bodies (excluding regenerative medicine products, which are separately regulated), and that is specified by a Cabinet Order.

If a company’s digital health product constitutes a medical device, the company must obtain a marketing licence, manufacturing licence and distributing licence in order to conduct marketing, manufacturing and distribution of the device, as well as authorisation, certification or notification for the specific device, according to the statutory classification. This is determined in accordance with the risk that the device would injure the human body in the case of malfunction. The classification is harmonised through the International Medical Device Regulators Forum, which succeeded the Global Harmonisation Task Force founded by Japan, the USA, the EU, Canada and Australia.

More specifically, a Class I medical device is classified as a general medical device under the Pharmaceuticals Act and requires only notifica-

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi, Anderson Mori & Tomotsune

tion to the regulator. A Class II medical device is usually classified as a controlled medical device and requires a marketing authorisation from the PMDA, but certain categories of Class II medical devices designated as relatively low risk are exempt from the requirement for a marketing authorisation and require only certification by an accredited body. Similarly, Class III and Class IV medical devices are classified as specially controlled medical devices requiring a marketing authorisation from the PMDA, with a few exceptions (designated specially controlled medical devices) requiring only a certification by an accredited body.

The question of whether a clinical trial is required depends on the classification of the product, the difference between the product and existing products on the market and the possibility of establishing the efficacy and safety of the product by means other than a clinical trial. However, a medical device with an apparently different structure, usage, effect or performance from existing medical devices will most likely be subject to a clinical trial and application for authorisation from the PMDA, regardless of the aforementioned classification.

Software as a Medical Device

The MHLW and other governmental bodies have issued guidance regarding the digital health sector. Notably, the MHLW issued the Basic Concept on whether a Computer Program falls under the Medical Device, which provides a clearer indication than is provided in the Pharmaceuticals Act, and a ministry ordinance on whether certain software constitutes a medical device. The guideline states that the question of whether certain software constitutes a medical device should be decided based on the impact that the software has on the diagnosis and treatment of a disease, considering the significance

of the results obtained by the software, and the risk of affecting the life and health of a person in the event of software malfunction. Even if certain software is used in the diagnosis, treatment or prevention of disease, it will not be treated as a medical device if it has a very low risk of injury to humans that is comparable with the risk of a Class I (hardware) medical device. Furthermore, the guideline contains examples of software that do and do not constitute medical devices.

The SaMD Guideline mentioned in **2.2 Recent Regulatory Developments** further distinguishes between various types of software according to their purpose and function, especially whether the software is to be used by medical professionals or by laypersons. Therefore, the purpose and function of the software must be clarified first. The Guideline then requires comparison between the purpose and function of the software with the purpose and function of existing software already categorised as a medical device. If the software has a similar purpose and function to those that are already categorised as a medical device, the software is also likely to be categorised as a medical device.

7. Telehealth

7.1 Role of Telehealth in Healthcare Guidelines Regarding Online Medical Treatment

In Japan, telehealth is mainly discussed in the context of online medical treatment. Under the Guidelines for Appropriate Performance of Online Medical Treatment, dated March 2018 (amended in March 2023), the MHLW describes “matters to be complied with at minimum” and “matters recommended” with respect to online medical treatment in order to promote its appropriate use.

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

Article 20 of the Medical Practitioners' Act stipulates that "no medical practitioner shall provide medical treatment or issue a medical certificate or prescription without personally performing an examination". Thus, arguably, in the past, an online medical treatment might have violated Article 20. However, the above Guidelines clarified that an online medical treatment does not violate Article 20 if that treatment is performed in compliance with the "matters to be complied with at minimum" under the Guidelines.

Definition of Online Medical Treatment

Under the Guidelines, telemedicine is defined as "an act concerning health improvement and medical treatment using information communications equipment". Also, online medical treatment is defined as "a type of telemedicine, which is an act of medical treatment, such as carrying out examinations, making diagnoses, transmitting examination results and prescribing medicines in real time by using information communications equipment".

