International
Comparative
Legal Guides

Practical cross-border insights into digital health law

# Digital Health

# 2023

## Fourth Edition

Contributing Editor:
**Roger Kuan**
**Norton Rose Fulbright**

ICLG.com

# Introductory Chapter



# Expert Analysis Chapters



# Q&A Chapters

# Portugal



Eduardo Nogueira Pinto


Ricardo Rocha

PLMJ


## 1 Digital Health

### 1.1 What is the general definition of "digital health" in your jurisdiction?

There is no specific definition of "digital health" under Portuguese law. However, the regulations for digital health matters – understood as the provision of healthcare using digital resources – are usually associated with the laws and regulations on medical devices and with the statutes and/or professional ethics codes of the associated professional associations.

### 1.2 What are the key emerging digital health technologies in your jurisdiction?

**1. Telemedicine**

Telemedicine is not a recent phenomenon in Portugal. In 2006, an attempt was made to regulate teleconsultations by defining their concept and establishing price lists for telemedicine services in the *Serviço Nacional de Saúde* ("**SNS**") – the Portuguese national health service.

The COVID-19 pandemic increased the use of teleconsultations, with several advantages: greater efficiency; reduction of financial costs; and better accessibility to health services.

**2. Medical Software**

Medical software is progressively being used in healthcare to help doctors make clinical decisions and establish therapeutic programs. This software is under permanent development and its use is expected to increase exponentially in the future.

**3. Health Apps**

The SNS already offers some apps and this demonstrates the development of these technologies in the digital health sector in Portugal. One example of these applications is "SNS24", allowing access to digital health services on mobile devices, including teleconsultation, medicines history, prescriptions and therapeutical programs.

Private health companies also offer apps supporting their services allowing teleconsultations, test results, drug prescriptions and monitoring of health parameters.

**4. Wearables**

Wearable devices, which are products controlled by electronic components and software that can be incorporated into clothing or accessories, are also significant in terms of digital health.

These devices often include heart rate sensors, fitness trackers, sweat meters and oximeters. Technological advances have facilitated an explosion in the range of new devices that can gather data linked to the health of the wearer. Based on rapid consumer uptake so far, it is certain they will become a more integral part of human life in years to come.

### 1.3 What are the core legal issues in digital health for your jurisdiction?

The main legal issues arise in relation to safety, health literacy, privacy, information security and personal data protection.

The use of digital health resources can lead to self-diagnosis and self-medication by patients using the technology who do not have the knowledge necessary to decide the best treatment for their – alleged – disease. There are also risks associated with this kind of practice. The misinterpretation of the results provided by those devices can lead to unease and anxiety, and to the overburdening of health services due to false emergency episodes.

For matters relating to privacy, information security and data protection, see section 4 below.

### 1.4 What is the digital health market size for your jurisdiction?

Some forecasts project the revenue in the Portuguese digital health market will reach around €307 million in the current year. The market's largest sector is the digital fitness and wellbeing sector with a total revenue value of around €173 million in 2022.

The future of digital health in Portugal seems even more promising, as the projected market volume by 2027 is around €470 million.

### 1.5 What are the five largest (by revenue) digital health companies in your jurisdiction?

This information is not publicly available even though some important companies are operating in Portugal in the digital health market.

## 2 Regulatory

### 2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

There are no specific regulations applicable to digital health. The legal framework arises from Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices ("**MDR**") and Regulation (EU) 2017/746 of

the European Parliament and of the Council of 5 April 2017 on *in-vitro* diagnostic medical devices ("**MDIVR**"). There are also the regulations of professional associations addressing professional ethics issues.

### 2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the General Data Protection Regulation ("**GDPR**").
- Decree-Law 7/2004 of 7 January on the legal framework for electronic commerce.
- Decree-Law 383/89 of 6 November on liability for defective products.
- Decree-Law 145/2009 of 17 June on the national provisions applicable to the advertisement of medical devices and governing the relationship between healthcare providers and medical device manufacturers.

