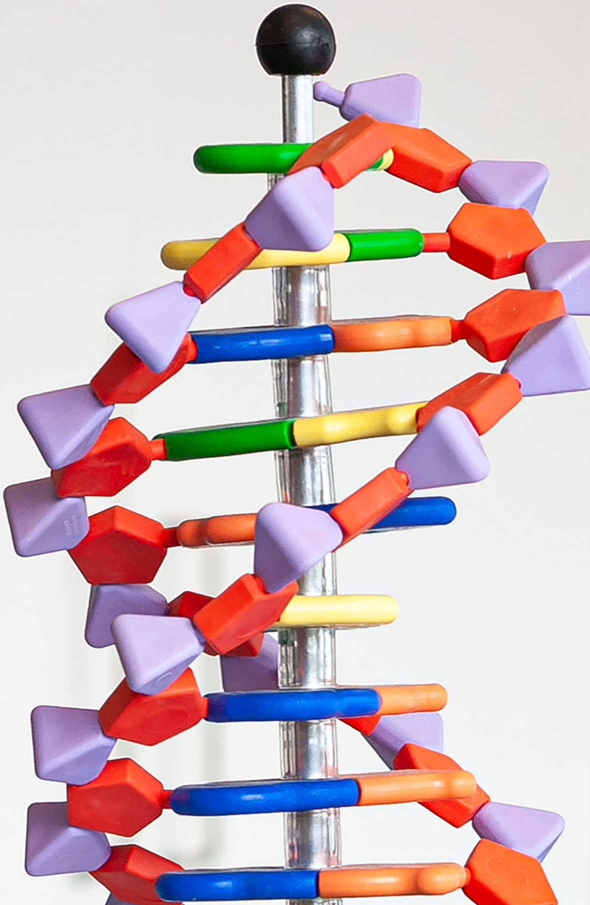
Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Digital Healthcare 2023

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



Israel: Law & Practice
Eran Bareket
Gilat, Bareket & Co.,
Reinhold Cohn Group

ISRAEL

Law and Practice

Contributed by:
Eran Bareket
Gilat, Bareket & Co., Reinhold Cohn Group

Contents

Gilat, Bareket & Co., Reinhold Cohn Group is the leading intellectual property consulting firm in Israel. RCG offers the full breadth of intellectual property-related services and expertise, including protection, asset management, due diligence, and litigation and legal services. The firm operates in all areas of IP, such as patents, trade marks, designs, copyrights, open source and plant breeders' rights. The group includes the intellectual property attorneys firm Reinhold Cohn & Partners and the law firm Gilat, Bareket & Co. RCG employs over 200 professionals, out of which over 50 are patent attorneys and attorneys at law. The synergy of patent attorneys experienced in a diverse spectrum of technological and scientific disciplines working alongside legal professionals creates a unique and effective platform for maximising the value of a client's intellectual property assets by securing optimal protection. RCG and its team of professionals are internationally renowned for excellence and continually ranked amongst the top tiers in leading international and local guides.

Author

Eran Bareket is a partner at the Gilat, Bareket & Co., Reinhold Cohn Group. He holds an LLB degree, 1990, from Tel Aviv University and teaches in leading Israeli universities. Eran's expertise is litigation of IP rights, unjust enrichment, competition law and complex litigations, particularly those involving issues of technology and management of multi-jurisdiction IP litigations. Eran has vast experience appearing before all Israeli courts, including the Patents, Designs and Trademarks Registrar. He is well versed in the fields of IP, high technology, technology transfer and licensing, digital health, big data licensing, competition law, agency and distributorships, regulatory law (pharmaceuticals and medical devices), defence and homeland security, and governmental companies. Eran is often involved in the Israeli Parliament (Knesset) legislative process, acting on behalf of various entities. He serves as consultant for IP matters to the Accountant General's Division of the Ministry of Finance and represents the government regarding disputes surrounding inventions by state employees (service inventions).

Gilat, Bareket & Co., Reinhold Cohn Group

26A Habarzel St.
Tel Aviv
Israel

Tel: +972 3 567 2000
Fax: +972 3 567 2030
Email: info@gilatadv.co.il
Web: gilat-bareket.rcip.co.il/en/

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Digital health products have become an integral part of medicine, whether in the prevention, diagnosis, treatment or management of health and diseases.

From the point of view of the patients/consumers, health apps have improved their ability to track their health and fitness, store or transmit health data, keep track of their test results or doctor appointments and improve their wellness and well-being. At the same time, these technologies increase the risk of invasion of privacy and leakage of personal sensitive information.

Healthcare providers (HMOs) use digital health products to improve and enhance the quality of medical services provided. This includes, among others, decision support systems, workload management systems, telehealth services, and early detection technologies. For instance, the Director General of the Ministry of Health (MoH) recently issued a directive encouraging hospitals and HMOs to increase the use of telehealth to monitor and examine patients in order to minimise physical clinic visits in anticipation of winter 2023.

