Chambers
Global Practice
Guides

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

Digital Healthcare 2022

Greece

Nikitas Fortsakis
Evangelos Courakis
Konstantinos Kritsotakis
Dimitrios Andriopoulos

practiceguides.chambers.com

GREECE

Law and Practice

Contributed by:
Nikitas P. Fortsakis, Evangelos N. Courakis, Konstantinos Kritsotakis and Dimitrios Andriopoulos
Koutalidis Law Firm see p.25

CONTENTS

Contributed by: *Nikitas P. Fortsakis, Evangelos N. Courakis, Konstantinos Kritsotakis and Dimitrios Andriopoulos,* ***Koutalidis Law Firm***

1. DIGITAL HEALTHCARE OVERVIEW

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Definitions and Main Differences

Digital healthcare or digital health (used interchangeably herein) may broadly be defined as a set of patient-engaging and/or consumer-engaging technologies (both hardware and software solutions and services), platforms and systems utilised for health-related purposes (including lifestyle and wellness) – often in service of supporting life science and clinical operations – and which are largely dependent on the collection, storage and transmission of health data. In this sense, digital health is the place where technology, day-to-day life and health care meet; and is thus aimed at both patients and consumers.

Digital medicine is a narrower term that conceptually falls within the framework of digital healthcare. Digital medicine focuses on evidence-based software and hardware products that perform two main functions, measurement and intervention, in the service of human health (including treatment, recovery, disease prevention and health promotion). In this sense, digital medicine, as a subset of digital healthcare, is mainly aimed at patients.

Digital therapeutics are software-driven, evidence-based therapeutic efforts to prevent, manage and/or treat a medical condition, disease or disorder. Digital therapeutics use mobile devices, apps, sensors, etc to aid patients (or persons supporting them) in (self-)managing their symptoms and/or creating customised health services.

The Healthcare Provider's Perspective

The variety of computational technologies and analysis techniques, smart devices and communication media – themselves the result of the development of interconnected health systems, with which digital healthcare is concerned – assist the healthcare provider (HCP) in performing its "traditional" dual function of preventing and managing illnesses and health risks and promoting health and general well-being. The HCP role in digital healthcare is perhaps most salient in the context of telemedicine or virtual care (ie, the provision of healthcare services through the use of information and communication technologies (ICTs) when the HCP and the patient are not in the same location) one of the main technologies used in the context of digital healthcare.

As in the case of digital healthcare, the HCP is also assisted in the practice of digital medicine, for instance through the use of evidence-based, digital medicine tools, such as measurement products (eg, digital biomarkers tracking change in tremors in Parkinson's patients), intervention products (eg, insulin pumps) or a combination of the two (eg, continuous glucose monitors in diabetes patients). At the same time, the HCP may also act in a scientific or research capacity, either by being part of the discovery and development of safe and ethical digital medicine products or by designing or executing clinical studies for digital tools.

The Patient or Consumer Perspective

Patients and/or consumers are the main stakeholders in digital health and digital medicine and digital therapeutics and the main (if not only) reason for the existence of and rapid development in the fields. In the context of digital health, these persons can act both as end users (eg, through the use of wearable devices tracking and collecting consumer health information) and patients (eg, in the context of telehealth or e-prescriptions).

The Regulatory Perspective

Digital healthcare is generally a less-regulated field than digital medicine. Most digital health

products (eg, wearables, health tracking apps, virtual assistants) do not require regulatory oversight from healthcare regulatory agencies (see **2.1 Healthcare Regulatory Agencies**). As is the nature of innovative products and services that are heavily reliant on sensitive personal data, digital health products can of course be subject to the regulatory oversight of non-healthcare regulators (see **3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies**).

Conversely, because of its evidence-based nature, digital medicine typically requires clinical evidence (ie, updates collected from randomised controlled trials), clearance and/or approval and is generally subject to heavy scrutiny by health regulators prior to its launch (and throughout its life cycle) (see **2.2 Recent Regulatory Developments** and **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies**).

At the EU level, the clinical investigation and sale of medical devices for human use is regulated by Regulation (EU) 2017/745.

The Technology Perspective

While digital health, digital medicine and digital therapeutics do make use of emerging technologies, such as AI and machine learning (ML) and big data analytics (see **1.3 New Technologies**), some technologies, such as electronic communication networks and virtual/augmented reality, are more relevant in digital health, while others, such as decision support software and robotic medicine, are more pertinent to digital medicine. Mobile devices, apps and sensors are more associated with digital therapeutics.

1.2 Regulatory Definition

Greek law does not have a definition of digital heath, digital medicine or digital therapeutics. On the issue of "e-Health", the Greek Ministry of Health (MoH) website refers to the definitions used by the World Health Organization (WHO): "[...] the efficient and safe use of [ICTs] in support of health and health-related fields, including healthcare, monitoring and treatment, research and knowledge". The European Commission defines e-health as, "[...] tools and services that use [ICTs] to improve prevention, diagnosis, treatment, monitoring and management of health-related issues and to monitor and manage lifestyle-habits that impact health."

As mentioned in **1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics**, most digital health products and services are not subject to regulatory oversight by health regulators.

1.3 New Technologies

Some of the key technologies in digital health and digital medicine are:

- AI and ML;
- robotic medicine;
- wearable devices;
- cloud-based integration of medical devices;
- electronic communication networks (fibre optics and 5G networks);
- 3D organ bioprinting for transplantation;
- big data analytics;
- sensor technology;
- virtual and augmented reality (VR and AR);
- genomics (CRISPR/Cas9);
- internet of things (IoT) and 5G technology in telesurgery;
- cryonics; and
- application technology.

Most of the aforementioned technologies apply to and concern not only digital healthcare and digital medicine but also digital therapeutics (eg, sensors technology and big data analytics), but some are more relevant to one than the other. For instance, wearable devices and telemedicine are at the core of digital health, while 3D organ

bioprinting for transplantation and genomics are closer to the digital health subset of digital medicine.

1.4 Emerging Legal Issues

The proliferation of digitalisation in the healthcare sector and the accompanying ever-growing need for collecting, storing and making use of electronic records containing sensitive data highlights the issue of data protection from unauthorised release and cybersecurity. Furthermore, the launch of innovative digital medical products creates – and will continue to create – issues of medical regulatory authorisations, copyright, safety and security, as well as issues of liability (eg, when the medical product in question is being used by an HCP relying on an automated diagnosis) and patient (information) rights.

1.5 Impact of COVID-19

The COVID-19 pandemic brought about a number of changes to the way healthcare is provided, most notably by increasing the pace of digitalisation that was already underway. Some of the most significant changes include:

- remote or in-person care to COVID-19 patients using modern and safe technological;
- remote guidance, counselling and support to COVID-19 patients;
- e-prescriptions without the need for the physical presence of the patient; and
- mapping and contact tracing technologies.

While created or pushed forward as a means to tackle the global pandemic, most of the above are expected to remain post-pandemic (see **7.2 Regulatory Environment**).

