International
Comparative
Legal Guides

Digital Health 2021

A practical cross-border insight into digital health law

Second Edition

Featuring contributions from:

Advokatfirma DLA Piper KB
Arthur Cox LLP
Astolfi e Associati, Studio Legale
Baker McKenzie
Bird & Bird LLP
Cliffe Dekker Hofmeyr
Consumer Technology Association (CTA)
D'LIGHT Law Group
Deloitte
Gilat, Bareket & Co., Reinhold Cohn Group
GVA LPC
Hammad and Al-Mehdar Law Firm
Haynes and Boone, LLP
Herbst Kinsky Rechtsanwälte GmbH
Johnson & Johnson
KYRIAKIDES GEORGOPOULOS LAW FIRM
Lee and Li, Attorneys-at-Law
LexOrbis
Llinks Law Offices
Machado Meyer Sendacz e Opice Advogados
McDermott Will & Emery AARPI
McDermott Will & Emery LLP
NeuroPace, Inc.
OLIVARES
Quinz
VISCHER

ICLG.com

ISBN 978-1-83918-097-2
ISSN 2633-7533

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Digital Health 2021

Second Edition

Contributing Editor:
Roger Kuan
Haynes and Boone, LLP

Introductory Chapters

Expert Chapters

Q&A Chapters

Mexico


Abraham Díaz


Ingrid Ortíz

OLIVARES

1 Digital Health and Health Care IT

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

Mexican legislation has not specifically defined "digital health". However, the Federal Commission for the Protection against Sanitary Risks (COFEPRIS) and other private and public entities are already addressing the matter in various aspects (i.e. regulation, guidelines, analysis, forums, etc.).

Nevertheless, a definition generally accepted in Mexico – although in constant evolution – is that digital health is a concept that incorporates Information and Communication Technologies, into sanitary assistance products, services and processes, as well as into organisations and institutions that may improve the health of individuals.

1.2 What are the key emerging technologies in this area?

Many areas of health technology are rapidly developing in Mexico, such as: portable and ingestible devices; mobile health apps; artificial intelligence (AI); robot health carers; medicine applied robots; 3D organ printing; blockchain; telemedicine; machine learning; genome research; drones; augmented and virtual reality; electronic records and big data, among others. As stated above, these technologies are in constant evolution.

In relation to the above, the most recent advances in digital health in Mexico have been mainly applied to three diseases: ischaemic heart disease; breast cancer; and diabetes. For example, with advances in the genetic analysis of diabetes, Mexican doctors and scientists may be able to predict which students within a student population are likely to develop diabetes, and therefore intercept with preventative measures that will save many costs in the future.

1.3 What are the core legal issues in health care IT?

As a type of medical device aimed to be used by healthcare practitioners and patients, healthcare IT has safety, quality and effectiveness implications. This is currently regulated by COFEPRIS, which grants marketing authorisations to products that are safe and effective.

Data protection is another important issue in the field of healthcare IT. IT often involves the collection and/or transfer of data, and healthcare IT could involve the collection and transfer of sensitive data. As a matter of fact, digital health is becoming more and more intrusive as it evolves, in itself a reason why the proper handling of personal information, especially the sensitive information, must be a core concern when dealing with new devices for digital health, thus having to bear in mind the concept of privacy by design. The mechanisms of data protection in Mexico are discussed further below.

It is advisable that entities offering healthcare IT are aware of professional liability issues, and that they check whether their professional liability insurance covers things that go wrong when providing healthcare IT services, including providing services that require a medical licence or administering medical care.

2 Regulatory

2.1 What are the core health care regulatory schemes?

Although developing, the field of digital health is still relatively new in Mexico and its application in real life settings is still limited. There are no specific healthcare regulatory schemes for digital health; the field is instead being covered by schemes which regulate medicinal products and medical devices, namely:

- the General Health Law (in Spanish, "*Ley General de Salud*");
- the Health Law Regulations over Healthcare Products (in Spanish, "*Reglamento de Insumos para la Salud*");
- Official Mexican Standards (NOMs), particularly the NOM-241-SSA1-2012 setting good manufacturing practices for medical devices and NOM-137-SSA1-2008 for the Labelling of Medical Devices;
- the Mexican Pharmacopoeia; and
- COFEPRIS' Rules listing healthcare products that do not require a marketing authorisation due to low risks on human health (published in December 2014).

COFEPRIS may already be addressing the need for regulations for mobile medical applications, especially for those that present health risks.