Matters to Be Complied With at Minimum

The Guidelines describe the "matters to be complied with at minimum", which include, among others, the following:

- a doctor and a patient must agree to the performance of an online medical treatment;
- in principle, online medical treatment from the first medical examination must be conducted by a primary care doctor;
- a doctor must prepare a medical treatment plan based on the result of the face-to-face medical examination and maintain that plan for two years;
- in principle, the identity of the doctor and patient must be verified through identity-verification documents;

- a prescription for certain pharmaceuticals must not be issued at the first medical examination; and
- an online medical treatment should be conducted using information communication tools with real-time visual and auditory information in order to obtain as much medical information as possible.

Regulation Regarding Online Medication Counselling

Another development of telehealth in Japan is online medication counselling.

Formerly, the Pharmaceuticals Act stipulated that medication counselling must be conducted face to face.

However, the Pharmaceuticals Act was amended in September 2020 to allow online medication counselling under certain conditions.

The conditions for online medication counselling are as follows:

- medication counselling was previously conducted face to face;
- online medication counselling should be conducted using a medication instruction plan that describes certain matters; and
- pharmaceuticals to be sold or given away must be prepared using a prescription issued by an online medical treatment or home-visit medical treatment.

7.2 Regulatory Environment Temporary Relaxation of Regulations

Due to the spread of COVID-19, the MHLW issued a notice on 10 April 2020 temporarily relaxing regulations regarding online medical treatment and online medication counselling.

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi, Anderson Mori & Tomotsune

Relaxation of Regulations Regarding Online Medical Treatment

Physicians were permitted to conduct a patient's initial medical examination using online medical treatment if the doctor determined that it is medically possible to make diagnoses or prescribe medicines through a medical examination using a telephone or information communications equipment. However, a doctor must attempt to gather and confirm information regarding a patient through past medical records, the medical information provision form, a local medical information collaboration network or a medical examination result.

Also, in order to conduct the initial medical examination by telephone or information communications equipment, the following conditions must be satisfied:

- a doctor must provide a patient with sufficient information (such as regards possible risks, policy in the case of emergencies, etc) and must record the content of the explanation in the patient's medical records;
- a doctor must secure a system for switching smoothly to face-to-face medical treatment if necessary; and
- a doctor must verify a patient's identity and eligibility.

Furthermore, a medical institution must report the implementation status of online medical treatment on a monthly basis to the prefecture in which the medical institution is located.

Relaxation of Regulations Regarding Online Medication Counselling

Pharmacists were permitted to conduct online medication counselling if the pharmacist determined that it is possible to conduct medication counselling appropriately by telephone or infor-

mation communications equipment, based on information regarding the patient and their medication status.

Also, in order to conduct medication counselling by telephone or information communications equipment, the following conditions must be satisfied:

- a pharmacist must provide a patient with sufficient information (such as regards possible risks, procedure of delivery and confirmation of medication status), and must record the content of the explanation;
- a pharmacist must confirm medication status and side effects by telephone during the medication period for a drug prescribed for the first time, in order to encourage medication adherence and secure appropriate usage of a drug;
- a pharmacist must switch smoothly to face-to-face medication counselling if necessary; and
- a pharmacist must verify a patient's identity and eligibility.

7.3 Payment and Reimbursement

In Japan, payment by a patient for medical treatment at a medical institution is generally covered by national health insurance and a patient is required to pay only a portion of the cost of medical treatment at a medical institution.

Also, medical fees for medical treatment are prescribed by the MHLW.

Medical fees for online medical treatment and online medication counselling are also prescribed by the MHLW; therefore, insurance reimbursement is available for a patient who receives online medical treatment and online medication counselling.

8. Internet of Medical Things

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

The IoMT makes it possible for various and multiple smart devices, including wearables and implantables, to connect with each other through the internet. 5G networks, which have been available in Japan on a limited commercial basis since March 2020, enable high-speed data exchange with other devices and hospital networks. The large volume of data to be collected through the networks is useful for AI to study.