2. HEALTHCARE REGULATORY ENVIRONMENT

2.1 Healthcare Regulatory Agencies

The Greek MoH

The core regulatory authority for healthcare in Greece is the MoH, responsible for – among others – defending, protecting and promoting public healthcare; ensuring universal and equal access to the provision of healthcare services by the National Healthcare System (Greek NHS); and regulating the operation of and exercising supervision of private healthcare institutions.

Specialised Regulatory Agencies

Specialised regulatory agencies and organisations also exercise control over their respective sectors of responsibility. Such regulatory agencies include the National Organisation for Medicines (EOF), the National Organization for the Provision of Health Services (EOPYY), the National Public Health Organisation (EODY), the Regional Health Administrations (YPEs) (comprising public hospitals in each region and other special departments) as well as the Hellenic Association of Pharmaceutical Companies, the National Doctors' Association and the National Pharmacists' Association and all respective regional associations. More specialised agencies are:

- the EOF's Institute of Pharmaceutical Research and Technology (IFET);
- MoH's National Council for eHealth Governance (ESDHY); and
- other non-profit or professional associations.

EOF and IFET

The EOF is the authority responsible for the protection of public health, as well as the safeguarding of the public interest in the field of medicines and other related products, ensuring adequate circulation of tested and quality products and

the promotion and development of technology and research in the field of healthcare. Among other responsibilities, the EOF has supervision over medicinal products, active substances and medical equipment.

The IFET – a subsidiary of the EOF – mainly engages in the production, importation and distribution of pharmaceutical products by private pharmaceutical companies, which are not marketed in Greece but are deemed to be indispensable for patients' treatment and the protection of public health.

EOPYY, EODY and YPEs

The EOPYY's responsibilities pertain to social insurance and the EODY's competence pertains to enhancing the Greek NHS, while doctors' and pharmacists' associations have competence over enforcing the licensing procedure and codes of conduct for healthcare professionals. The YPEs are responsible for issuing the relevant licences for the operation of private hospitals and pharmacies.

There is no express provision that digital healthcare falls within the scope of the EOF. However, according to Greek Law 1316/1983, the EOF's regulatory supervision includes technologically evolved medicinal products and various medical aids such as medical equipment used for diagnostics, treatment. The EOF has been deemed the competent regulatory authority for the inspection of marketing of medical devices in Greece under Greek law and EU Directives. EOF will maintain this authority following the implementation Regulation (EU) 2017/745, the Medical Device Regulation (MDR) and of Regulation (EU) 2017/746 for in vitro diagnostic medical devices (IVDR).

ESDHY

The ESDHY's purpose is to provide consulting and advisory services to the MoH and to recommend policy priorities, action plans and necessary institutional reforms.

EDiT

Specifically, regarding telemedicine, the National Telemedicine Network (EDiT), established by the second YPE of Piraeus and the Aegean, has installed telemedicine systems in 43 healthcare units. The EDiT provides the following services:

- teleconsulting;
- tele-education;
- tele-psychiatry; and
- the establishment of special healthcare units.

Telehealth in Greece was mainly promoted to address the issues of lack of healthcare professionals and infrastructure in remote areas, the remote islands of the Aegean Sea.

2.2 Recent Regulatory Developments

Digital healthcare in Greece has been on the regulatory agenda for several years without constituting the regulator's main point of interest. The core legislative act focusing on digital healthcare regulation is Greek Law 3984/2011, which provides that the use of telemedicine methods is the responsibility of the HCP and according to the doctors' code of conduct. The regulatory framework for medical devices also sets out generic rules that are directly relevant to digital healthcare.

However, the integration of digital healthcare in the Greek NHS recently drew specific regulatory attention with the adoption of EDiT for telemedicine systems (see **2.1 Healthcare Regulatory Agencies**). Another important development has been the digital prescription of medicines/medical examinations. The introduction of a more specialised regulatory framework for medical devices, brought about by the aforementioned MDR and IVDR (see **2.1 Healthcare Regulatory**

Agencies), is another important development shaping the field.

More broadly, the last couple of years have seen digital healthcare methods being promoted by regulatory agencies and hospitals. The COVID-19 pandemic exposed the need for more technology and innovation in the healthcare sector and pushed for changes in the digitalisation of healthcare, through the introduction of a special digital procedure for the supervision of COVID-19 patients as well as the establishment of specific telemedicine departments. Against this backdrop, hospitals can issue guidelines on the utilisation of digital healthcare methods – albeit these would merely be for advisory purposes to HCPs, with the latter bearing the ultimate responsibility for the use of such methods.

2.3 Regulatory Enforcement

Regulatory enforcement is particularly active in the areas of circulation of medical products in the Greek market, licensing procedures for HCPs and private clinics, prudent exercise of healthcare-related professions and control over medicine prescription and reimbursement for the costs of medicines. The rationale behind these regulations is (i) the protection of public health by not allowing potentially dangerous or misleading products to reach patients/consumers and (ii) placing restrictions on the exercise of medical practices.

3. NON-HEALTHCARE REGULATORY AGENCIES

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

Technological advances in the healthcare sector have necessarily entered the regulatory radar of authorities that are not subject to the supervision of the MoH such as the following.

The Hellenic Data Protection Authority

Perhaps the most important issue that digital healthcare raises is the processing of sensitive personal data. Accordingly, the Hellenic Data Protection Authority (HDPA) plays a big role in digital health and digital medicine. The HDPA is concerned with issues relating to the collection, processing, saving, filing, transferring, etc of personal data and generally with ensuring the application of Regulation (EU) 2016/679 (GDPR) and the relevant personal data protection national legislation. The general scope of the HDPA's competence allows it to intervene by issuing guidelines and enforcing the personal data protection legislation where necessary. Against this backdrop, the HDPA has dealt with many cases of personal data protection in the healthcare sector.

The Ministry of Digital Governance

In the context of cybersecurity (which, as mentioned in **1.4 Emerging Legal Issues**, is a key legal issue to digital health and digital medicine), the Ministry of Digital Governance and its General Secretariat of Cybersecurity provide regulatory services for the security of informatic systems.

The Hellenic Authority for Communication Security and Privacy and the Hellenic Telecommunications and Post Commission

In the context of electronic communication networks (which, as mentioned in 1.3 New Technologies, is one of the key technologies to digital health and digital medicine), the Hellenic Authority for Communication Security and Privacy (ADAE) and the Hellenic Telecommunications and Post Commission (EETT), namely, the authorities responsible for the security of the public electronic communication networks, also play a key role in regulating digital health and digital medicine.

Other Non-health Regulators

The Hellenic Copyright Organisation is another non-healthcare regulator that plays a significant role in digital healthcare and digital medicine since they involve patents on innovative products and services. The Greek Standardisation Organisation contributes to the European standardisation process and participates in the preparation of relevant guidelines. Other non-profit or professional associations are also involved in the regulatory process.

Unregulated Areas

Other areas of healthcare and digital monitoring, such as the areas of wellness, fitness and self-care are not strictly regulated in Greece. Nevertheless, the law provides that these activities are promoted and managed by professionals.