HMOs are also actively engaged in out-licensing access to their highly valuable databases of health data.

From a regulatory standpoint, the primary entities are the MoH and the Authority for the Protection of Privacy, with the Authority for Innovation and others occasionally playing a role.

Combining technological platforms with clinical evidence that measures intervention leads to considerable technological progress. A prime example is the digital surgery platform, VELYS™, which employs AI and patient-specific data collection to transform orthopedic surgery. This platform not only changes the way surgeons work, but also improves patient recovery by facilitating the creation of personalised treatment and surgery plans.

Combining technological platforms with clinical evidence that measures intervention leads to considerable technological progress. For example, the digital surgery platform VELYS™ uses AI alongside specific data collection capabilities on each patient, and leads to a change in the field of orthopedic surgery – both in the way surgeons work and in the patients recovery through the creation of a personalized treatment and surgery plan.

1.2 Regulatory Definition

There are no regulatory definitions of digital health and digital medicine. There are several circulars of the MoH addressing certain aspects of these activities. The main body of regulation that is not health specific but that applies to digital healthcare is the privacy protection framework.

1.3 New Technologies

Some of the key technologies enabling new capabilities in digital healthcare and digital medicine are:

- sensor technologies, facilitating nano-level detection as well as various non-invasive techniques; these are particularly useful for wearables;
- AI and machine learning technologies – these are useful both for studies aimed at finding treatment and diagnostic solutions that will improve predictive medicine and personalised medicine,
- research platforms and technologies based on big data, AI, and machine learning to find treatment and diagnostic solutions and to identify new medicines and biomarkers, etc;
- decision support systems based on AI and machine learning technologies for physicians and other workers of the healthcare industry that will improve the quality of healthcare services;
- high-speed and high-bandwidth sophisticated telecommunications systems useful for both telemedicine and remote care; and
- advanced computer vision technologies that facilitate, together with AI and machine learning technologies, improved interpretation of various medical imaging devices and are currently used as decision support tools for physicians.

1.4 Emerging Legal Issues

The emerging key legal issues in digital health are explored in more detail in other sections of this chapter. Briefly put, they include privacy and data security issues, healthcare regulatory concerns such as anonymisation and preservation of confidentiality of health data, regulatory limitations on data sharing, data portability and the application of contract and commercial law to the evolving industry of data access and licensing.

1.5 Impact of COVID-19

The State of Israel has emerged from the grips of the COVID-19 pandemic, yet the pandemic's legacy continues to shape the country's healthcare landscape. The surge in digital prescriptions and other tech developments, such as telemedicine capabilities, have transformed healthcare delivery. Moreover, the pandemic has been a catalyst for the expansion of home-based medical services, enabling healthcare professionals to offer treatment beyond the confines of traditional healthcare facilities.

The impetus behind developing and adopting digital healthcare technologies was strong even before the COVID-19 pandemic. Nevertheless, the pandemic did bring about a certain acceleration because of the increased motivation, both for the public sector and the private sector, to invest financial resources into more efficient provision of healthcare services. This included telemedicine solutions, AI-based monitoring solutions (for example, a monitoring system that enables advance prediction of respiratory complications of patients hospitalised in intensive care units or another hospital unit) and automation of digital processes. Home diagnostics devices connected to the internet enabled patients struggling to attend in-person appointments to transmit medical data on an ongoing basis to their physician.

Lastly, the highly developed infrastructure for big data studies enabled data studies of the results of the national vaccination programme that resulted in millions of people being vaccinated in a very short period of time. The results reported in prestigious magazines have enabled the global medical community to benefit from Israel's experience within a very short period of time.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

The key regulatory agency is the MoH, which is responsible for most aspects of the healthcare and pharmaceutical industries. It issues marketing authorisations for pharmaceuticals and for medical devices, including regulation of the requisite clinical trials. It also regulates the activities of the HMOs. Finally, the MoH regulates the practice of medicine by physicians. There is no separate agency that is entrusted with the regulation of digital medicine, digital health and/or medical devices.

2.2 Recent Regulatory Developments

The digital transformation of the healthcare industry is unfolding rapidly, but the development of a comprehensive and detailed digital healthcare regulatory scheme is lagging behind. The government published a national digital transformation plan and the MoH followed suit with its own digital health programme. However, primary legislation was not amended. Draft regulations (secondary legislation) relating to health data anonymisation and health data sharing have been published for public consultation but have not yet been published.

As it stands, the main regulatory documents that have been published today are circulars of the general manager of the MoH that concern certain aspects of secondary use and sharing of health data, the use of digital means in the process of obtaining informed consent, the use of cloud computing in the Israeli healthcare system, the criteria for operating telehealth medicine, providing patients accessibility to personal health data ("healthcare in the palm of your hand"), the protection of information in computerised systems in the healthcare system, the rules of ethics for remote care of Israel Medical Association, etc. The circulars are intended to be binding for HMOs and hospitals, although this is partially disputed by certain HMOs. Their authority over the private sector remains uncertain, yet due to the private sector's reliance on healthcare institution data, considerable control over conduct is largely maintained.