Concerning the security risks associated with use of the networks, such as use of a cloud storage service for storing electronic medical records and images, the MHLW issued the Guidelines regarding Security Management of Medical Information Systems, with which medical institutions must comply. Additionally, the Ministry of Internal Affairs and Communications (MIAC) and the Ministry of Economy, Trade and Industry jointly issued the Security Management Guidelines for Information System Service Providers dealing with Medical Information, with which service providers must comply. The Guidelines appear to take a risk-based approach – ie, requiring the parties to:

- identify the risks;
- analyse the level of each risk;
- evaluate how to treat the risk, based on the analysed level of each risk;
- treat the risk, evaluate the remaining risks and the record thereof;
- reach an agreement; and
- continue risk management.

Various types of digital assistants for human health have been introduced recently. To the

extent that certain digital assistants fall within the scope of medical devices to be regulated by the Pharmaceuticals Act, the digital assistants would be subject to the same regulations. Whether the digital assistants fall within the scope of medical devices depends on the importance of the results to be generated by them and the seriousness of the risk that may be caused by a malfunction or defect in the digital assistant. For example, in 2020, the PMDA approved, as regulated medical devices:

- a program for curing nicotine addiction; and
- Apple’s electrocardiograph program and heart-rate monitoring program for Apple Watch.

By contrast, the MHLW found that a tool for predicting the onset of diabetes, which was uploaded for the public by the National Centre for Global Health and Medicine on its website in 2018, did not fall within the scope of regulated medical devices. A program that takes an important role in a doctor’s diagnosis of diabetes would appear to be a medical device, while a program that only shows the possibility of developing diabetes in the near future would not be considered a medical device.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

5G networks are wireless telecommunications networks with high speed, large capacity, low latency and multiple connections. They are expected to enable telemedicine, remote surgery, online medication instruction and online collection, storage and use of medical data and images. These are especially valuable for medical treatment in disaster areas. 5G networks

are also considered to be able to mitigate the reduced access to medical treatment of residents, including elderly people, in rural areas that may be caused by the uneven distribution of doctors in urban and rural areas in Japan.

However, the areas in which 5G networks are available are still limited. Further, when health-care institutions enter into arrangements with telecommunications providers to deploy and manage 5G networks, those institutions must address the allocation of the risks that may arise, such as interruption, malfunction and defects of the networks. Similarly, allocation of the risk of potential infringement of intellectual property rights owned by third parties may also be an issue.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

Law to Protect Data Relevant to Personal Health

The APPI provides protection for personal data handled by private entities. While the APPI does not provide a special protection and management scheme for data relevant to personal health, it defines “special care-required personal information” as personal information that may lead to discrimination against, or other disadvantage to, an individual, such as information regarding race, religion, social status, medical records and criminal records. Therefore, data relevant to personal health usually falls within the definition of special care-required personal information.

Disclosure of Personal Data to a Third Party

Under the APPI, disclosure of personal information to a third party requires consent from the data subject. Consent may be obtained through an opt-out procedure. Pursuant to an opt-out procedure, disclosure of personal information to a third party will be permitted without the individual’s explicit consent if the individual was informed (or was otherwise notified in a way that made it possible for the individual to acknowledge) that their personal information would be disclosed to a third party, and the individual had the opportunity to refuse disclosure.

However, an opt-out procedure is not permitted for the disclosure of special care-required personal information. Therefore, explicit consent must be obtained prior to providing health data to third parties if that health data is considered to be special care-required personal information.

Anonymisation of Data

The APPI defines the term “anonymously processed information” as information relating to an individual that may be created by processing personal information so as not to be able to identify a specific individual. In particular, processing personal information for de-identification means deleting:

- descriptions that may identify a specific individual;
- individual identification codes;
- codes that link the processed information with the personal information; and
- idiosyncratic descriptions (ie, descriptions that could identify an individual because of the uniqueness of the information).

The APPI substantially eases the restrictions on the acquisition, disclosure and use of personal

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

information for anonymously processed information.