New healthcare technologies are steadily affecting different regulatory fields, calling for convergence and co-operation between regulatory authorities. The HDPA has already been alerted by the emergence of digital healthcare methods, while other authorities are also expected to become involved as digital healthcare expands and becomes even more integrated into Greece's NHS. In any case, the radical advances that digital healthcare entails shall test the reflexes of many regulatory agencies, necessitating the adoption of a co-ordinated action plan.

4. PREVENTATIVE HEALTHCARE

4.1 Preventative Versus Diagnostic Healthcare

Preventative healthcare refers to the system of timely interventions to protect against or treat diseases or other harmful-to-health conditions. Preventative healthcare may take various forms, such as population screening (eg, of high-risk groups) with the primary purpose of early diagnosis and/or informing and providing awareness to the population about specific diseases or other harmful-to-health conditions.

Diagnostic healthcare, on the other hand, refers to the process of identifying a disease, condition, or injury from its signs and symptoms. Diagnostic checks in this regard include physical examination and testing (eg, blood tests, imaging tests, biopsies).

Technological developments, however, allow for new or additional ways to provide preventative and diagnostic healthcare to the general population. New tools, such as the Internet of Medical Things (IoMT) – for example, sensor technology – allow HCPs to achieve better results and maintain better and more detailed records of their patients, as well as to pre-emptively cope with any eventuality. Such tools also allow for quick – even painless – and, if required, continuous examination of the patient for an effective diagnosis.

However, wellness and fitness devices should not be discounted with regard to the preventative healthcare solutions they offer since such devices allow individuals to also monitor themselves. For example, these devices may provide feedback regarding the physical activity and physical status of an individual, as well as promote a healthier lifestyle.

4.2 Increased Preventative Healthcare

There are doubtless numerous reasons as to why preventative healthcare has increased to such an extent. Advances in technological capabilities (such as AI, IoMT and wearables), cost savings, healthcare insurance developments and social trends, such as fitness and wellness, are just a few.

The COVID-19 pandemic has also contributed to the increased use of preventative healthcare,

either through awareness provision or vaccination of the population, etc. The extensive use of social media and new technologies' penetration in Greek society have also been among the reasons that preventative healthcare is gradually increasing in Greece.

Despite the high cost-savings that may be achieved by the adoption of preventative healthcare, Greece ranks among the EU countries with the lowest expenditure on preventative care (1.3% according to Eurostat calculations for 2018).

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

General wellness products (eg, wellness, fitness and self-care) are not currently strictly regulated in Greece. These products could also be considered medical devices, meaning they would have to pass through the strict regulatory framework of the MDR and IVDR.

However, personal information gathered through such devices falls under the regulatory framework of the applicable personal data legislation (eg, the GDPR, Greek Law 4624). For information regarding personal data protection, see **10. Data Use and Data Sharing**.

4.4 Regulatory Developments

The EODY is the operational centre for the planning and implementation of public health protection actions in Greece with preventative, operational and interventionist responsibilities and is supervised by the MoH. Its aim is to defend and promote the health of the population of Greece and to protect public health by:

- monitoring and assessing the health of the country's population and the biological, socio-economic and environmental parameters affecting it;
- continuous monitoring and recording the impact of diseases, both infectious and non-communicable, on public health;
- taking preventative measures and providing the population with ongoing information to protect health and ensuring its well-being; and
- taking actions aimed at protecting the population from all kinds of threats arising from the spread of diseases or situations harmful to health.

4.5 Challenges Created by the Role of Non-healthcare Companies

Non-healthcare companies face challenges and requirements similar – albeit less stringent – to those faced by companies manufacturing medical devices.

Some of these are:

- forging connections with medical manufacturers, software application development companies, HCPs and the general public;
- having advanced architecture and data management systems to manage, analyse and process the data collected;
- having a solid cybersecurity framework and taking proper measures to protect the personal information.

5. WEARABLES, IMPLANTABLE AND DIGESTIBLES HEALTHCARE TECHNOLOGIES

5.1 Internet of Medical Things and Connected Device Environment

The use Bluetooth and/or near-field communications (NFC) technology and the improvement of wireless connectivity (speed and range) have

been key enablers for the enhanced use of connected devices in digital healthcare.

Nowadays, the development of cloud computing and storage is the main reason that humanity can keep hold of the vast amount of data gathered and analysed as a result of the digitalisation of healthcare.

The device environment interconnection is becoming key to the provision of healthcare and technological advancement has affected all areas of healthcare, irrespective of whether it is about the prevention or the treatment of a disease and regardless of whether this takes place remotely or in person.

5.2 Legal Implications

HCPs, medical service providers (eg, hospitals), as well as producers of medical devices may be subject to liability for adverse healthcare outcomes. The relevant provisions of the Greek Civil Code, consumer protection legislation and the code of medical ethics may all be applicable, in concreto, in this regard. For more details regarding liability, see **15.1 Patient Care** and **15.2 Commercial.**

5.3 Cybersecurity and Data Protection

Cybersecurity risks are present regardless of whether a device is running in or connected to a cloud computing environment or in an on-premises, local computing environment. The reason is that security breaches do not always require an "external attack or threat", being equally endangered by "internal threats"; in fact, they can even take place "accidentally".

Companies that collect, process and share health data should ensure a high level of protection for such information. Confidentiality, integrity and availability constitute the fundamental elements of cybersecurity and describe the basic aspects that should be followed within organisations as a guide to addressing information technology policies and for establishing the information security framework. Confidentiality is the basis for the rules that limit access to information, integrity ensures that the information is trustworthy and accurate, and availability guarantees reliable access to information by the persons authorised.

5.4 Proposed Regulatory Developments

The EU currently regulates the field of medical devices and in-vitro medical devices through two new regulations (the MDR passed down in 2021 and the IVDR in 2022), creating a robust, transparent and sustainable regulatory framework aimed at improving safety and creating fair market access.

Certain types of medical devices (eg, pacemakers) are likely to fall under the scope of other regulatory frameworks, such as the Radio Equipment Directive and thus be subject to the security requirement provisions therein.

More details regarding the relevant healthcare governing agencies can be found in **2.1 Healthcare Regulatory Agencies.** For information on software as a medical device see **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies**.

6. SOFTWARE AS A MEDICAL DEVICE

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

Regulatory Framework

According to EU and national legislation, software may be considered as a medical device under certain conditions. The regulatory framework on medical devices is therefore applicable on Software as a Medical Device (SaMD) and the

Medical Device Regulation (MDR), which defines the term SaMD.

The classification of Medical Device Software (MDSW) under the MDR takes place in accordance with Annex VIII to the MDR. MDSW is considered an active device and can be classified in all four risk classes, according to their intended purpose and their inherent risks. Stand-alone MDSW, such as most health apps, will be classified independently from any hardware medical device (Annex VIII, Chapter 2, paragraph 3.3 to the MDR) and will thus mainly be governed by Rule 11 of Annex VIII to the MDR.