2.2 What other regulatory schemes apply to digital health and health care IT?

Since digital health and healthcare IT implies health information management across computerised systems and the secure exchange of information between consumers, providers, payers and others, it is necessary to keep in mind the compliance with data protection laws in Mexico, as well as regulations dealing with e-commerce and electronic payments.

2.3 What regulatory schemes apply to consumer devices in particular?

Consumer devices require marketing authorisations from COFEPRIS in order to be marketed in Mexico. Marketing authorisation requirements, for medical devices in particular, depend on the level of risk involved in their use, according to a threefold classification system:

- Class I: products that are well known in medical practice and for which safety and efficacy have been proven. They are not usually introduced into a patient's body.
- Class II: products that are well known in medical practice but may have material or strength modifications. If introduced, they remain in a patient's body for less than 30 days.
- Class III: products either recently accepted in medical practice or that remain in a patient's body for more than 30 days.

The Mexican Pharmacopoeia provides manufacturers with specific rules and examples as guidance to classify medical devices.

Furthermore, COFEPRIS published a list of medical devices in 2014, which specifies which devices do not require regulatory approval in order to be marketed and sold in Mexico. Such products are usually those that are low risk to a patient's health.

In addition, since consumer devices are also collecting and transferring personal information to various parties, it is also necessary that they comply with data protection laws in Mexico, as well as with regulations dealing with e-commerce and electronic payments.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The Mexican authority responsible for enforcing the regulatory framework is COFEPRIS. COFEPRIS analyses all medical devices, and if applicable, software that enables them to work.

Additionally, the National Center of Health Technology Excellence was created in order to develop guidelines to evaluate health technologies and clinical practices and manage medical equipment and telemedicine.

The National Institute of Transparency, Access to Information and Personal Data Protection (INAI) is the authority responsible for overseeing the Law. Its main purpose is the disclosure of governmental activities, budgets and overall public information, as well as the protection of personal data and the individuals' right to privacy. The INAI has the authority to conduct investigations, review and sanction data protection controllers, and authorise, oversee and revoke certifying entities.

The Ministry of Economy is responsible for informing and educating about the obligations for the protection of personal data between national and international corporations with commercial activities in the Mexican territory. Among other responsibilities, it must issue the relevant guidelines for the content and scope of the Privacy Notice in cooperation with the INAI.

The Federal Consumer Office (PROFECO) monitors the compliance of the applicable provisions concerning information and advertising which could also be applicable to digital health. Additionally, PROFECO observes that "information or advertising of goods, products or services that are disseminated by any means or form must be truthful, verifiable, clear and free of texts, dialogues, sounds, images, trademarks, appellations of origin and other descriptions that lead or may lead to misleading, confusing, deceptive or abusive information".

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

COFEPRIS can initiate *ex officio* legal proceedings to sanction non-compliance. Ultimately, these legal proceedings can result in the revocation of the marketing authorisation. COFEPRIS is also entitled to implement measures on behalf of public health, such as the seizure of products and ordering partial or total suspension of activities, services or adverts. Under certain conditions, COFEPRIS has statutory authority to revoke any manufacturing approval or impose sanctions, ranging from a fine of up to 16,000 times the minimum wage to closure of the establishment.

The imposition of administrative sanctions does not exclude civil and criminal liability. Administrative infringements can incur penalties ranging from a fine of up to 20,000 times the minimum wage to final closure of the establishment. Repeated infringement is also considered to be a criminal offence.

COFEPRIS has broad jurisdiction to seize counterfeit or illegal devices. The General Health Law classifies the manufacturing and sale of counterfeit or falsified devices as a crime. In addition, COFEPRIS commonly enters into collaborative agreements with the *Fiscalía General de la República* (*FGR*) and the Customs Office in order to investigate and prevent counterfeit and illegal devices from entering the Mexican market.

In accordance with the Federal Law on Protection of Consumers, the PROFECO can monitor the compliance of the applicable provisions concerning information and advertising which could also be applicable to digital health. This Law provides that "information or advertising of goods, products or services that are disseminated by any means or form must be truthful, verifiable, clear and free of texts, dialogues, sounds, images, trademarks, appellations of origin and other descriptions that lead or may lead to misleading, confusing, deceptive or abusive information". In addition, the provider of goods and services is obliged to comply with the specifications of the goods or services offered.