However, explicit consent is still required when providing special care-required personal information to an outside information processor for the anonymising process. Moreover, medical information is often held by individual hospitals and entities, and explicit consent from the patient is required when the original data, which in many cases constitutes special care-required personal information, is provided to, or used by, an outside information processor. Therefore, the accumulation of medical information and construction of a database has been difficult.

To ease this difficulty, Japan has enacted the Act Regarding Anonymised Medical Data to Contribute to R&D in the Medical Field (the “Next-Generation Medical Infrastructure Act”, or NGHIA) to facilitate the accumulation of medical information and to promote the use of big data for the development of medical technologies, while also protecting patients’ privacy and personal information. Under the NGHIA, the Japanese government authority will examine and authorise entities to be data-processing entities that collect, de-identify and provide medical information to third parties (Authorised De-identified Medical Information Preparer). Provision of medical data to the Authorised De-identified Medical Information Preparer still requires consent from the patient, but the opt-out procedure applies. The Authorised De-identified Medical Information Preparer will identify and link a patient’s data from different medical institutions, adjust the data format and integrate the data into a database. When a third party, typically a healthcare company or a research institution, requests data, the Authorised De-identified Medical Information Preparer will select the relevant data, de-identify it and provide an anonymised data set for a fee.

Enforcement

Under the APPI, the Personal Information Protection Commission, an organisation within the Cabinet Office, provides the necessary guidance and advice to business operators handling personal information, including health data, and collects reports, conducts on-site inspections and makes recommendations and orders regarding legal violations. Japan does not have a long history of using digital healthcare technology, so no notable regulatory or private enforcement actions have yet been published in the medical service sector.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare AI and Medical Devices

Artificial intelligence (AI) technology has been developed in recent years and has the potential to design programs with performance that would have been difficult to achieve with conventional algorithms, such as enabling detailed prediction of disease changes in patients and detecting lesions that even a specialist could not identify.

The question of whether a specific AI program should constitute a medical device (and therefore be subject to the Pharmaceuticals Act) is determined based on the same concepts as other programs using conventional algorithms. However, the relationship of AI technology-based programs to medical devices must be considered in connection with the specific risks associated with the level of technology at the time, such as how to add new data for machine learning.

In accordance with the Pharmaceuticals Act, the term “programmed medical device” means

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

programs intended to be used for diagnosis, treatment or prevention of human diseases in the form of tangible objects installed in general-purpose computers, personal digital assistants, or to influence the structure or function of human bodies. However, programs that are unlikely to have an impact on human life and health, even if functional impairment occurs, are excluded from the scope of medical devices.

The following programs using AI technologies will be included in the scope of medical devices:

- a program in which AI substitutes for diagnoses that can only be performed by specialists, such as detecting cancer with a certain degree of accuracy and predicting life expectancy using medical images;
- a program in which AI predicts the name of a disease based on information such as body temperature and blood pressure entered by non-healthcare professionals using an original algorithm; and
- a program that uses AI to identify and assist in the testing of suspected disease areas during the use of a medical device.

By contrast, the following programs will be excluded from the scope of medical devices:

- a program that allows users to enter health data and self-manage their weight and health based on information provided by AI;
- a program that provides detailed 3D images of the human body after image correction by AI for use in medical students' learning and in patient explanation;
- a program in which AI extracts necessary information from medical record information and presents the names of potential diseases along with the relevant parts of the guidelines and the basis for the determination according

to information on publicly available medical care guidelines;

- a program utilising AI that presents the information necessary for medical practice from clinical data using publicly available formulas;
- a program that uses AI to allow doctors to search for publicly available guidelines and package inserts when making a diagnosis; and
- a program using AI that assists in the use of medical devices in accordance with known guidelines.

Cybersecurity

For details on AI and cybersecurity, see [5.3 Cybersecurity and Data Protection](#).