To address the continuous software improvement, the EU is revising and re-drafting the relevant device standards in the context of the MDR and the IVDR (see **2.1 Healthcare Regulatory Agencies**). The European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) are the competent bodies for the adoption of harmonised standards. The first lists of MDR/IVDR harmonised standards were published in 2021. These standards are the cornerstone of the MDR and IVDR. The manufacturers will be able to argue that they have demonstrated compliance with the General Safety and Performance Requirements (GSPRs). On a national level, the EOF is the authority responsible for notifying the Commission and the authorities of other member states of the bodies designated to carry out the procedures.

According to the GSPRs for software, which are included in the new Section 17.2 of Annex I (MDR), software shall be developed and manufactured in accordance with the state of the art, taking into account the principles of development life cycle and risk management, including information security, verification and validation.

Developments in AI and ML

An extension of SaMD is ML software (ie, where the software device keeps learning automatically after it has been released into the market) which will also need to undergo the same MDR classification process and be classified as SaMD accordingly. However, the inherent issues of AI, bias, explainability and, mainly, accountability when suggestions or medical actions are triggered, are also present in ML software. In this regard, Greek Law 4780/2021 established the National Bioethics and Techno-ethics Commission, which has already issued opinions on – among others – Electronic Health Records (2015) Big Data in Health (2017).

Prospective Market Entrants

New entrants in the SaMD area should seek regulatory advice regarding understanding the nature of their solution/software and if and how it classifies as SaMD. There is EU guidance on the subject, especially from the Medical Device Coordination Group (MDCG). Concerning the conventional timeframes for approving a medical device, the CE Mark process is considered faster than others with less clinical evidence, especially in the case of self-certification. However, the safety and suitability of the products should be the main criteria for the assessment of regulatory systems.

Concerns relating to (sensitive) data privacy, data confidentiality, security, integrity and availability remain in the spotlight and given that a number of new healthcare, fitness and consumer products launched could be now considered medical devices, these products (previously not classified as such) need to be raised to the same standards. To launch new products, market entrants will need to establish new processes, software, tools and understand the relevant regulatory changes.

7. TELEHEALTH

7.1 Role of Telehealth in Healthcare

Telehealth is transforming the way healthcare services are accessed and provided. It allows for fast, high-quality and convenient care services in a cost-effective way. Using technology to deliver health care has several advantages. Prime examples of telehealth advantages include:

- remote diagnosis;
- remote patient monitoring (RPM);
- the ability to provide care to people with mobility limitations, or in rural areas; and
- cost savings.

In Greece, the adoption of digital healthcare infrastructure will be a key component in ensuring access to health care services in isolated geographical areas. An effective deployment of telehealth technologies will enhance the ability to better meet the healthcare needs of those in rural and frontier parts of the country.

However, there is currently no regulatory framework on telehealth and, as a result, issues such as data privacy, security or medical liability remain to be addressed and the ways to address them are still unclear.

Telehealth and Virtual Hospitals/Virtual Visits

In virtual hospitals, patients are connected with healthcare professionals remotely (via video or other technologies) in real-time for consultation on medical issues. Similarly, a virtual visit is the capability to consult with a doctor through a smartphone, tablet or computer, whether from home or work, without the need for an in-person appointment, regardless of the time of day.

Telehealth and Remote Healthcare

Constant monitoring of the patient's condition and performance of medical examinations away from medical facilities is described as remote medical care. This form of healthcare is performed with the use of specific technologies (such as mobile devices, wearables, sensors) to facilitate interaction between clinicians and patients at home.

As mentioned in **2.1 Healthcare Regulatory Agencies and 2.2 Recent Regulatory Developments**, the EDiT has installed telemedicine systems in 43 healthcare units, with further developments under way. Furthermore, as mentioned in **1.5 Impact of COVID-19** and **7.2 Regulatory Environment**, during the COVID-19 pandemic, the digital provision of services of public sector HCPs was promoted to allow for treatment, counselling and support of patients with COVID-19. However, such capabilities and tools have only been partially incorporated into the Greek NHS.

Notwithstanding, the use of telehealth raises issues of cross-border provision of services, especially regarding licensing and authorisation. Doctors generally obtain a licence to practice in a certain area and are subject to the legislation and rules of conduct (including, most notably, medical ethics rules) of that area.

The main liability considerations regarding cross-border provision of medical services include:

- patient rights;
- product liability;
- jurisdictional issues; and
- personal data.

7.2 Regulatory Environment

COVID-19 Treatment and Support

The COVID-19 pandemic brought about a series of regulatory changes in Greece. One of these changes was introduced by Greek Law 4690/2020, pursuant to which family doctors and contracted doctors of the EOPYY may provide services to patients suffering from COV-

ID-19 with home visits and remote sessions, using modern and safe technological means. It is uncertain whether such regulatory changes will become permanent.

E-prescriptions

One of the most innovative measures taken was the digital prescription of medicines/medical examinations. Greek Law 4704/2020 allows healthcare professionals to issue prescriptions electronically and even without the need for physical patient presence. The complete overhaul and digitalisation of the prescription regime has long been underway and constitutes a pivotal and permanent change in the Greek NHS.

Relaxation/Restriction of Legislation

Aside from introducing new regulatory frameworks, the COVID-19 crisis has also led to the relaxation – and even restriction – of the applicable legislation. Personal data and privacy, where tracking or mapping of contacts was used for identification or monitoring of the location of individuals, is a prime example of this. Furthermore, restrictions of fundamental rights and freedoms were implemented regarding movement, socialisation, etc. Measures (such as the use of masks, the COVID-pass) have been introduced and/or abolished according to the status of and pressures on the healthcare system, based on epidemiological data.

Challenges

The main challenges of the new national and international legislative framework are:

- promoting digital health;
- regulating technologies in order to ensure that patients receive treatment that is safe and up to specific standards; and
- responding to ethical issues.

7.3 Payment and Reimbursement

Regarding payment for telehealth services to patients with COVID-19, according to Greek Law 4690/2020, compensation for family doctors of the Primary Health Care Units and doctors having a contract with the EOPYY who make home visits is set at pre-fixed Euro amount per visit and per patient (for follow-up purposes).

Compensation for family doctors of the Primary Health Care Units of the Greek NHS and doctors having a contract with the EOPYY who provide distance services to patients with COVID-19 is also set at pre-fixed Euro amount (lower than for in-person visits) per session and per patient (for follow-up purposes).

Greek law also provides for a specific procedure for the compensation of doctors who offer healthcare services remotely (eg, issuance of medical prescriptions and/or medical consultation) during the COVID-19 pandemic.

It is uncertain if such regulatory changes will become permanent, or if their application will be further extended and/or if such provisions will cover other, similar cases.

8. INTERNET OF MEDICAL THINGS

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

Definition and Relevant Technological Developments

From a technical point of view, the IoMT is defined as a network of physical and virtual elements that monitor and electronically transmit medical data, such as vital signs, physical activity and medication adherence, to provide swift diagnosis and treatment by interconnecting to hospital and healthcare networks.