Since all information dealing with consumer's health is deemed to be sensitive, affected consumers of digital health devices or services may request INAI to initiate an investigative process in case of a data breach, or in case of any other violation to the health information of a data subject. INAI, attending said complaint or *ex officio* may initiate the investigative process and if it considers that there was any data breach or any other violation to Mexican Data Protection Laws, it may impose administrative sanctions such as fines of up to MXN25,000,000 (approximately USD1,400,000).

Additionally, there are two activities deemed as felonies related to the wrong use of personal information (PI), which are:

i) When a data owner authorised to collect, store and use PI with the aim of profiting, causes a security breach in the database containing PI under its custody. This is sanctioned with imprisonment from three months up to three years.

ii) To collect, use or store PI, with the aim of profiting, through error or deceit of the data subject, or error or deceit of the person who has to authorise the transfer. This is sanctioned with imprisonment from six months up to five years.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

There are no specific regulations that apply to Software as a Medical Device (SaMD) and its approval for clinical use. As mentioned above, medical devices, a group under which digital technologies would currently fall, would require a marketing

authorisation from COFEPRIS in order to be marketed and sold in Mexico.

So far, the regulations applicable to SaMD are those mentioned in the answer to question 2.1. However, COFEPRIS may already be addressing the need for regulation of digital health technologies, especially for those that may present health risks.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  In Mexico, *telemedicine* is understood to include all aspects of incorporating information and communication technology (TIC) into health systems, with the aim of exchanging information in the field of health.
  If providing medical attention or services that require a medical licence *via* telemedicine, it is important to consider professional liability and whether insurance policies cover such services.
  Furthermore, if personal or sensitive personal information is collected or transferred, entities will need to be aware of the legal implications, which are discussed further below.
  There is a proposal of amendments to the General Health Law. This initiative aims to implement telemedicine through electronic means. For this purpose, it suggests that both:
  - Medical prescriptions should be issued in digital form.
  - The provision of prescriptions in digital form should be implemented by public and private agencies as well as the organs of the National Health System, subject to any Mexican regulatory and official regulations issued by the COFEPRIS.
- **Robotics**
  Robotics, particularly robotic surgery, has advanced to a world class standard in Mexico. However, risks still exist, and again, liability is an important consideration for when things go wrong. Legislation in Mexico is yet to be developed to cover such situations.
- **Wearables**
  As explained above, a medical device is defined as to be used in the diagnosis, monitoring or prevention of diseases in human beings, or in the treatment of those diseases or disabilities, as well as in the replacement, correction, restoration or modification of human physiological processes or anatomy.
  Whether a "wearable" or smartwatch will be considered as a medical device will depend on the specifications of such device and its purpose.
  In the List of Medical Devices that do not require regulatory approval, stopwatches are included ("*Relojes de tiempo transcurrido*"). Therefore, depending on the function of the particular wearable, regulatory approval may or may not be required.
- **Virtual Assistants (e.g. Alexa)**
  In Mexico, Virtual Assistants are used in the healthcare sector to schedule patient appointments. Virtual Assistants involve intelligent bots to organise, confirm and cancel appointments without any need for human intervention.
  Given that this technology stores information on the Cloud, an important consideration is data security and privacy. This is discussed in more detail below.
- **Mobile Apps**
  As explained for *telemedicine*, medical mobile application developers or entities that deliver services through the same will need to be aware of any professional liabilities or licences required when providing medical services or advice.
  In relation to regulatory approval, COFEPRIS may already be addressing the need for regulations for mobile medical applications, especially for those that present health risks.
- **Software as a Medical Device**
  Due to its nature, it is common that SaMD in Mexico involves data collection, so if personal or sensitive personal information is collected or transferred, entities must be aware of the legal implications, which are discussed further below.
  In addition, it is worth considering that patent protection is not available for software as such, unless it implicates computer-readable claims which meet the patentability requirements in its methodology and functions involved. Also, copyright protection is available for software.
- **AI-as-a-Service**
  In Mexico, the most recent development of AI in health is the use of AI-as-a-Service for the analysis of cancer data. The requirement of large amounts of data for AI means the risks of data security and privacy must be considered, particularly because the data used, i.e. sensitive medical data, has higher legal requirements.
- **IoT and Connected Devices**
  Similarly to the above, applying internet of things (IoT) and Connected Devices to the healthcare sector carries risks in data security and privacy. The close monitoring of this technology and the implementation of safeguards is crucial when using it in a medical setting.
- **3D Printing/Bioprinting**
  In the following years, 3D Printing/Bioprinting will provide the health sector with the possibility to print human organs. Currently, sections of bones are already being printed. Nowadays it is possible to print tissue with blood flow, but it is not yet approved for use. Evidence and studies are still needed to avoid risks for the population. Legislation in Mexico related to 3D Printing/Bioprinting is still pending, but it should be considered a medical device and should require marketing authorisation.
- **Natural Language Processing**
  As mentioned above in the answer to Virtual Assistants, Natural Language Processing tools such as chatbots can be applied in the healthcare sector to program medical appointments and answer frequently asked questions without the need for human intervention.
  Given that this technology stores personal information on the Cloud, an important consideration is data security and privacy. This is discussed in more detail below.