11.2 AI and Machine Learning Data Under Privacy Regulations

The MHLW published Benchmarks for Next Generation Medical Device Evaluation on 23 May 2019. It included Benchmarks for Evaluation of Medical Image Diagnosis Support Systems Using Artificial Intelligence Technology. It provided the MHLW's view on points to be considered when evaluating the effectiveness and safety of medical image diagnosis support systems using AI technology.

In December 2019, the Ministry of Economy, Trade and Industry (METI) also published Guidelines for the Development of Medical Diagnostic Imaging Support Systems (Including Systems Using Artificial Intelligence Technology), which summarises the points to be considered by researchers and developers during the development of Computer Aided Diagnosis (CAD) systems. These Guidelines are a revision of the developmental guideline on CAD published in the early 2010s and combine the then two existing CAD development guidelines into one, with an additional description on AI technology.

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

Under the APPI, medical information is further classified into special care-required personal information, for which care must be taken when handling such information. In addition, it is necessary to obtain the consent of patients when handling such information outside medical institutions. It is also necessary to obtain consent for the intended use, such as for the learning of AI in medical devices and applying the learning results to products. In the case of academic research, personal information may be used for research without individual consent under Article 76 of the APPI. However, this Article does not apply in cases of product development. On the other hand, the use of medical information in academic research is highly likely to fall under “clinical research” stipulated in the Clinical Research Act or “research” stipulated in the Ethical Guidelines for Life Science and Medical Research Involving Human Subjects, and the consent of the research subjects is required. The collection, use and storage of data based on clinical trials under the Pharmaceuticals Act need to comply with GCP Ordinances set forth by the MHLW and are not subject to the APPI.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Established IT companies have vast experience and resources for dealing with personal information through existing businesses, but they still need to pay close attention to regulations under the Personal Information Protection Act because the information dealt with by digital healthcare technology is highly sensitive, and personal information and the Personal Information Protection Act itself (and the ordinances and guidelines thereof) have been updated. Healthcare institutions and other clients need to make

sure that their agreements with vendors manage their personal information properly. Further, it is necessary to comply with the regulations under the Pharmaceuticals Act, which is usually new to such companies. Such regulations have traditionally been handled by in-house specialists in pharmaceutical and medical device companies. Some established IT companies have started to hire regulatory specialists as well as to seek consultation with independent external experts on the matter.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

Japan is the first country in the world to have a rapidly declining birth rate and an ageing population. Under these circumstances, it is necessary to take measures to promote a healthy life expectancy of each citizen, and to ensure the sustainability of social security. Such measures include improving efficiency and productivity, while also maintaining and improving the quality of services at busy medical and nursing sites.

These issues must be addressed by:

- promoting ICT in the fields of health, medical care and nursing care;
- ensuring that each and every citizen and patient makes effective use of their own medical and other data; and
- ensuring that health and medical facilities and related industries make appropriate use of that data.

Social Changes, Data Protection and Cybersecurity

In addition, the social change known as Society 5.0 is rapidly progressing, through the use of advanced information and communication

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

technologies and data. In the field of healthcare, data is handled not only by entities engaged in healthcare, but also by new entities, including private companies. These social changes have brought about a number of important issues that must be addressed, not only in Japan but also internationally, such as rules for data utilisation, the protection of personal information, and cybersecurity measures.

Special consideration should also be given to privacy regarding health, medical and nursing care information. For this reason, all actors, including the State, must take necessary measures in promoting these efforts. In particular, it is essential to take all possible measures to ensure information security in the medical field, as one of the important infrastructure fields.

With the advancement of ICT in the medical field, it is also important to confirm the identity of healthcare workers and promote measures to prevent forgery and falsification of electronic documents.

Information Management

From the viewpoint of the availability of user data stored in cloud services, public entities that use cloud services to collect and store medical and other information nationwide must be required to:

- ensure thorough information management by selecting domestic data centres subject to Japanese laws;
- conclude treaties and cloud services with jurisdiction over Japan as candidates for adoption; and
- make cloud security certification mandatory.

Medical information is also subject to the APPI as personal information requiring special care.

However, from the perspective of protecting medical information while also promoting the use of information and the promotion of research and development at medical sites, issues remain, such as how to obtain consent from individuals.