Contributed by: *Nikitas P. Fortsakis, Evangelos N. Courakis, Konstantinos Kritsotakis and Dimitrios Andriopoulos,* ***Koutalidis Law Firm***

The technological developments that have critically influenced and assisted the growth of the IoMT include:

- wireless technology;
- use of AI and ML;
- application technology growth;
- development of better and more secure internet and messaging protocols; and
- sensor technology.

Moreover, innovative uses of IoMT will be further enabled by the introduction of 5G networks, with low-latency support of millions of devices and increased bandwidth.

Regulatory and Security Risk Concerns

The main regulatory concerns for IoMT devices, such as wearables, implantables and mobile apps, is whether and to what extent they are subject to the relevant legal framework for medical devices. For example, depending on their classification, different regulatory schemes may be applicable. Other important subjects of regulatory nature are:

- privacy;
- security; and
- liabiilty.

From a regulatory and technological point of view, Greece remains at the same level as the majority of the EU member states and has not taken any extraordinary or individualised initiatives to promote the IoMT.

Security Risks

Categorisation does not distinguish connected and non-connected devices; however, connectivity increases the security risk of any device. On an EU level, the threats generated by the integration of IoMT systems are not yet fully captured by traditional risk assessment methodologies and relevant security controls for IoMT devices have still not yet been fully established, rather relying on the security landscape of generic IoT.

Cybersecurity infringement is a major security risk. Classic methods of cybersecurity attacks include:

- the exploitation of software vulnerabilities;
- social engineering tactics (phishing); and
- ransomware attacks.

Furthermore, non-intended exposure and internal misuse of data also pose a security risk. Mitigation efforts include the implementation of:

- security awareness and training programmes;
- boundary defence; and
- data by design and by default.

Mitigation and Best Practices

It should be noted that, due to IoMT hardware limitations (eg, battery constraints), some mitigation mechanisms are difficult (or even impossible) to implement and therefore these devices have a much wider threat coverage.

While cybersecurity of digital health should be prioritised, the Greek legislator has not yet specifically addressed it (see **13. Upgrading IT Infrastructure**). In addressing this matter, Greek authorities should consider global practices.

To date, several attempts have been made to regulate IoT, however, it is still remains largely unregulated. An example of non-regulated devices is shadow IoT devices such as Home Assistants (HA) which cannot be classified strictly as IoMT devices. Shadow IoT is becoming a real security challenge and HA devices can be a back door to the IoMT environment enabling unauthorised access and non-secure collection and processing of data, etc.

9. 5G NETWORKS

9.1 The Impact of 5G Networks on Digital Healthcare

Positive Effects of 5G on Digital Healthcare

In technical terms, 5G networks are characterised by:

- low latency ie, near real-time network responsiveness;
- wider bandwidth: for ultra-fast data sharing and guaranteed quality; and
- network reservation for a particular use.

These features make 5G the foundation for launching technologies, such as the IoT, AI, VR and AR. A number of healthcare areas could benefit from 5G, including:

- remote monitoring of health;
- the home care of patients;
- addressing the needs of patients in remote areas; and
- robotic surgery.

Telemedicine allows doctors and other clinical staff members to collaborate more efficiently to deliver healthcare to remote locations. With high-speed and reliable 5G networks, patients can be treated sooner and have access to specialists otherwise not available; improving access improves quality of care.

Using IoT devices or wearables will allow for reliable monitoring of patients not limited by network restrictions in terms of reliability, capacity, latency, etc. Healthcare organisations can use AI tools to provide the best care possible, from wherever they are. By enabling all these technologies through 5G networks, healthcare systems can improve the quality of care and patient experience, as well as reduce the cost of care.

The aforementioned capabilities are critical for first responders and disaster management. Deployment of 3C (Communications Command and Control) integrated solutions with the use of AR/VR, AI and IoT technologies will be accommodated by the ability to offer medical treatment using telemedicine or telesurgery thereby exploiting health resources of the remote hospitals on the scene.

In Greece, the established telemedicine network (see **2.1 Healthcare Regulatory Agencies**, **2.2 Recent Regulatory Developments** and **7.1 Role of Telehealth in Healthcare**) will benefit from the introduction of 5G, as the 5G spectrum has already been allocated to licensed mobile operators that are gradually deploying 5G service.

Contractual Considerations

The main contractual considerations that healthcare institutions face, are:

- the integrity of the platforms used, since – usually – providers use third party solutions that may impede security (confidentiality, integrity and availability); and
- assurance that privacy requirements set by the regulatory authorities are met.

10. DATA USE AND DATA SHARING

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

Using Versus Sharing of Personal Data

Data usage poses much fewer risks and concerns, regarding privacy and security, compared to data sharing. However, according to Article 4 of the GDPR, data use and data sharing both fall under the definition of processing.

Contributed by: *Nikitas P. Fortsakis, Evangelos N. Courakis, Konstantinos Kritsotakis and Dimitrios Andriopoulos,* ***Koutalidis Law Firm***

The Greek Legal Framework

The main applicable legislation, regarding data protection, that healthcare providers may be subject to is:

- the GDPR;
- Greek Law 4624/2019 (and Greek Law 2472/1997, some articles of which are still in force) which supplements GDPR;
- Law 3471/2006 regarding processing of data in the field of electronic communications; and
- Law 4577/2018, which implements the Network Information Systems (NIS) Directive.

Processing of Health Data Under the GDPR

Law 4624/2019 draws a distinction between data use by public and private sector bodies and introduces more favourable provisions on data processing by the latter. Greek Law 4624/2019 allows public authorities to process data also for purposes of national security and provision of humanitarian aid.

The processing of health data is, in general, prohibited under the GDPR, unless the exceptions of Article 9 paragraph 2 apply. HCPs should make every effort to achieve compliance with the applicable regulatory frameworks on personal data protection and security of networks and information systems. HCPs can do this by undertaking the following:

- finding the appropriate lawful basis of processing (based both on Articles 6 and 9 of the GDPR ie, consent, legal obligation, etc);
- taking all the appropriate technical and organisational measures;
- informing the data subjects on the processing activities and/or potential transfers of data, (which in the case of data transfers outside the European Economic Area, require additional measures and actions; and
- having in place the appropriate documentation and agreements (eg, data processing agreement or data processing impact assessment).

These are only some of the issues arising in connection with such data processing.

To make processing of personal data less complex, HCPs can process data following the basic principles of the GDPR, such as data minimisation and purpose limitation. Furthermore, de-identification methods, such as pseudonymisation, anonymisation and/or data aggregation, may be useful; however, they cannot ultimately guarantee security because reverse identification analysis may – in some cases – reveal private information. HCPs should follow an overlapping use of the basic GDPR principles and de-identification methods in order to address, to some extent, considerations of personal information privacy.

Patient Consent

Digital healthcare has changed the nature of patient consent. However, the GPDR tries to balance patient privacy rights and digital market development. European bodies such as the Article 29 Working Party (WP29) and the European Data Protection Board (EDPB) have issued opinions regarding consent (eg, Guidelines 05/2020, Opinion 3/2019). Controllers and Processors are advised to be cautious over the use of consent and should explore alternative legal grounds for a given purpose of data processing.