In early 2023, a draft bill proposing a health data portability law was introduced. The objective of this bill is to provide the necessary regulatory infrastructure to ensure patient health information is available and reviewable when and where it is needed, all the while maintaining patient privacy and information security.

To realise the vision of quality information in the Israeli healthcare system and to facilitate and improve co-operation between the authorities, a medical nomenclature project was recently launched. This project promotes the use of documentation and data coding in the Israeli healthcare system, with the first phase involving the implementation of SNOMED-CT for uniform medical terminology to document medical operations and diagnoses.

At the data protection and privacy level, the Privacy Protection Authority has published statutory regulations covering the various aspects of data protection. The regulations were inspired by, and are generally consistent with, the European General Data Protection Regulation (GDPR).

2.3 Regulatory Enforcement

The main regulatory enforcement activity currently conducted concerns privacy protection enforced by the Privacy Protection Authority. This Authority supervises and enforce not only hospitals and HMOs, but also the Medical Examination Institute and imaging institutes, which naturally hold sensitive medical information. The pressing need for stringent oversight by the Privacy Protection Authority is clearly underscored by two key factors: the extreme sensitivity of health information and the rapid pace at which digital health solutions are being adopted, all set against a backdrop of an underdeveloped and non-systematic healthcare regulatory scheme. For example, in 2021, during the COVID-19 pandemic, enforcement actions revolved around the transfer of personal information from the MoH to the various local authorities and municipalities.

The enforcement actions of a regulatory authority can take place either on an administrative or criminal level. Administrative measures might include imposing fines or recommending the removal of officers from their posts. Before imposing an administrative sanction, the regulatory authority must gather evidence sufficient enough to justify its decision and, in most cases, must allow the institution an opportunity to present its case before a final decision is reached.

On the other hand, criminal enforcement involves bringing a case before a competent court and may result in imprisonment, a fine or both.

3. Non-healthcare Regulatory Agencies

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

The Privacy Protection Authority is a non-healthcare regulatory agency responsible for enforcing the privacy and data protection legislative scheme in Israel. All other health-related issues (including wellness, fitness and self-care) are regulated by the MoH.

The Privacy Protection Authority is primarily concerned with issues, including: the way data is collected; the way data is shared; preserving the confidentiality of private data, including health data; protecting against data breaches; managing medical terminology; and preventing cyber-attacks, amongst others. The MoH is concerned with almost all aspects of the healthcare and medical industries. These include the health of patients (safety and efficacy of treatments), proper management and financial stability of health institutions, the national health budget, and the rights of patients. As such, the matter of health data usage and sharing falls under the joint jurisdiction of these two authorities. Regarding data anonymisation, the MoH typically assumes the lead role. Interactions between these two entities generally lack transparency.

Government participation is also manifested through the Authority for Innovation, which offers financial support for digital medicine projects across various fields.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

There is no significant difference between preventative care and diagnostic care under Israel's healthcare systems, since both of them are regulated under the same laws and regulations and are provided by the same healthcare providers, namely the HMOs. For example, the definition of "practice of medicine" under the Physicians Ordinance [New Version], 1976, does not differ between specific fields: "means any examination, diagnosis or treatment of, and the giving of any prescription for, sick or injured persons, attendance to women in connection with pregnancy and childbirth, and other services generally performed by a physician". Accordingly, health maintenance organisations provide a wide range of medical services, including services of preventative care, as well as of diagnostic care.

4.2 Increased Preventative Healthcare

Social trends such as people becoming more knowledgeable and active about their health during the COVID-19 pandemic, brought about an expansion of digital health. Government initiatives (such as the food labelling reform) have also contributed to health awareness and increased the focus on preventative care. Accordingly, healthcare and non-healthcare organisations began investing in the wellness field. Health maintenance organisations began to implement their services and technologies for healthcare and wellness. For example, Clalit (the largest HMO in Israel) provides its members with the "Active" app, which promotes a healthy lifestyle by recommending various personal goals, such as a daily number of steps, and other physical activity, as well as recommending how much water to drink, and providing data about sleeping patterns, and more.

Clalit also recently announced the launch of an AI platform called CPI (the Clalit protective-preventive intervention platform), which provides doctors with data regarding which patients would benefit from preventive medicine due to certain risk factors.

Israel is a leading country in preventative care. One of the fields in which Israel invests is food technology. For example, in 2020 the Inaugural Global Wellness Summit Prize for Innovation was awarded to Amai Proteins, an Israel-based innovator that developed protein-based products for food and beverages, including a sweet designer protein as a substitute for sugar ("designer sweet proteins"), that significantly reduces added sugar in a wide variety of food and beverages. The awareness of preventative care is constantly rising, leading to the development of new technologies that promote a healthy lifestyle.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Wellness and fitness data are not subject to specific healthcare or privacy regulations, but rather to general regulations that apply to data and digital health (see a list of relevant regulations in **4.1 Preventative Versus Diagnostic Healthcare**).