### 2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Apart from the Regulations on medical devices and *in-vitro* medical devices mentioned above, the following consumer protection legislation is applicable:

- Law 24/96 of 31 July, the Portuguese Consumer Protection Law ("**Law 24/96**").
- Decree-Law 57/2008 of 26 March on Unfair Commercial Practices.
- Decree-Law 330/90 of 23 October, the Portuguese Advertising Code.
- Decree-Law 69/2005 of 17 March on the General Product Safety Law, transposing Directive 2001/95/EC into Portuguese law.

### 2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

- The Ministry of Health, as responsible for the definition of the national health policy and for the SNS.
- *Entidade Reguladora da Saúde*, which supervises all entities providing healthcare services, except pharmacies ("**ERS**").
- *Infarmed - Autoridade Nacional do Medicamento e Produtos de Saúde I.P.*, the regulatory body supervising medicines and health products ("**Infarmed**"), including pharmacies.
- *Comissão Nacional de Proteção de Dados*, the Portuguese Data Protection Agency ("**CNPD**").

### 2.5 What are the key areas of enforcement when it comes to digital health?

- The ERS ensures that healthcare providers comply with the requirements for engaging in licensed activities.
- Infarmed supervises the placing of medicines and medical devices on the market, and it enforces conformity with the applicable laws and regulations.
- The CNPD, if processing of personal data is required.

### 2.6 What regulations apply to software as a medical device and its approval for clinical use?

Software classified as a medical device is subject to the MDR or MDIVR, as applicable.

From a domestic law point of view:

i) Decree-Law 145/2009 of 17 June, without prejudice to the MDR.

ii) Decree-Law 189/2000 of 12 August on *in-vitro* diagnostic medical devices, without prejudice to the MDIVR.

### 2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

There is currently no specific legislation regarding artificial intelligence in digital health devices.

There is a proposal from the European Commission to harmonise the legislation on artificial intelligence in the Member States.

## 3 Digital Health Technologies

### 3.1 What are the core issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  The main challenges in telemedicine and virtual care are obtaining resources and infrastructure to use telemedicine in the public health services and training health professionals to implement telemedicine as an effective method of consultation.
  The inclusion of digital health implies the redesign of working processes, as well as the integration of new technological systems with existing ones.
  Doctor–patient relationships can also suffer with the use of digital health tools. It is essential to preserve the relationship and the quality of the healthcare services provided to the patients.
  The confidentiality and security of patients and health professionals must always be preserved. All technological devices used must guarantee these matters.
- **Robotics**
  The main concern about the use of robotics in healthcare is the safety of patients and the quality of the healthcare provided. Questions regarding liability for accidents and/or medical negligence can also arise.
  Patient detachment due to the lack of health and digital literacy and the decrease in the improvision capacity of healthcare professionals are also relevant.
  The risk of technical errors and failures is also significant when it comes to the use of robotics in healthcare activities.
- **Wearables**
  Qualification and the requirements to put them on the market are probably the most important issues regarding wearables and mobile apps. Qualification as a medical device is highly important considering that the requirements for the placement on the market differ significantly. As the line between medical devices and non-medical or fitness apps is fine, it is important to ensure the safety of

the users without harming the innovation and development of new technological solutions.
These kinds of technologies can also induce misdiagnosis by users, with the associated danger to the health and safety of the patients.
There are also concerns about the security of patient data and privacy in this field.