Patient consent for medical interventions is fundamental in both ethics and the law and patient consent is required whenever data is provided to persons not involved in patient treatment. Consent in the context of health data should be freely given, be specific, informed and unambiguous and explicit.

Changes Brought About by IoT Devices

However, IoT devices have changed the type and amount of data collected and the way data is being processed. Many ethical questions are raised about the use of data being captured especially by non-healthcare providers, for which the level of confidentiality and security does not always comply with the requirements of sensitive personal data. To date, there is still no clear legislative framework in the Greek law dealing with this issue.

Enforcement of the regulatory framework relevant to personal data is generally achieved through the imposition of severe administrative fines, of up to EUR20 million or up to 4% of global turnover. Furthermore, a breach of the GDPR could potentially establish and substantiate civil claims by the data subjects. Finally, violations of the GDPR may also entail criminal liability, especially regarding HCPs where the Code of Medical Ethics foresees the imposition of disciplinary sanctions by the competent disciplinary bodies.

11. AI AND MACHINE LEARNING

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

Application of AI in Digital Healthcare

AI's application in digital healthcare promotes, among other things, the analysis, screening and diagnosis of different conditions. To date, no specific EU or national legislation on AI is in place. It was only recently that the European Commission made a proposal for a regulation on harmonised rules on AI (the Artificial Intelligence Act). The proposal is under discussion.

Augmented intelligence (Aul) is an alternative approach to AI, which chooses to build on the concept of cognitive technology designed to enhance human intelligence rather than removing humans from the decision process.

The Assistive Role of AI

Medical associations endorse a conceptualisation of AI that focuses on its assistive role and results in the physicians' active involvement as a key control in any related process. Such checks and balances improve specific capabilities and leverage decision making and cognitive power and could thus help address the accountability issue in AI.

AI Concepts in ML

AI concepts also apply to ML. In the process of creating an ML model, the biggest portion of available datasets will be used as training data and the remaining as test data. The sources of such data may vary and can include cases of personal data, patient data (medical records), health statistics or even IP-protected data. In all cases, relevant laws and regulations apply to the collection (genuine not modified data), anonymisation (real-time when applicable), processing, transfer and minimisation of bias (ie, gender, race, or other personal characteristic).

As current developments ask for measures to create trustworthy AI (explainability/transparency remains a challenge as AI and primarily deep learning, is often characterised as a "black box") the provider should be reporting data quality (conformance, completeness and plausibility) or even apply external validation (eg, based on specific tools).

ML can provide physicians with relevant information to keep them up to date on medical progress and deliver accurate input into their decision-making process. It can also automate hospital and office processes and improve physicians' workflow using smart records. Furthermore, ML models can diagnose diseases or early signs of

various diseases (eg, Alzheimer's) or enable and enhance quicker drug development cycles.

ML-Associated Risks and Regulation

ML insights and data and systems, however, may be subject to risks such as corporate espionage, or taking over control of system by malicious parties. In general, areas where access to information is shared and the number of end users is increased pose a higher risk of data misuse and attack.

Regulating ML, therefore, may take place by:

- requiring the AI system to satisfy pre-defined requirements (lawfulness, ethics, robustness);
- regulating the AI system;
- controlling the development process; or
- adopting a licensing system to regulate developers.

AI and ML are indirectly regulated mainly through:

- the GDPR, which impacts all firms that utilise EU citizens' personal data, regardless of location and prohibiting the use of health data unless exceptions under Article 9 paragraph 2 GDPR apply;
- intellectual property; and
- product liability policies.

Natural Language Processing

Also relevant to AI is Natural Language Processing (NLP), which is the ability for a programme to recognise human communication as it is meant to be understood. NLP in healthcare is impacted by the wider EU AI regulatory frameworks mentioned previously (such as the GDPR) and industry standards, such as the Health Level Seven (HL7) and ISO standards (eg, ISO 11073). Uses of NLP include automation of mining clinical concepts from unstructured data, suggestion of codes to assist turning clinical documentation into rich data sources for capturing physicians' reports and recording diseases. Regulatory compliance itself can be assisted using NLP enabling extraction of intelligence embedded in internal and external regulatory data feeds/documents.

As already discussed, Greece uses the central Electronic Health Records (EHR) system hosted in the H-Cloud (the Government Cloud Health Sector; see **13.1 IT Upgrades for Digital Healthcare**). This approach provides for immediate access to accurate and up-to-date patient information regardless of time and location while ensuring maximum protection of privacy and security risks and imposing information access systems and security controls.

11.2 AI and Machine Learning Data Under Privacy Regulations

The EU Commission, in 2021, published its proposal of the Artificial Intelligence Act. This new legal framework on AI aims to fill the regulatory gap and establish the legal regime under which AI will be implemented, all the while trying to guarantee the safety and fundamental rights of people and businesses.

However, one of the dangers is the in-built bias and black box AI. These issues arise from the training data that will be 'fed' into the algorithm. There now seem to be no official regulatory guidelines around the use of training data. One of the ways to deal with such issues is transparency and this is what EU regulators will be asking from the producers, according to the AI Act.

12. HEALTHCARE COMPANIES

12.1 Legal Issues Facing Healthcare Companies

The digitalisation of healthcare has met extreme growth, due not only to the technological development but also to health requirements (eg, the

COVID-19 pandemic significantly accelerated the use of digital healthcare due to the emergency of the situation).

Healthcare companies that develop and sell new digital healthcare technologies face numerous legal risks, one of which is associated with privacy and security/cybersecurity (eg, data breaches, account hijacking, DoS attacks). To mitigate such risks and liabilities, healthcare organisations must establish policies and/or service agreements with third parties with detailed provisions relating to security and privacy. Specific provisions regarding physical or technical controls (eg, employee background screenings, authentication/authorisation methods) should be implemented or agreed between the parties. Technical standards should follow relevant regulation and compliance requirements, industry standards and best practice.

Since healthcare providers tend to outsource a range of services, they need to have full visibility on the vendor's security risks and management. Next to third-party risk, fourth-party risk management arises due to vendors further outsourcing their services, in which case the supply chain risk rises exponentially. A third-party risk management programme and relevant policies should be in place addressing the full depth of risk. Another issue that healthcare providers may have to deal with includes intellectual property (IP). Device hardware and software may be covered by IP rights. Patents, designs and trademarks are registered rights that may be used to protect digital health technology.

Digital healthcare providers may also find themselves dealing with antitrust matters, especially in attention-drawing transactions such as M&As and joint-ventures.

13. UPGRADING IT INFRASTRUCTURE

13.1 IT Upgrades for Digital Healthcare

Cloud Management and Cybersecurity

Greek Law 4727/2020 introduced cloud management for the information systems of the public health sector. All electronic applications and central information systems of the Ministry of Health, hospitals and health centres, concerning the processing of medical data as well as medical transactions of citizens, must be installed in the Government Cloud Health Sector (H-Cloud) by 1 January 2023.

The Greek National Cybersecurity Strategy does not explicitly address the medical device and healthcare issue as a separate element, but it is affecting key actions of the Digital Transformation Bible.