3.2 What are the key issues for digital platform providers?

The key issues that should be taken into consideration by digital platform providers are:

- Safety.
- Quality.
- Effectiveness.
- Data protection.
- Tax (see question 7.2).

These providers should carefully monitor changes to the legislation given that this field is still developing in Mexico.

4 Data Use

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

The main issues are the scope of data storage, processing and

sharing, the requirement to appoint a data protection officer and how to manage data security and data breaches.

- The key issue to consider, regarding personal information in digital health, is that all information regarding the health of any data subject is deemed to be sensitive. Therefore, the basis for the collecting, processing, sharing or transferring of said information, is the consent of the data subject, being the case that when dealing with sensitive information, the consent must be expressed in writing (consent obtained through digital means is acceptable, but the data subject must express his/her consent through an active process such as an opt-in mechanism, without any pre-checked boxes).

  It is also important to remember that an exception for the obtaining of the consent of the data subject, for the collection, use and transfer of his/her personal information, is when said personal information is essential for certain medical or health matters where the individual is unable to provide consent.
- In Mexico, there is no regulation dealing with the sharing of data that does not constitute personal information. In other words, if the information to be shared between two or more parties involved in digital health is not personal information as set forth in Mexican law, then it can be shared. This may change in the future, since international trends are starting to impose some restrictions on data sharing, which may be adopted in the future by Mexico.

Another key concern must be that if any digital health product or service implies the creation of a database including sensitive personal information, the authorisation from Mexican DPA (INAI) is required.

As stated above, it is advisable to bear in mind the concepts of privacy by design and self-certification schemes when designing digital health products or services, in order to ensure that they are fully compliant with Mexican law.

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

Although in Mexico we have two different bodies of law regulating the protection of personal information, depending on whether the data collector or data processor belongs to the public administration, or whether it is a private entity; the principles for the collection, use, sharing and transfer of data are basically the same, the key principle and basis for the treatment being the consent of the data subject.

4.3 Which key regulatory requirements apply?

The principal data protection regulation is found (i) in Articles 6 and 16 of the Mexican Constitution, and (ii) in the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations, published in July 2010 and December 2011, respectively.

Other applicable regulations include:

- The General Law for the Protection of Personal Data in the Possession of Obliged Subjects, which regulates the processing of personal information in any Federal, State or local authority's possession.
- The Privacy Notice Rules.
- The Binding Self-Regulation Parameters.

In general, Mexican data protection laws follow international correlative laws, directives and statutes, and therefore have similar principles, scopes of regulation and provisions.

The key principles that apply to the processing of personal data are:

- Transparency – although not specifically defined, the Law clearly states that personal data cannot be collected, stored or used through deceitful or fraudulent means.
- Lawful basis for processing – the collector is responsible for processing personal and/or sensitive data in accordance with the principles set forth in the Law and international treaties.
- Purpose limitation – personal data shall only be processed in compliance with the purpose set out in the Privacy Notice.
- Data minimisation – the collector shall make reasonable efforts to ensure that the amount of personal data processed is as little as necessary according to the purpose.
- Proportionality – data controllers can only collect personal data that is necessary, appropriate and relevant for the purpose.
- Retention – the collector can only retain personal data for the period of time necessary to comply with the purpose, and is obliged to block, cancel or supress the personal data thereafter.

4.4 Do the regulations define the scope of data use?

The regulations define "processing" as the collection, use, disclosure or storage of personal data, by any means. The use covers any action of access, management, benefit, transfer or disposal of personal data.

"Personal data" is defined as any information concerning an individual that may be identified or identifiable.