- **Virtual Assistants (e.g. Alexa)**
  The safety and the possible illegal practice of health procedures by unqualified "entities" is a very significant risk when it comes to virtual assistants and healthcare.
- **Mobile Apps**
  Please see "Wearables" above.
- **Software as a Medical Device**
  Software can induce overconfidence in patients with the information provided, which may be subject to errors. As mentioned in "Wearables" above, the qualification of software as a medical device is complex, as it depends primarily on the purpose of the manufacturer. As such, it is essential to ensure that the use of software as a medical device is properly supervised by a healthcare professional to avoid risks and misinterpretation of results.
- **Clinical Decision Support Software**
  As support software, this kind of tool should be used to support decision-making by healthcare professionals and not as the final decision-maker. Healthcare professionals should critically analyse the results of software and evaluate whether the suggested decision is correct and suitable for the specific pathology.
  If not, technical errors can compromise the result and the health and safety of the patient. This could then lead to an error in the final diagnosis or in the choice of the most suitable treatment.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  As a technology based on algorithms, it is essential that the algorithm is tested to be fully reliable and safe. A validation system would be essential to ensure the safety and the suitability of those systems. Healthcare professionals need to be specifically trained and educated to apply those technologies to their healthcare activities.
  Another significant issue is the trust of the patients in those tools. It is necessary to provide accurate information on the benefits of AI in healthcare, and to adopt a fully transparent policy and communicate all the risks involved. The increase in use of AI can create a negative impact on the abilities and knowledge of healthcare professionals, which is why all digital tools used in healthcare should be decision-supporters for the professionals and not decision-makers.
- **IoT (Internet of Things) and Connected Devices**
  The privacy and safety of patients are the main issues in the IoT. There is a risk of cyber-attacks that compromise the privacy and safety of the patients and of a lack of trust in the results obtained by those tools.
- **3D Printing/Bioprinting**
  Quality, safety and suitability of these products are the main concerns regarding 3D printing and bioprinting when applied in the field of healthcare.
- **Digital Therapeutics**
  There is a high risk regarding patient data, especially because it may involve very sensitive data. It is also difficult to monitor quality and therapeutic compliance by the patient. The resistance of patients to those therapeutical methods is also an important factor.
- **Natural Language Processing**
  The main concerns are privacy and data protection and the capacity of the systems to correctly interpret messages which may lead to contradictory and meaningless communications. In turn, this could cause the unreliability of the system and risk the safety of patients.

### 3.2 What are the key issues for digital platform providers?

The key issues for digital platform providers are the need to (i) ensure that no illegal content is transferred to the digital platform, (ii) ensure the safety of the patients' data, (iii) ensure that the use of digital platforms is safe, efficient and improves the quality of the healthcare, (iv) design tools that enable a smooth transition to the use of digital platforms and, finally, (v) train and educate healthcare professionals to confidently use those digital tools in their practices.

## 4 Data Use

### 4.1 What are the key issues to consider for use of personal data?

The processing of personal data must consider the nature of the data, as information that relates to an identified or identifiable person, the process of anonymisation, in compliance with the principle of storage limitation, the process of pseudonymisation, to enhance data protection and authentication procedures. Article 9 of the GDPR prohibits the "processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" ("**Health Data**").

This prohibition may not apply under the exceptions in article 9(2), particularly when the data subject gives explicit consent, the processing relates to personal data which are manifestly made public by the data subject, or the processing is necessary for reasons of public interest in public health.

### 4.2 How do such considerations change depending on the nature of the entities involved?

Pursuant to article 7 of the GDPR, when processing is based on consent, the controller must be able to demonstrate that the data subject has consented to the processing of their personal data. The consent must be freely given, informed, specific and unambiguous, and the data subject must be able to withdraw it at any time.

Public authorities may process health data when this processing is necessary for reasons of public safety, regardless of consent. In these cases, the processing of health data must be properly justified to ensure the pursuit of a public interest that cannot otherwise be safeguarded. The processing of health data must be carried out by a person bound by duties of confidentiality, and appropriate security measures must be guaranteed to safeguard the security of the information, as defined in Law 58/2019 of 8 August.

### 4.3 Which key regulatory requirements apply?

Article 5 of the GDPR sets out the principles governing the processing of personal data: lawfulness; fairness and transparency; purpose limitation; data minimisation; data accuracy; storage limitation; integrity; and confidentiality. Exemptions or restrictions to these principles must be provided for by law, pursue a legitimate aim and be necessary and proportional.

Even in cases where the public interest allows for the processing of health data, confidentiality obligations, requirements of proportionality and appropriate security measures must be guaranteed.