The activities with direct impact are:

- the cybersecurity of 5G networks;
- the need for specialised security measures for Industrial IoT;
- the requirement of special measures in order to protect AI systems from attacks; and
- the development of a monitoring platform of cyber-attacks.

13.2 Data Management and Regulatory Impact

Privacy and security risks may be mitigated by upgrading IT infrastructure and data management practices and technologies.

A prime example is the GDPR requirement for data controllers and data processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account state-of-the-art technology.

The Digital Services Act (DSA) and the Digital Markets Act (DMA) frameworks establish rules that ensure fair and open digital markets and aim to establish a level playing field for businesses and to foster innovation, growth and competitiveness.

Other EU legislation that may impact the data management practices and technologies are the e-privacy directive (currently under discussion to be renewed by an e-privacy regulation), the Artificial Intelligence Act (currently under discussion) and the NIS directive (currently under discussion to be renewed by the NIS 2 directive).

In Greece, Greek Law 4727/2020 introduced cloud management for the information systems of the public health sector which is an important IT upgrade (for more information see **13.1 IT Upgrades for Digital Healthcare**).

14. INTELLECTUAL PROPERTY

14.1 Scope of Protection

Applicable Legal Framework

In the absence of a special national or European legal regime regarding IP protection in digital health, the existing general national and European legal regime on patent, copyright and trade secret protection is applicable. However, given the continuous growth of the application of AI in digital healthcare, new challenges that need to be regulated arise from the day-to-day practice.

In particular, the following legal frameworks are applicable:

- Greek Law 1733/1987 on the Grant and Protection of Patents as well as Greek Law 1607/1986 on the Grant of European Patents, according to which the inventor of a machine which incorporates AI software and databases is protected through the establishment of a special intellectual property right (patent);
- Greek Law 2121/1993 on Copyright (especially Articles 2α and 45α), according to which the creator of a database ("work" under Greek Law 2121/1993) automatically has the right of copyright – it is noted that the data itself is not protected; and
- Greek Law 4605/2019 on the harmonisation of Greek legislation to Directive (EU) 2016/943 on the protection of undisclosed know-how and trade secrets, according to which know-how and trade secrets related to AI systems (eg, robots or machines with incorporated AI software) are protected in case of illegal possession or usage from third parties.

Output Results of Intelligent Machines as IP Rights

Apart from the above, the national and European legal system is faced with the following fundamental issue: what might be the legal treatment of the output results of intelligent machines? Could they be recognised as subjects of intellectual property rights?

The human authorship principle in the Greek legislation dictates the anthropocentric character of the subject of protection. In the context of Greek Law 2121/1993 – and according to its travaux – the creator always corresponds to a human being, ie, a natural person.

In view of the above, the creator of the output results of intelligent machines recognised as "works" under Greek Law 2121/1993 may be:

- natural person who got involved in the development and learning of the machine; or
- the users of the machine, including every natural person executing, using and giving instructions to the intelligent machine to produce a creative result.

Given that there is no relevant provision in the legislation, the identification of creative causality between machine creation and human factor shall take the form of an ex-post evaluation. Then, if the output can be described as intellectual property due to creative causality with a human factor, the award of protection will be judged on the basis of the assessment of the originality of that creation, which (assessment) will concern the above crucial contributions establishing creative causality.

14.2 Advantages and Disadvantages of Protections

There are generally four types of IP:

- patents;
- copyright;
- trade marks; and
- trade secrets.

Patents are a set of exclusive rights granted to an inventor for a fixed period in exchange for the disclosure of an invention. Patents represent the legal right to exclude others from the market and generally cover the discovery of a new and useful process. Patents protect a design of something functional and the patent owner is provided with monopoly protection for up to the statutory life of the patent (in Greece it may be renewed up to 20 years and for medicines up to 25 years). Patents, however, are expensive to acquire and provide protection for only a relatively short period compared to other IP types. Additionally, in order to gain patent protection, it is required to fully disclose the nature of the invention and fully describe how the invention works.

Copyright describes the exclusive rights granted for a work of authorship for a fixed period. The statutory life of copyright is the author's lifetime plus 70 years after the author's death. In case of infringement, the author is entitled to actual damages and any additional profits enjoyed by the infringer, or statutory damages. The registering process of copyrights is relatively inexpensive and simple since the author gains protection and ownership when the work is in a tangible medium. As a general note, ideas are not protected, unless they are put in a tangible form.

Trade marks reflect the protections provided to brands, slogans, logos, etc. The registration of a national trade mark lasts for ten years and may be renewed for another ten years. Such renewal may take place for an unlimited number of decades. A trade mark's statutory life is as long as the trade mark owner maintains registration of the trade mark, maintains continuous use of the trade mark and enforces owner's rights. The registration of a trade mark is a relatively inexpensive and easy procedure (filing a form and paying a registration fee).

Trade secrets are protections to inventors or creators, such as customer lists, chemical or other formulas, manufacturing processes, etc. Trade secrets can cover any type of information or design as well as any type of item. Furthermore, trade secrets remain outside of any public disclosure and, unlike patents, which require (as mentioned above) full disclosure, they present a competitive advantage against reproduction or reverse engineering. However, nothing can (or will) protect the original creator against the risk of someone arriving at the same or similar result unwillingly or unknowingly.

14.3 Licensing Structures

Patents can be licensed in whole or in part, exclusively or non-exclusively. Licensing of a patent may include restrictions and may be provided contractually or judicially (under certain conditions).

Trademarks can be licensed in whole or in part, exclusively or non-exclusively, for a whole region (eg, country) or just for specific regions.

Copyright can be licensed freely, either in whole or in part and can be exclusive or non-exclusive. Limitations in respect of content, purpose, duration, territorial scope and means of exploitation may be included within the licensing agreement.

No specific requirements exist for the licensing of trade secrets. However, due to the nature of this right, special care should be taken to maintain the secret and confidential nature of the information. This may be achieved, for example, by entering into a confidentiality agreement.

14.4 Research in Academic Institutions

According to Article 8 of Greek Law 2121/1993, private legal entities acquire copyright in a "work" created by an employee only on a contractual basis, except for software development (Article 40), where a copyright is, under circumstances, automatically acquired by law. Public legal entities automatically acquire a copyright by law.

According to Article 6 of Greek Law 1733/1987, legal entities acquire patent rights either:

- ex post on a contractual basis;
- automatically by law in case the employee had the contractual duty to make an invention; or
- in a 40% application where the invention was created with means/material/information provided by the legal entity.

14.5 Contracts and Collaborative Developments

Greek law allows the parties to deviate from the default statutory rules and to contractually determine the IP rights allocation as they wish. Legal rules in regard to IP protection are not mandatory and, therefore, standard contractual freedom applies in this regard.

15. LIABILITY

15.1 Patient Care

Theories of Liability

The theories of liability arising from decisions based on digital health technologies are mainly as follows.