4.5 What are the key contractual considerations?

From the data protection standpoint, the main key contractual consideration to be observed is that the data collector is responsible for any processing of personal information carried out by the data processors that it decides to use for the operation of digital health devices or services. Therefore, in accordance with Mexican law, the data collector must make sure that any data processors that it employs assumes the same obligations as the data collector, towards the personal information of the data subjects. For this purpose, it is convenient to use binding corporate rules or standard contractual clauses.

If a processor is appointed to process personal data on behalf of a business, there must be a contract in place to establish the scope of the relationship.

The agreement should be in writing and signed by both parties. It should contain at least the following obligations for the processor:

i) to treat personal data only according to the instructions of the business;
ii) to treat personal data only for the purposes outlined by the business;
iii) to implement security measures in accordance with the law, and other applicable provisions;
iv) to keep the personal data to be processed confidential;
v) to delete all personal data processed once the legal relationship with the business has ended, or when the instructions of the business have been carried out, provided there is no legal provision that requires the preservation of the personal data; and
vi) to refrain from transferring personal data unless the business or a competent authority requires it.

4.6 How important is it to secure comprehensive rights to data that is used or collected?

It is highly important to guarantee the rights of the personal data used or collected, as to provide certainty to the users. As well, it is worth bearing in mind that any violation to such rights would be subject to a sanction in accordance to the applicable legislation. The Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations contemplate infringements and sanctions that might be imposed, previous rights protection procedure or the verification procedure carried out by the Institute.

5 Data Sharing

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

If the controller wishes to transfer any personal data to third parties, whether domestic or foreign, it must obtain the data subject's informed consent for such data transfer in advance of any transfer, by means of a Privacy Notice.

According to Article 37 of the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations (FLPPIPPE), consent is not necessary in the following circumstances:

- When the transfer is expressly allowed by the Law.
- When personal data is already available in the public domain.
- When personal data has been disassociated from any identifiable parameters.
- When the collection of personal data is required for the compliance with obligations pursuant to a legal relationship between the data subject and the data owner.
- When there is an emergency that jeopardises the data subject.
- When the collection of personal data is indispensable for medical attention and/or diagnosis, for rendering sanitary assistance, for medical treatment or sanitary services. This applies provided that the data subject is not in a condition to give consent, and provided that the data collection is performed by a person subject to legal professional privilege.

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

Mexican law does not really establish different considerations regardless of whether the collecting, processing and sharing of personal information is carried out by a private entity or an entity from the public administration.

The key principle is that the basis for the lawful collection and processing of personal information is the consent, and when dealing with sensitive personal information the consent must be obtained in writing (digital means accepted).

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

In general, Mexican data protection laws follow international correlative laws, directives and statutes, and therefore have similar principles, scopes of regulation and provisions.

The key regulatory requirement consists of bearing in mind that a consumer's health information constitutes sensitive personal information and therefore, previous consent in writing is necessary for its sharing.

If the information to be shared is not personal information or has gone through an anonymisation process, or was obtained from any public source, then so far there are no restrictions for its sharing.

6 Intellectual Property

6.1 What is the scope of patent protection?

The criteria for patentability are:

- patentable subject matter (i.e. subject matter that is eligible for patent protection);
- novelty (i.e. anything not found in the prior art);
- inventive step (i.e. results of a creative process which are not obvious from the prior art to a person skilled in the art); and
- industrial application (i.e. the possibility of an invention being produced or used in any branch of economic activity).

According to Article 49 of the Federal Law of Protection to the Industrial Property the following subject matter is not patentable:

- inventions whose commercial exploitation would be contrary to public order or contravenes any legal provision, including those whose exploitation must be prohibited in order to protect the health or life of persons or animals, or to preserve plants or the environment;
- processes for modifying the germ line genetic identity of human beings and its products when they involve the possibility of developing a human being;
- uses of human embryos for industrial or commercial purposes;
- processes for modifying the genetic identity of animals which are likely to cause them suffering, without any substantial medical benefit to man or animal, and also animals resulting from such processes;
- plant varieties and animal breeds, except in the case of microorganisms;
- essentially biological processes for obtaining, reproducing and propagating plants and animals and the products resulting from such processes;
- methods for treatment of the human or animal body by surgery or therapy, as well as diagnostic methods;
- biological material can be patented if it is isolated or produced by means of a technical process; and
- the human body, at any stage in its formation or development, including germ cells, and the simple discovery of one of its elements or one of its products, including the sequence or partial sequence of a human gene.