### 4.4 Do the regulations define the scope of data use?

Law 12/2005 of 26 January ("**Law 12/2005**") defines health information as all types of information directly or indirectly linked to the present or future health of a person, whether living or deceased, as well as their medical and family history. Law 12/2005 stipulates that such information may only be used by the health system under the conditions expressed in the written authorisation of the data subject or their representative. Access to health information can be provided for research purposes on the condition that it is anonymised.

Article 6 of Decree-Law 131/2014 of 29 August provides that the processing of genetic information and the creation of genetic databases are allowed exclusively for the provision of healthcare or health research, including epidemiological and population studies.

### 4.5 What are the key contractual considerations?

Pursuant to article 24 of the GDPR, the controller must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. Article 32 of the GDPR provides that such measures include (i) the pseudonymisation and encryption of personal data, (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. The controller and the processor should also take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller.

### 4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

When using or collecting personal data, it is vital that the data subject has the rights to be informed, to access the data, to rectify inaccurate data, to erase data, to be forgotten, to restrict the use of the data, to enjoy data portability and to object to the processing. In particular, Law 12/2005 defines a genetic database as any record, whether computerised or not, which contains genetic information about a set of persons or families. Regarding such databases, the law establishes that any person may request and have access to information about themselves contained in files containing personal data.

### 4.7 How are issues with data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Under article 6(2) of Law 59/2019 of 8 August, profiling activities leading to discrimination of natural persons based on special categories of personal data, such as health data, should be prohibited.

Article 11 of Law 12/2005 establishes that (i) no one may be prejudiced in any way on the basis of a genetic disease or of their genetic heritage, (ii) no one may be discriminated against in any way on the basis of the results of a genetic test diagnostic, including for the purpose of obtaining or retaining employment, obtaining life and health insurance, access to education and for the purpose of adoption, (iii) no one may be discriminated against in any form, including in their right to medical and psychosocial follow-up and genetic counselling, for refusal to undergo a genetic test, and (iv) everyone is guaranteed equitable access to genetic counselling and genetic testing, with due safeguarding of the needs of the populations most severely affected by a given disease.

## 5 Data Sharing

### 5.1 What are the key issues to consider when sharing personal data?

The GDPR provides for the free flow of data within the EU. There are specific requirements regarding the transfer of personal data to third countries outside the EU and international organisations, such as adequacy decisions, standard contractual clauses, binding corporate rules, certification mechanisms and codes of conduct. The primary purpose of these requirements is to offer the same level of protection when the personal data of EU citizens is transferred abroad.

### 5.2 How do such considerations change depending on the nature of the entities involved?

Pursuant to Directive 2016/680, competent authorities may exchange personal data within the EU. The exchange of personal data in these cases is neither restricted nor prohibited for data protection reasons.

### 5.3 Which key regulatory requirements apply when it comes to sharing data?

Articles 45 and 46 of the GDPR provide for two ways of allowing the transfer of personal data to third countries and international organisations: an adequacy decision; or, in the absence of an adequacy decision, a controller or processor may transfer personal data by providing appropriate safeguards, including enforceable rights and legal remedies for the data subject.

## 6 Intellectual Property

### 6.1 What is the scope of patent protection?

Patent protection confers an exclusive right on the holder to exploit an invention. An invention may be defined, broadly, as a new way of doing something, or a technical solution to a problem in the field of technology. Patent types may amount to a new product, may consist of a new process to obtain a new or an already known product, or to a new use/application of such product.

To be subject to patent protection, the invention must have a technical nature, and meet the standard requirements of novelty, inventive step and industrial application.

### 6.2 What is the scope of copyright protection?

In broad terms, copyright, referred to in Portugal as authors'

rights, grants protection over externalised expressive intellectual creations, designated as "works" or "artistic, scientific or literary works".

Originality and creativity are the general requirements for a work to be protected by copyright. This means that the work must be the author's own intellectual creation, and that at least some creative aspect is required.

Copyright protection is independent of the disclosure, publication, use or exploitation of the protected work.