Civil liability

Healthcare service providers bear, under certain circumstances, contractual and non-contractual (especially tortious) liability towards the patient for any adverse outcome arising from decisions based on digital health technologies. In the absence of a specific European and National legal framework on AI, according to the general provisions of the Greek Civil Code (especially Articles 914 and 330) and Article 8 of the Consumer Protection Act (Greek Law 2251/1994), HCPs are obliged to compensate the patient if, during a medical act, they fail to comply with statutory rules and principles of healthcare ethics that govern medical practice (illegality).

The liability of HCPs (both contractual and non-contractual) is also formed as fault-based, which means that compensation for losses is due to the patient only if the damage is caused by fault or negligence. In addition, according to Article 922 of the Greek Civil Code, private healthcare institutions are also objectively liable for the damage caused by their employees/HCPs.

Decisions based on digital health technologies

While making a decision based on digital health technologies (especially a disease diagnosis), HCPs must comply, inter alia, with specific statutory rules: Greek Law 3418/2005 (Code of Medical Ethics) and Article 66 paragraph 16 of

Greek Law 3984/2011 on Telemedicine. In case they fail to correctly operate the digital healthcare equipment during decision-making, they bear contractual and non-contractual (especially tortious) liability towards the patient as stated above.

However, it must be noted that they bear no objective liability for the damages caused by an undetectable defect of the equipment used. Only the manufacturer (and in some cases the supplier) is liable towards the patient for defects that could not be easily detected by the healthcare services providers.

Ex ante (before the injury) limitation of liability is not allowed according to Article 332 paragraph 2 of the Greek Civil Code and Article 8, paragraph 6 of Greek Law 2251/1994. Ex post (after the injury) limitation of liability is allowed if the patient agrees.

Criminal liability

HCPs bear, under circumstances, criminal liability according to Articles 302 and 314 of the Greek Criminal Code for unintentional injury or death attributed to negligence.

15.2 Commercial

Without prejudice to the provisions of Presidential Decree 131/2003, third-party vendors bear tortious liability towards the healthcare institutions in accordance with Article 914 of the Greek Civil Code. They also bear contractual liability on the basis of an existing contractual relationship with the healthcare institutions.

Third-party vendors bear no liability according to Articles 6 (Manufacturer's Liability for Defective Products) and 8 (Service Provider's Liability) of the Consumer Protection Act and Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services, as long as healthcare institutions are not considered "a consumer".

16. HOT TOPICS AND TRENDS ON THE HORIZON

16.1 Hot Topics That May Impact Digital Healthcare in the Future

Managing Stress-Inducing Situations

Digital health and digital medicine are expected to open new frontiers in the management of various excessively stress-inducing situations affecting mental processes – ironically themselves the result of technological advances (most notably, social media). For example, VR and AR have been tested and could be useful in treating anxiety, depression or certain phobias, without – in most cases – even requiring the presence of a therapist.

These novel instruments are a research priority for many institutions around the world and, if these results continue to be successful, they will likely prove to be a powerful weapon for protecting public mental health.

Physical Pain

Physical pain is another domain where pharmaceutical companies have invested a lot in producing plain painkillers, narcotics or other more sophisticated antidepressants, often with serious side effects.

Experimental studies with participants immersed in VR and AR experiences have showed reductions in levels of pain and general distress. In fact, the patients participating in these studies expressed the desire to use VR and AR again during painful medical procedures. Researchers hypothesise that VR and AR act as a non-pharmacological form of analgesia by a mechanism of emotion-affecting and emotion-based cognitive and attentional process of the body's

complicated pain modulation system. Put simply, it could be described as a distraction from the painful stimulus.

Mental Health

Digital health applications are expected to greatly affect the ways in which HCPs, pharmaceutical companies and all other major stakeholders operate in preventing, monitoring and managing/treating mental health disorders, physical pain and pain-inducing medical procedures.

In Greece, these novel therapies have not yet been officially approved, but the prediction is that in the not-too-distant future, these practices could become mainstream modalities.

Contributed by: *Nikitas P. Fortsakis, Evangelos N. Courakis, Konstantinos Kritsotakis and Dimitrios Andriopoulos,* ***Koutalidis Law Firm***

Koutalidis Law Firm was founded in 1930 and is regarded as one of the most prestigious top-tier law firms in Greece. The firm has advised on some of the most high-profile and groundbreaking transactions in Greece and has a varied client list that includes leading Greek and foreign corporations, major investment and commercial banks and financial institutions. The firm's work and commitment to providing excellent service and finding innovative solutions covering a variety of law and business sectors has been recognised by clients and independent commentators. With an Athens-based team of 12 lawyers dedicated to the healthcare and pharmaceutical industry, the firm provides all-inclusive legal services to its demanding clients on both contentious and non-contentious matters. In order to address the novel challenges brought by digital healthcare and provide stellar service, the team often works closely with the firm's TMT and data protection practices.

AUTHORS

Nikitas P. Fortsakis is a partner at Koutalidis Law Firm and head of the TMT practice and co-head of the healthcare and pharmaceutical practices. Nikitas regularly advises clients on EU and Greek healthcare regulatory and compliance matters, negotiates a wide range of commercial agreements, including distribution and collaborations agreements, on their behalf and represents them before administrative courts. He also represents them in cross-border anti-corruption investigations. In his dual capacity as a healthcare and TMT lawyer, Nikitas brings a unique mix of technical and legal knowledge that can help his clients navigate the new landscape of digital healthcare.

Evangelos N. Courakis is a partner at Koutalidis Law Firm, head of the energy and data protection practices and co-head of the healthcare and pharmaceutical practices. Evans frequently advises healthcare and pharmaceutical clients on regulatory compliance and transactional matters and also represents them in cross-border anti-corruption investigations. Capitalising on his solid experience with complex data protection matters, Evans can assist clients in identifying and mitigating relevant risks that are inherent in the ever-growing field of digital health. Moreover, his experience with working in the energy sector allows Evans to advise his clients on how to address the energy-associated needs of digital healthcare products.

Contributed by: *Nikitas P. Fortsakis, Evangelos N. Courakis, Konstantinos Kritsotakis and Dimitrios Andriopoulos,* ***Koutalidis Law Firm***

Konstantinos Kritsotakis is an associate at Koutalidis Law Firm. Konstantinos focuses on personal data protection and security and privacy matters and has significant experience working with healthcare and pharmaceutical clients. Konstantinos is also an accredited mediator, a certified GDPR expert and a member of the Athens Bar. He recently co-authored a publication on Greece's TMT sector, where he also touched on digital health aspects.

Dimitrios Andriopoulos is an associate at Koutalidis Law Firm. Dimitrios focuses on international arbitration in the energy sector and also has significant experience working with healthcare and pharmaceutical clients on contentious and non-contentious matters. Dimitrios is a member of the Athens Bar and recently co-authored a publication on Greece's TMT sector, where he also touched on aspects of digital health. He has also co-authored a piece on Greece's cross-border capabilities, which contains useful insights on the broader digitalisation of the Greek economy.

Koutalidis Law Firm

The Orbit
115 Kifissias Ave.
11524 Athens
Greece

Tel: +30 210 3607 811
Fax: +30 210 3600 069
Email: info@koutalidis.gr
Web: www.koutalidis.gr