In addition, the General Director (GD) of the MoH published a few circulars referring specifically to digital health, as listed below:

- GD Circular dated 17 January 2018, regarding secondary uses of health data;
- GD Circular dated 17 January 2018, regarding collaborations based on secondary uses of health data; and
- GD Circular dated 11 November 2019, regarding patient access to personal health data – "Healthcare under your Control."

- GD Circular dated 15 December 2019, regarding the management of patient records in the health system;
- GD Circular dated 5 January 2020, regarding the code of ethics for maintaining the confidentiality and integrity of personal information;
- GD Circular dated 21 February 2021, regarding the use of cloud computing in the health system;
- GD Circular dated 30 November 2021, regarding recommendations to the public in the use of wearable devices for sports and health purposes; and
- GD Circular dated 13 March 2022, regarding cyber protection in the health system.

The health data circulars currently prescribe the extent of protection over health data. In general, unless otherwise specified by law or approved by an explicit opt-in, any data for secondary use will be anonymised. Furthermore, any secondary use of health data for research purposes must be pre-approved by the Helsinki Committee.

No law in this field has been developed by courts or judges, but rather by legislative enactment.

4.4 Regulatory Developments

To date, no binding regulation applying specifically to preventative healthcare has been enacted in Israel.

4.5 Challenges Created by the Role of Non-healthcare Companies

The digital healthcare market's landscape is in constant flux, and there are many areas of uncertainty; it may also vary among countries. Thus, partnering with an institution with experience in the field is advantageous. Special attention must be paid to the regulatory schemes applicable to both the R&D stage, as well as to the commercial marketing and sales stage.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

The following have enabled the enhanced use of connected devices in digital healthcare:

- technologies of telehealth;
- wearable electronics that allow user data capture;
- AI/machine learning that enable user data processing, analysis, diagnostics and prediction;
- a cloud that allows remote monitoring of patients; and
- robotics that allow performance of certain tasks in hospitals and assisted surgery.

At the end of 2021, the Authority for the Protection of Privacy published a document of recommendations concerning the use of wearables for sports and health purposes.

In this regard, Clalit provides its members with the "TytoHome" device that can be used at home, through which doctors can remotely perform a live examination and provide a diagnosis, treatment notes, and any referrals or prescriptions. The TytoHome kit allows for detailed health readings on critical areas of the body, such as the heart, lungs, ears, throat, abdomens and skin, as well as heart rate and body temperature. Another example is the CardioSen'C device of SHL, a portable device that monitors heart activity, and which can communicate the results instantaneously to a cardiologist.

5.2 Legal Implications

There is no specific legislation on digital health, hence general tort law applies. This includes, primarily, the tort of negligence and the regime of strict (no fault) liability under the Defective Products Liability Law, 5740-1980. Breach of contractual warranties may also come into play.

5.3 Cybersecurity and Data Protection

When using a cloud computing environment, questions arise regarding the privacy and security of the data uploaded to the cloud. When the cloud is located outside of Israel, questions arise regarding the authority to transfer such data outside the country's borders.

The Privacy Protection Regulations (Transfer of Personal Information to Databases Outside the State Borders) 5761-2001 set out conditions for transferring data abroad; for example, the party the data is transferred to must undertake to comply with the conditions for data retention and use applying to a database located in Israel (section 2 (4) of the Regulations). In July 2019, the MOH authorised, for the first time, hospitals and healthcare organisations to use cloud services. Alongside the benefits of using cloud services (such as digital medicine upgrading and cutting back on computing costs), there is concern about the theft of patient medical data and the risk of cyber-attacks. Oracle decided to set up a data centre in Israel, which will include two cloud servers: one designed for the government and security forces, with a particularly high level of security; and the other for the business sector, corporate clients, as well as start-ups.

The health sector was one of the ten most cyber-attacked sectors in Israel in 2021. Accordingly, in 2022, the MoH published basic principles for the regulation of cyber defences in the healthcare system alongside principles for integrating remote medicine systems into emergency medical centres. Furthermore, the Ministry of Justice and the Authority for the Protection of Privacy published a document concerning the protection of patient privacy in telemedicine services. On May 2023, an annual report of the state auditor on cyber and information systems was published, following a cyber-attack on Hillel Yaffe hospital in Hadera that occurred in mid-October 2021.

As to the local computing environment, concerns regarding the privacy and security of uploaded data still exists but can be minimised by setting forth and implementing data security standards. The Protection of Privacy Regulations (Data Security) 5777-2017 states that, in the event of a contract between a database owner and an outside entity for the purpose of receiving a service, a number of provisions must be stipulated in the agreement, including:

- the data that the outside entity may process and the purposes of the use permitted in the contract;
- the manner of implementation of data security obligations the holder has;
- the contract term; and
- the return of the data to the owner at the end of the contract.