### 6.3 What is the scope of trade secret protection?

The Portuguese Industrial Property Code ("**CPI**") provides that trade secrets are protected and that information will be considered as a trade secret if it meets the following requirements: (i) it is secret, in that it is not generally known or easily accessible to persons in the circles that normally deal with this type of information; (ii) it has commercial value by virtue of being secret; and (iii) it is subject to reasonable diligence in order to keep it secret. Articles 314 and 315 of the CPI identify the acts that constitute a legal or illegal use, acquisition or disclosure of the trade secret.

### 6.4 What are the rules or laws that apply to academic technology transfers in your jurisdiction?

Pursuant to article 59 of the CPI, inventions made by employees or collaborators as a result of their research activities belong to the legal entity under whose statutory scope the research and development activities are carried out.

The inventor will, in any case, reserve the right to participate in the economic benefits arising from the exploitation or transfer of the patent rights.

The terms of this participation and further issues regarding academic technology transfers are defined in the articles of association and the intellectual property regulations of the legal entity in question.

### 6.5 What is the scope of intellectual property protection for software as a medical device?

Under the CPI, software *per se* cannot be subject to patent protection. However, patent protection may be granted to software which exhibits a technical effect. The EPO has held that computer software can be patented in certain circumstances: (i) when the software affects the execution of processes which take place outside the software or the computerised system; or (ii) when the software leads the computer/hardware to operate in a new manner. Furthermore, software can be protected by copyright under Decree-Law 252/94 of 20 October, which grants software protection analogous to that conferred on literary works.

The source code of a piece of software may also be protected under the trade secrets rules provided that the necessary requirements are met.

### 6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction?

There are no specific rules on AI devices being named as inventors in Portugal. When referencing the inventor and "*his/her successors in title*", article 57 of the CPI appears to be construed around the concept of the inventor being a natural person. Therefore, it seems to exclude legal persons and AI devices from being named as the inventor.

### 6.7 What are the core rules or laws related to government funded inventions in your jurisdiction?

There are no specific rules on Government-funded inventions. These are subject to the general principles of contractual freedom. The parties can draft the terms of ownership of any IP right and, in the absence of such terms, any supplementary rules will apply.

## 7 Commercial Agreements

### 7.1 What considerations apply to collaborative improvements?

There is no specific regulation on collaborative improvements in Portugal. However, these collaborations are accepted depending on the organisations and professionals involved. The regulatory and legal framework must be observed, particularly with regard to interactions between healthcare companies or pharmaceutical industry companies and healthcare professionals, healthcare organisations or patient associations. Under Portuguese law, an "interaction" includes granting benefits to any of the above professionals and organisations, supporting events, granting scholarships and any other interaction that results in the concession of a benefit.

### 7.2 What considerations apply in agreements between healthcare and non-healthcare companies?

It is advisable for these agreements to be concluded in a written instrument where key issues are addressed. IP rights, data protection and confidentiality are the main issues to be considered. When concluding agreements with public healthcare entities, legal regulations should be considered to prevent distortions to competition and undue influence of healthcare professionals and organisations.

## 8 Artificial Intelligence and Machine Learning

### 8.1 What is the role of machine learning in digital health?

As part of AI, machine learning can have a very important role in healthcare. However, this role must respect the patient, his/her safety and privacy.

### 8.2 How is training data licensed?

Training data may fall under the scope of Decree-Law 122/2000 of 4 July which incorporated into Portuguese law Directive 96/9/EC regarding the protection of database rights. In such cases, the licensing of training data is subject to the general provisions regarding the licensing of intellectual property rights. If it includes personal health data, the limitations imposed by the GDPR should also be considered in the context of licensing.

### 8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

Pursuant to article 11 of the Portuguese Copyright and Related

Rights Code, copyright belongs to the intellectual creator of the work, unless expressly provided otherwise. To date, there are no specific rules for the IP rights resulting from machine learning improvements. Portuguese law does not recognise machine learning or AI as "authors" for copyright purposes. In Portugal, the creation of intellectual works is strictly associated with human beings.