The Japanese government plans to examine the handling of personal information in the medical field while investigating the status of legislation in foreign countries regarding the protection of personal information (including issues related to data portability) in the medical field.

13.2 Data Management and Regulatory Impact

In August 2020, METI and MIAC issued the Safety Management Guidelines for Providers of Information Systems and Services Handling Medical Information, which combines two sets of then-existing guidelines (ie, the Safety Management Guidelines for Information Processing Service Companies Managing Medical Information issued by METI, and the Guidelines for Safety Management by Cloud Service Providers Handling Medical Information issued by MIAC). The purposes of the combined Guidelines are to:

- ensure the same level of safety management as compliance with past guidelines, while taking into account consistency with other standards and guidelines;
- define risk management processes based on a risk-based approach for the purpose of designing necessary and sufficient measures according to the characteristics of medical information systems, etc;
- emphasise risk communication for the purpose of operating medical information systems, etc based on a correct common understanding and explicit agreement on the efficacy and limitations of security measures; and

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

- clarify points to be considered in the handling of medical information and requirements in the system for the purpose of preventing omission of required measures under the laws and regulations related to medical information systems.

In March 2022, the MHLW issued Guidelines for the Safety Management of Medical Information Systems, Version 5.2, which describe, from the viewpoint of technical and operational management, necessary measures for ensuring the safety management of medical information systems and appropriate compliance with the Act on the Utilisation of Information and Communications Technology in Document Preservation Conducted by Private Business Operators, etc. Section 6.8 “Modification and Maintenance of Medical Information Systems” of the Guidelines states that regular maintenance is necessary to maintain the availability of medical information systems. Such maintenance work includes troubleshooting, preventative maintenance and software revision. As the system maintenance personnel may have direct access to medical information in administrator mode, the Guidelines require sufficient countermeasures against possible data leakage.

14. Intellectual Property

14.1 Scope of Protection

Hardware can be protected by a patent, utility model right or design right, provided that:

- the hardware is novel; and
- it has an inventive step over prior art or is not similar to prior designs.

Software is eligible for protection not only by copyright, but also by patent and utility model

right, and may also be protected as a trade secret. User interfaces for medical devices may be protected by copyright and design right. Notwithstanding the foregoing, methods for medical treatment are not eligible for protection by patent or utility model right.

Data and databases used in machine learning are eligible for trade secret protection, provided that confidentiality can be maintained. Big data, which is not managed in such a way as to maintain confidentiality but is collected and managed to be provided to other specified entities, may also be protected under the Unfair Competition Prevention Act. A database is also eligible for copyright protection as long as it is creative in terms of selection or systematic construction of data contained therein.

Despite recent frequent discussions, there is no prevailing view under Japanese law regarding inventions and works of authorship created by AI technologies without direct human contributions. However, a person or entity operating AI technologies with a certain purpose or theme may be recognised as an inventor or author.

14.2 Advantages and Disadvantages of Protections

Patents for inventions which are claimed as consisting of elements accessible by users and design rights in user interfaces are good in the sense that it is easy to identify the infringement carried out by competitors, whereas structures and codes that are embedded in competitors’ programs and data are difficult to identify. Further, patents and design rights are easier to enforce in many cases compared to copyright or trade secrets because alleged infringers’ access to or knowledge of such rights are not required as a condition for enforcement thereof; whereas alleged infringers’ access to, or knowledge of,

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi, Anderson Mori & Tomotsune

the original works or the trade secrets which have been managed to be kept secret is required as a condition for enforcement thereof.

That said, the life of patents and design rights is limited to 20 or 25 years from filing, while copyright protection is eligible for 70 years and there is no periodical limitation for trade secret protection. Further, patents and design rights are easy to design around, whereas eliminating contamination of copyrighted codes or trade secrets is not so easy. Therefore, it is important to protect products or processes by a combination of multiple types of intellectual properties.