The health data circulars prescribe the extent of protection over health data. In general, unless otherwise specified by law or approved by an explicit opt-in, any data under secondary use will be anonymised. Furthermore, the circulars set detailed conditions for privacy, medical confidentiality, standards for managing patient records in the health system, and data security.

5.4 Proposed Regulatory Developments

To date, there are no specific proposed regulations or regulatory guidance in the field of the internet of medical things.

6. Software as a Medical Device

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

Unfortunately, there is no statutory definition of software as a medical device. The registration of medical devices is entrusted to the medical accessories and devices (MAD) unit of the MoH. It must be noted that there is no legal requirement to obtain marketing approval for medical devices. The MAD unit nonetheless operates because HMOs and hospitals will not purchase non-approved devices. The MAD unit recognised US (510K) and EU (CE) approvals, meaning that holders of such approvals can easily obtain authorisations in Israel as well.

In December 2022, the MOH published a request to receive input regarding guiding principles for the development of AI-based technology in the digital health sector. The request was based on a similar request from the FDA in 2019 (Good Machine Learning Practice for Medical Device Development: Guiding Principles). The input received is currently being reviewed.

7. Telehealth

7.1 Role of Telehealth in Healthcare

To date, telehealth has been more widely used in Israel in some fields. However, just recently, in August 2022, the Authority for the Protection of Privacy published a document of key recommendations on the provision of remote medical services.

Patient-physician consultations through video calls have become popular but primarily after hours (through central service centres). Remote monitoring by means of handheld medical devices carried by patients in their homes has also become popular. This device not only monitors certain indices but also allows the physician to (partially) inspect the patient as if the patient were in the clinic, and to receive medical data obtained by remotely monitoring the patient using sensors. Surgeries have been conducted in hospitals with the participation of foreign experts through video calls. Virtual hospitals have not yet been established.

One of the concerns raised in the context of telemedicine is the digital divide and the concern that certain populations will be discriminated against and not be able to benefit from these new services.

As yet, there are no special regulations for cross-border provision of services and the general rules apply (meaning that non-licensed practitioners cannot provide health services from abroad).

7.2 Regulatory Environment

During the COVID-19 pandemic, certain relaxations of the regulatory scheme were made. For example, the guidelines regarding clinical trials were modified and relaxed in several aspects with a view to achieving social distancing during the informed consent process, and during meetings to discuss and approve the conduct of clinical trials, etc. Notably, studies on health data were exempted from certain approvals if the data was anonymised. All such relaxations were cancelled after the pandemic subsided.

7.3 Payment and Reimbursement

Almost all healthcare services are provided by the four major HMOs. The HMOs are funded by the government based on the number of patients they treat. The HMOs are generally not required to provide drugs and medical services not funded by the government. Each year, a special committee approves the introduction of new drugs and new technologies to the "healthcare basket", thereby requiring the HMOs to provide such solutions.

8. Internet of Medical Things

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

A host of technological developments have enabled the internet of medical things (IoMT) to develop to its current stage. One could begin with continuous improvements in authentic communications infrastructure (culminating in the recently introduced 5G network technology) that facilitates connectivity and bridges geographical gaps, improvements in computer vision, as well as various imaging techniques, coupled with the miniaturisation of chips and other hardware components, the increased computational power of computers, the development of highly sophisticated sensors (in particular, non-invasive wearable ones), the improvement in energy storage and battery life, and the maturity of machine learning and AI as applied to health data, to name just a few of the driving technologies.

The development of IoMT facilitates a wide scope of functionalities, such as remote monitoring; remote measurements of patients' indices, such as pacemaker monitoring, infusion pumps, insulin pumps and implant condition monitoring; as well as control and management of available resources and assets, building control and monitoring the environment of patients.

However, the growing use of these components and technologies results in increased exposure to cyberthreats, privacy risks through the exploitation of existing vulnerabilities, hostile takeovers and the like.

In order to assist health organisations in addressing these risks, the National Cyber Authority published in late 2020 a guide entitled "IoMT-Based Medical Device Protection Recommendations", which concerns actions and controls to strengthen IoMT devices, while making recommendations for dedicated controls. The guide builds on classifications published by the Cloud Security Alliance (Managing the Risk for Medical Devices Connected to the Cloud). As it states, it should be remembered that there is no single technology applicable for all types of systems. Therefore, cyber protection for IoMT components has necessitated requirements for the protection of such components as well as protection from them. Also, a variety of components are provided by a variety of vendors and not everyone comes with the same security settings. These facts make it difficult to create standardisation and uniform component management. This results in a need to protect IoMT components and their environments while combining different controls (policies, technologies, code, and hardware).