### 8.4 What commercial considerations apply to licensing data for use in machine learning?

If the licensed data consists of health data, the commercialisation of sensitive information must always comply with the GDPR rules, in particular, the ones in articles 7, 9 and 32. Contractual provisions regarding indemnifications and liability for the use of data in violation of the GDPR should also be implemented by the parties, as should the customary representations and warranties regarding the ownership of the rights over the licensed data. Further issues regarding the definition of ownership of rights relating to that data should also be considered, including the ownership of any future works based on the licensed data, and the conditions and scope of use of that derivative data.

## 9 Liability

### 9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Depending on the specific service provided, contractual liability may be applicable. This liability is governed by the law chosen by the parties in the contract or the law where the service is provided. Moreover, non-contractual civil liability may be applicable if the legal criteria are met. Law 24/96 establishes an objective liability of the manufacturer for any damage caused by defects in the product or service placed on the market. Other bases of liability may be applicable depending on the nature of the event that led to the adverse outcome.

### 9.2 What cross-border considerations are there?

When it comes to liability in cross-border interactions, B2B relations must be distinguished from B2C relations. Concerning B2C relations, the parties' choice of the applicable law may not always be the prevalent criteria. Under the Rome Convention on the Law applicable to Contractual Obligations ("**Rome Convention**"), other criteria may be adopted to determine the applicable law depending on the specific circumstances of the case. In these cases, the parties may be able to choose the applicable law. However, if mandatory provisions exist in the country where the consumer has their habitual residency, these provisions will prevail. Under the Rome Convention, the applicable law is the law of the habitual residence of the consumer. As regards non-contractual liability, the Rome Convention determines, as a rule, that the applicable law is the one of the countries where the damage occurs, regardless of where the event giving rise to the damage occurred and the country where the indirect consequences of that event occur. However, there are other criteria depending on the specific circumstances of each case.

With special relevance to B2B relationships, under the Rome Convention, the law applicable to a non-contractual obligation arising from an infringement of an intellectual property right will be the law of the country where protection is claimed. In the case of a non-contractual obligation arising from an infringement of a unitary EU intellectual property right, the applicable law will be the law of the country where the infringement was committed, except for questions that are not governed by any relevant EU instrument.

## 10 General

### 10.1 What are the key issues in Cloud-based services for digital health?

Issues raised by Cloud-based services relate mainly to data protection, data transmission and privacy. It is essential to be aware that data treatment and data transfer by Cloud service providers raise additional legal issues.

### 10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

The healthcare sector is a heavily regulated sector. EU instruments and national laws establish a framework that must be properly acknowledged by any company before entering the market. Other issues may be raised, particularly regarding intellectual property and data protection.

### 10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Considering the level of regulation of the health sector in Portugal, a compliance check is one of the most important requirements any firm should consider when approaching a target firm. The position of the target company in the relevant market, manufacturing costs and distribution channels, IP rights and commercial agreements are key issues to check when entering the market. Possible partnerships with governments in countries with public health systems as well as reimbursement agreements are also important issues that must be addressed before investing in a digital healthcare venture.

### 10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key barriers are the legal frameworks, the lack of investment from governments in digital health technologies and the lack of adequate regulation regarding some specific technologies.

### 10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Public entities such as the Central Administration of the Health Services, Health Authorities or the Shared Services of the Health Ministry perform an important role in this field. Depending on the type of technology, associations representing manufacturers and other stakeholders can influence clinical adoption of digital health solutions. Associations such as the Portuguese Association of Medical Devices, Portuguese Association of Health Engineering and Management and the Portuguese Telemedicine Association may be able to influence such decisions. Professional associations that regulate healthcare professions are also able to influence the clinical adoption of health solution from the perspective of the healthcare professionals.

**10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?**

Reimbursements by the Government depend on the product itself and are subject to specific regulation. Requirements for reimbursement are settled by law or administrative order. Solutions focused on efficiency are more likely to be subject to reimbursement rather than solutions focused on preventive health. Reimbursements by private insurers depend on the type of technology and the insurance policy.