14.3 Licensing Structures

There are various types of licensing structures in this field but, in some cases, it is preferable for intellectual property (IP) holders to charge a running fee on a monthly or yearly basis rather than receiving a lump sum payment. In such cases, it is necessary to be careful that patents and design rights can be subject to exhaustion of rights once products protected by such rights are sold by holders or licensees thereof. A combination of granting a licence of software and data as well as providing support for updating it can be legitimate grounds for claiming a running fee.

14.4 Research in Academic Institutions

As long as university or healthcare institutions (“Institutions”) have their own rules stipulating that they acquire IP rights over inventions, etc, created by physicians/inventors working for the Institutions in the course of performing their tasks, the Institutions will own the rights to file applications for patents, utility model rights and design rights. However, the physicians/inventors are eligible for reasonable compensation. Additionally, the Institutions will be recognised

as authors and holders of trade secrets and big data.

If IP is jointly created by two entities, such as by a university and a private company through their joint research and development, the IP rights will be jointly owned by those entities unless otherwise stipulated in the governing agreement. If patents, utility model rights or design rights are jointly owned by multiple parties, each party may exploit those inventions without consent from the other parties, although assignment and licensing will require consent, unless otherwise stipulated in the governing agreement. Copyrighted works may not be used, assigned or licensed without consent of the other joint owners, unless otherwise stipulated in the governing agreement.

14.5 Contracts and Collaborative Developments

It is most desirable to have all joint ownership assigned to a single entity subject to its control. In such a case, the right to create derivative works and the right of the original author over derivative works under Articles 27 and 28 of the Copyright Act of Japan must be expressly stipulated as included in the assigned rights. Further, as the moral rights of authors are not assignable, authors must promise not to exercise those rights. If the rights are to be jointly owned by multiple parties, a contractual provision should address the exploitation of rights by a single joint owner.

15. Liability

15.1 Patient Care

In Japan, final decisions on diagnosis and medical treatment must be made by doctors, regardless of whether the doctors are using healthcare technologies such as data analytics or medical

Contributed by: Junichi Kondo, Yasufumi Shiroyama, Hiroshi Ishihara and Masayuki Yamanouchi,
Anderson Mori & Tomotsune

devices driven by AI or software. Accordingly, in principle, doctors and the medical institutions for which they work are considered to be responsible for the diagnosis or medical treatment and also liable for any injury caused to their patients thereby. However, both civil and criminal liability of doctors and medical institutions require a showing of physician negligence, and the burden of proof is on the patient. A doctor's reliance on digital assistance through healthcare technology is not an absolute defence, but in such a case, an accuser would be required to establish the doctor's negligence in the selection, maintenance or operation of the device.

If a doctor is successful in proving the possibility of malfunction or latent defects in the medical device, the doctor and relevant medical institution may not be found liable. There is no special legislation under which doctors and medical institutions are immune from liability, or are subject to strict liability, simply because the doctor relied on healthcare technology. Bias in AI or the possibility or failure of recognition thereof are factors that may affect a finding of negligence.

15.2 Commercial

Healthcare institutions that entered into contracts with vendors may choose to pursue contract claims against those vendors. A healthcare institution seeking to bring a contract claim against a vendor would be required to establish that:

- the vendor's products or services did not comply with the specifications or service level of the products or services agreed between the institution and the vendor;
- the vendor was negligent with respect to that non-compliance; and
- the damages caused to the healthcare institution by the vendor's products or services were foreseeable by the vendor.

For claims of healthcare institutions against vendors which are not parties to a contract with those institutions, contract claims are not available. A tort claim may be an option, provided, however, that those institutions have the burden to prove vendors' negligence or wilful misconduct and predictability of causing the damages.

Further, healthcare institutions may bring a claim under the Product Liability Act, which prescribes manufacturers' strict liability for damages caused by product defects. The term "defect" as used in this Act means a lack of safety that the product ordinarily should provide, taking into account:

- the nature of the product;
- the ordinarily foreseeable manner of use of the product;
- the time when the manufacturer delivered the product; and
- other circumstances concerning the product.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com