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

The introduction of 5G networks is expected to have a major beneficial impact on the healthcare industry. Owing to its high bandwidth, high speed and improved latency and error rate, 5G technology is expected to:

- be more secure and reliable;
- better facilitate remote monitoring and telemedicine;
- enable sophisticated surgeries conducted from remote locations and improved machine learning capabilities, particularly with respect to large image files;
- enable high computing power to mobile devices dependent on communications;
- obviate the need for close proximity between machine learning servers and data sets; and
- facilitate global immediately available medical consultation and other similar improvements.

The deployment of 5G networks in Israel is slowly progressing. As part of the activity and enforcement plan of the Authority for the Protection of Privacy in preparation for the deployment of the network, adjustments are also required regarding digital health and TELEHEALTH applications.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

The key legal issues in using and sharing personal health in research and clinical settings are as follows.

- Compliance with the requirements imposed by the privacy protection regulatory scheme. These include the maintenance of appropriate data security protocols, the use of collected data solely for the purpose declared upon collection, and the registration of databases containing sensitive health information.
- On 7 May 2023, new regulations were adopted with stricter instructions that set a higher bar for maintaining information that came from the EU.
- Compliance with the requirements imposed by the MoH regarding the use and sharing of health information. These include the requirement to maintain the anonymity of patients through anonymisation, aggregation and sometimes the use of synthetic data; the need to obtain approval for the conduct of clinical trials as big data research is considered a type of clinical trial requiring pre-approval; limitations on the grant of exclusivity for conducting big data studies; certain limitations on the permissible nature of big data studies; and requirements pertaining to their contractual undertakings for entities wishing to have access to health data in order to conduct studies, etc.

There are no different regulatory frameworks for data use or for data sharing. The distinction made is between primary use, which is use of a person's health data (including identifiable data) substantially for the purpose of treatment of that particular individual, and secondary use, which is defined as any other use. Primary use does not require the patient's consent. Secondary use requires either the patient's informed consent (opt-in) or the use of anonymised data (which, if done properly, means a patient's consent does not need to be obtained).

In this context, the MoH recently launched the "World of Data" platform, which allows the public to see a broad picture of the health system and the quality of its medical care.

Alongside this, a national platform was launched for conducting big data research in health data (research infrastructure for huge data). The platform is intended to serve the research community in conducting groundbreaking research in the field of health, by collecting health data from HMOs, but it faces difficulties and considerable barriers with regards to its implementation.

There are cases when the comparison of anonymised data with other data sources can result in re-identification. When access to the other data source requires informed consent (such as genetic data), the patient will typically be requested to provide consent to access their other phenotypic data. Alternatively, the database holder (eg, the HMO) will provide the researcher with unique keys that enable only the HMO but not the external researcher to connect and then analyse data with the identified data of the patient.

Informed consent may be obtained either by traditional means or by digital means. When digital means are used, this must be done in a procedure published by the MoH in October 2020. The general rule is that there must be a face-to-face meeting between the participant in the trial and the researchers. However, such a meeting can be conducted virtually and not necessarily in person. When choosing whether to make use of digital means in the process of obtaining informed consent, one must examine, among other things, the balance between the benefit of using such means and the associated risks, the severity of the medical intervention in the clinical trial, the characteristics of the target population and their level of access to the proposed digital means, the number of participants and their level of access to the place where the trial is conducted.

One declared goal of the procedure is to prevent the exclusion of various populations, particularly in light of the digital divide. Lastly, when asking a patient to opt in to participate in studies and activities that do not have direct benefits for such person, it is preferable to obtain their opt-in consent through a special recruiter instead of the attending physician.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

The regulatory scheme mainly addresses the issues of data security, data sharing, secondary use, accessibility to personal health data, ethics and anonymisation. It does not yet regulate the utilisation of AI and machine learning in general or the digital healthcare industry in particular.

Machine learning is particularly useful in the healthcare industry in research fields such as computer vision (the analysis of images for the purpose of diagnostics); associations between phenomena that are useful, for example, for drug repurposing and identifying novel indicators useful to predict illness; and harnessing collective wisdom, namely by creating algorithms for decision support systems that match or even outperform the output of large peer consultations.

One of the challenges for training machine learning algorithms is the need for access to sufficiently large and representative data sets and the need for removing bias underlying past decisions studied by the algorithm. Luckily, the data sets of the two large HMOs in Israel are relatively large. Nevertheless, when a particular research topic requires the pulling of data from different sources, the process is still cumbersome. Another limiting factor is the need to have geographical proximity between the machine learning server and data set.

Natural language processing (NLP) is particularly useful in big data analysis of interactions between a physician or a therapist and their patient. NLP may also be useful in the digitisation of handwritten records.

Research involving genetic data poses substantial privacy risks due to its inherent sensitivity. While in other use cases, such as studying medical conditions, the risk lies in the potential for an attacker to connect the data to a specific individual, genetic data takes this a step further. The genetic data inherently pertains to the individual's identity, making it a high-risk category for sensitive information misuse.

11.2 AI and Machine Learning Data Under Privacy Regulations

To date, there are no specific enacted regulations that address the use of AI and machine learning data in healthcare.