**10.7 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.**

According to the Deloitte study "Shaping the future of European Healthcare" (2020), the current main challenges identified in the health digitalisation process in Portugal are bureaucracy, the choice of the most appropriate digital solution and training of healthcare workers. Moreover, adjustments in the regulatory framework are said to be needed to increase patient confidence in the use of digital solutions in healthcare. Inclusion of digital health in the education of healthcare professionals and patient literacy in digital health are also identified as key issues to be developed to allow the advancement of the digital transformation.

The Portuguese Government is engaged in the digital transformation of the healthcare sector and the Portuguese eHealth strategy has been referred to as exemplary by the WHO since 2015.

The Portuguese National Centre for Telehealth was launched in 2016 and was the first centre of this kind in the world. Its mission is to facilitate citizens' access to healthcare, ensure its fairness and increase the efficiency of national resources by taking advantage of information and communication technology. Furthermore, the National Strategic Telehealth Plan of 2019 demonstrates the engagement of the Portuguese Government in the digital transformation of the healthcare sector.

The National Strategy for the Health Information Ecosystem also performs an important role in fostering the digital transformation of the health sector in Portugal. The COVID-19 pandemic allowed some barriers to be broken down as it created an environment that was even more receptive to the implementation of digital solutions in the health sector in Portugal.

**Eduardo Nogueira Pinto** heads PLMJ's healthcare, life sciences and pharmaceutical practice. He has more than 20 years' experience in advising Portuguese and foreign companies, and he has worked on many projects in the areas of healthcare and pharmaceuticals.
He focuses on regulatory matters, licensing, compliance, advertising, prices and reimbursements, contracts and market access.
Eduardo has handled numerous licensing, public procurement and administrative offence proceedings, and he has also advised clients on M&A operations. Furthermore, Eduardo provides regular legal support and advice to the National Association of Pharmacies and to dozens of Portuguese and foreign companies from the pharmaceutical sector.
Eduardo won the M&A Lawyer of the Year in the *LMG Life Sciences Awards 2022 EMEA*.

**PLMJ**
Avenida Fontes Pereira de Melo, 43
1050-119 Lisbon
Portugal

Tel: +351 213 197 300
Email: eduardo.nogueirapinto@plmj.pt
URL: www.plmj.com/en

**Ricardo Rocha** is a senior associate with 10 years' experience who focuses on providing regulatory advice to Portuguese and international companies in the pharmaceutical industry. He assists his clients with all matters relating to the development and marketing of medicines, medical devices, food supplements and cosmetics.
Ricardo is building a strong track record and is advising various clients operating in the medical cannabis sector. He is also very active in writing opinion articles and giving conferences on this topic.
Ricardo has a Master's in legal-business sciences from the Faculty of Law of the University of Lisbon and completed a postgraduate course in healthcare law at the Faculty of Law of the *Universidade Católica Portuguesa* and attended the European Pharma Law Academy in Cambridge.
Before joining PLMJ, he was a lawyer at Glintt - Global Intelligent Technologies.

**PLMJ**
Avenida Fontes Pereira de Melo, 43
1050-119 Lisbon
Portugal

Tel: +351 213 197 300
Email: ricardo.rocha@plmj.pt
URL: www.plmj.com/en

PLMJ is a law firm based in Portugal that combines a full service with bespoke legal craftsmanship. For more than 50 years, the firm has taken an innovative and creative approach to produce tailor-made solutions to effectively defend the interests of its clients. The firm supports its clients in all areas of the law, often with multidisciplinary teams, and always acts as a business partner in the most strategic decision-making processes.
With the aim of being close to its clients, the firm created PLMJ Colab, its collaborative network of law firms spread across Portugal and other countries with which it has cultural and strategic ties. PLMJ Colab makes the best use of resources and provides a concerted response to the international challenges of its clients, wherever they are. International collaboration is ensured through firms specialising in the legal systems and local cultures of Angola, China/Macao, Guinea-Bissau, Mozambique, São Tome and Príncipe and Timor-Leste.

**www.plmj.com/en**

PLMJ Transformative Legal Experts

# ICLG.com

## Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group