However, an Artificial Intelligence and Data Science Committee was appointed in February 2020 by TLM (the Forum for National Infrastructures for Research and Development), with the aim of examining the need for government intervention to accelerate the development of Artificial Intelligence and Data Science.

The committee recommended that future regulation in the field of AI should address the following:

- "Enabling regulation", namely a regulation that enables a rapid technological development that is not slowed down by out-of-date regulation;
- standardisation and legislation of algorithms, models and data;
- purchase and sale policy of algorithms and products, especially regarding products of the security forces;
- establishment of data centres and platforms for data sharing and models; and
- data management, cybersecurity and information protection.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Companies that develop and sell new digital healthcare technologies must comply with the provisions of the health data circulars, as well as with the provisions of the law and the privacy regulations (if the technology collects personal data).

Agreements with public healthcare companies require that special attention be given to the regulatory environment of the healthcare entity (eg, an HMO):

- Public-regulated healthcare entities are limited in their ability to hold equity in non-healthcare companies.
- Public-regulated healthcare entities are restricted in their ability to accede to requests for non-compete/exclusivity arrangements.
- Healthcare organisations involved in the development of new technologies will typically consider implications of the operations, such as the duty to call back, the cost of adding a new technology to their basket of services, etc.
- In addition to access to data, healthcare organisations may serve as an alpha site for the development of new technologies.

In general, the lack of stringent digital health enforcement in Israel creates a more accessible landscape for the digital healthcare market.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

The IT infrastructure of the HMOs providing care to the majority of the patient population in Israel is well developed to support digital healthcare. The same is true for the main large hospitals. Some of the challenges ahead include:

- commonly accepted standardisation of classification of clinical data;
- digitisation of old records;
- data curation;
- establishing infrastructure and promoting participation in platforms for the pulling of clinical information; and
- securing the resources necessary to recruit patients when opt-in is required, such as genetic and bio-sample studies.

13.2 Data Management and Regulatory Impact

To date, there are no specific proposed regulations or enacted regulations regarding the implementation of IT upgrades. In general, the manner in which data is managed is not statutorily regulated, except for regulation in connection with the protection of data privacy (Protection of Privacy Law, 5741-1981 and Protection of Privacy Regulations (Data Security) 5777-2017) and the health data circulars aimed at regulating secondary use of health data and big data research.

14. Intellectual Property

14.1 Scope of Protection

Patents are generally available for any invention that is a product or a process in any technological field that is novel, non-obvious, useful and capable of industrial application. A noteworthy exception to patentability is the prohibition of patents for a process of medical treatment of humans. This exception, coupled with case law trends concerning patentable subject matter, sometimes creates hurdles in pursuit of patent protection for inventions relating to personalised medicine. The territorial limitation of patents (patents being enforceable only within the territory of the country where they were registered) requires careful drafting of claims of patents relating to ex vivo diagnostics of medical conditions.

Copyright protects software as a literary work, but such protection generally extends only to the way of expression rather than the functionality and technological ideas underlying the code. The latter should be protected by patents where possible. Data sets are generally not protected by copyright and there is no sui generis database protection in Israel.

Trade secret protection is available in Israel and may protect confidential information, including non-patentable inventions and non-copyrightable data sets. However, in order to benefit from such protection, the information must be kept confidential, and the owner of the confidential information must show that they took reasonable efforts to protect the confidentiality of the trade secrets. Reverse engineering, as such, is permissible.

There is no case law, as yet, regarding inventions and works of authorship created by AI technologies without direct human contributions. However, it would seems that any person who was involved in the process of creation and has provided inventive contribution to the inventive concept of the invention (under the classic inventorship criteria) should be deemed an inventor.

14.2 Advantages and Disadvantages of Protections

In general, IP rights in the field of healthcare are difficult to enforce, since there is a convention that healthcare should be for the benefit of the public and enforcing rights in this field can be deemed as harming access to health.

Patent protection is governed by the Patents Law, 5727-1967. The law defines a patentable invention as one that is a product or process in any area of technology, which is novel, has inventive step, and has utility and industrial application. However, the law excludes a certain type of invention: a process for human medical treatment. Diagnostic and veterinary methods are not excluded per se.

A discovery, scientific theory, mathematical formula, game rules and computer software, are not patentable per se, due to case-law precedents. In general, if the invention involves a technological solution to a technological problem, it is patentable, whether the solution is in the software, or not. There is no specific legislation applicable to digital health inventions and every application is examined on its merits.

There are some difficulties in protecting software and algorithms, since, on the one hand, patentability issues may arise, and, on the other hand it is difficult to enforce such rights from the evidentiary aspect (to prove that the competitor copied the code).

Copyright protection is governed by the Copyright Law, 5768-2007. Copyright law protection may be particularly relevant to software and certain compilations of data, but there is no protection of databases per se.

As of 2018, icons, graphical user interfaces and screen presentations are not protected by copyright, but rather by the Designs Law, 5777-2017. Non-registered designs are protected for three years and registered designs are protected for up to 25 years.

Trade secret protection is governed by the Commercial Torts Law, 5759-1999. A trade secret is defined as "business information, of all kinds, which is not in the public domain and is not easily disclosed by others lawfully, and the confidentiality of which affords its owners a business advantage over their competitors, provided that its owners take reasonable steps in protecting its confidentiality".

The law prohibits misappropriation of a trade secret which is defined as:

(i) taking a trade secret without the owner's consent by improper means, or the use of the secret by the acquirer;

(ii) use of a trade secret without the consent of its owner where the use is contrary to a contractual obligation or a duty of trust the user has to the trade secret owner; and

(iii) acquiring a trade secret or using it without the consent of its owners, where it is clear that the trade secret has been unlawfully obtained according to (i) or (ii).

It should be noted that disclosure of a trade secret through reverse engineering will not, in itself, be regarded as improper. Health data is a classic example of a trade secret but the requirement of keeping it "not easily disclosed by others" can be difficult while using AI technologies.

14.3 Licensing Structures

The health data circulars set forth the provisions to be included in collaboration agreements based on secondary uses of health data (such as the purpose of using the data or maintaining the confidentiality of the data). In general, the main contractual issues that need to be taken into account are:

- ownership of data;
- ownership of know-how products based on collaborations through which data is used;
- consideration for data sharing or know-how products based on use of the data, such as ownership in the outside organisation (if a company is concerned);
- right to use the know-how products;
- monetary compensation (such as royalties, licence fees, exit fees);
- period of use of the data;
- exclusivity of the data's use;
- reach through royalties/licences;
- royalty rate and stacking; and
- the need to use other databases.

In general, HMOs request monetary considerations and rights to use the products, based on use of the data they grant access to. The issue of royalty-stacking may arise, leading to a burden of royalties to be paid by start-ups.

14.4 Research in Academic Institutions

Employers, including universities and healthcare institutions, will generally be the owners of IP rights generated by their employees in connection with their employment. This is both in terms of the default rule under the Patents Law and the Copyright Law, as well as the standard practices of such organisations, which often expand beyond the statutory provisions by means of employment contracts and intellectual property by-laws. All academic institutions share the revenues collected by the commercialisation of such intellectual property with the researchers. HMOs differ in their approaches and practices. The allocation of IP rights when private sector technology companies are involved in developing the device or medical innovation is typically governed by contract. Special provisions apply to governmental hospitals, which are more limited in their ability to contract with the private sector.

14.5 Contracts and Collaborative Developments

The default rule is that any person who made an inventive contribution to the inventive concept of the invention is an inventor and is the owner of the invention. When there are several co-inventors, they will be co-owners (unless they are in the employ of a third party, in which case the employer will own a share of the invention). All of these default rules may be superseded by contract.

It is standard practice to distinguish between background IP and foreground IP, with ownership of the background IP remaining with the original owner, who may grant limited licences to use the background IP in order to exploit the foreground IP, and the foreground IP being owned as agreed by the parties. Because of regulatory constraints and other considerations, many HMOs will waive co-ownership in exchange for various monetary rights, such as royalties, milestone payments, exit phase, cross-licence or the right to use the resulting foreground IP.

15. Liability

15.1 Patient Care

The first theory of liability arising from decisions based on digital health technologies such as data analytics, AI, machine learning and software as a medical device is, of course, the tort of negligence. In general, the three main elements of this tort are the existence of a duty of care, deviation from a reasonable standard of practice, and a causal connection between the defendant's act or omission and the damage suffered by the plaintiff. The manufacturer of a medical device will generally be held to owe a duty of care towards users of the device. Adherence to acceptable standards should mitigate the risk of liability. Otherwise, the manufacturer will have to show that it took reasonable efforts to prevent the damage, with the foreseeability of the damage and the level of efforts required being directly related, namely, the more foreseeable the damage is, the higher the level of efforts required.

It is hard to see how a decision to use an approved medical device can be deemed negligent. However, a decision to use a medical device in development could theoretically attract liability and the putative defendant would have to show that they took reasonable measures to verify that the device's algorithm would not cause harm or produce misleading results. As is the case with other industries, the courts will have to acquaint themselves with the developing best practices that aim to deal with the problem of lack of transparency of machine learning algorithms.

If a medical device inflicted physical damage on a patient, the manufacturer of the device may be held liable under the Defective Product Liability Law, which imposes a strict liability (no fault) on the manufacturer.

15.2 Commercial

Theories of liability when third-party vendors' products or services cause harm to healthcare institutions are generally the same as those discussed in **15.1 Patient Care**. The main difference, however, is the ability of the healthcare institution to protect itself through contract by obtaining proper warranties and indemnification obligations. In addition, health institutions may forfeit at least part of the right for compensation if they are shown to have breached their obligation to mitigate damage. Thus, some institutions already proactively monitor their internet-connected equipment to detect vulnerabilities and prevent cyber-attacks.