Further, Article 47 of the Federal Law of Protection to the Industrial Property states that the following subject matter is not considered an invention:

- discoveries, scientific theories or their principles;
- mathematical methods;
- artistic or literary works or any other aesthetic creations;
- schemes, rules and methods for performing mental acts, playing games or doing business;
- computer programs;
- methods of presenting information;
- biological and genetic material as found in nature; and
- juxtapositions of known inventions or mixtures of known products, or alteration of the use, form, dimensions or materials thereof, except where in reality they are so

combined or merged that they cannot function separately or where their particular qualities or functions have been so modified as to produce an industrial result or use that is not obvious to a person skilled in the art.

Computer-readable claims are eligible for patent protection as long as the methodology and functions involved meet the patentability requirements.

6.2 What is the scope of copyright protection?

Copyright protection would be applicable for the protection of any original software used for rendering digital health services or for operating digital health devices, since Mexico opted for this sort of protection in connection with software.

A copyright certificate of registration would serve as the basis for bringing legal actions derived from the reproduction or unauthorised use of the copyrighted software.

6.3 What is the scope of trade secret protection?

Mexico does not have any national trade secret protection laws. Instead, it adheres to the provisions of Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), of which it is a signatory. Article 39 specifies that in order to qualify as a trade secret:

- The information must be secret (i.e. not generally known among, or readily accessible to persons within the circles that normally deal with the kind of information in question).
- The information has commercial value because it is secret.
- The information has been subject to reasonable steps to keep it secret, by the person lawfully in control of the information.

These principles are recognised in domestic law, through the Mexican Law of Industrial Property.

It has to be mentioned that as from November 5, 2020, a new Federal Law for the Protection of Industrial Property has been set into force, and in connection with trade secrets, this new law includes some changes, the most relevant one being the introduction of administrative infringement causes related to trade secrets, and the possibility of starting civil actions, before civil courts, aimed at collecting damages and losses derived from industrial property violations, including trade secrets.

This means that now the legal holder of trade secrets may attempt in Mexico either administrative, civil or criminal actions aimed at protecting its trade secrets.

6.4 What are the typical results on academic technology transfer rules?

There have been some examples of positive outcomes on the development of policies for academic technology transfer processes, however, this area of law requires further development in Mexico.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Mexico does not have any specific regulation for the intellectual property protection of SaMD.

Software as such cannot be patented in Mexico, since it falls within the prohibitions of Article 19 of the Industrial Property Law, which provides that computer programs are not considered inventions. Nevertheless, computer-readable claims are eligible for patent protection as long as the methodology and functions involved meet the patentability requirements.

As mentioned above, copyright protection is also available for software.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The main considerations that should be taken into account are the delimitation of tasks, rights and obligations of each party involved in the agreement. In addition, other external factors should be considered, such as regulatory requirements of the healthcare products and services, the speed of development of the field, the regulation for data collection, use, processing, and sharing, and tax and corporate compliance requirements.

7.2 What considerations apply in agreements between health care and non-health care companies?

Recently, the Mexican government approved several amendments to the Tax Law. In summary, digital health platform providers could be taxed even though the medical service itself is exempt from tax. Agreements between telemedicine providers and digital platforms can help to determine whether these entities fall within the scope of the law.

8 AI and Machine Learning

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

In Mexico, the role of machine learning in digital health would be exactly the same as those observed in any other country wherein machine learning is being applied in digital health; namely, in the obtaining of more accurate and faster diagnostics and diseases detection; the development of new and better drugs and treatments, and the improved provision of medical services through digital platforms and electronic devices.

8.2 How is training data licensed?

There are no special considerations from a Mexican perspective in connection with the licensing of training data. Since this is a topic of recent discussion in Mexico, international trends and best practices are being adopted. One of the most important ones is to have the attorneys involved in the machine learning process where the training data will be used, in order to elaborate an agreement wherein it is defined who owns the data, verify the accuracy of the data and determine the licensed uses of the training data, among others.

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

The ownership of inventions created by AI has not yet been tested in Mexico. Current legislation specifies that a human inventor is required in order for an invention to be patentable. Therefore, such algorithms would not be protected under any intellectual property rights.

As AI creates more and more inventions without active human involvement, Mexican lawmakers will need to debate and develop new laws in order to protect the inventions created.

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

As stated above, some of the main commercial considerations to have in mind when drafting data licensing agreements are:

- The ownership of the data.
- The treatment of original and derived data.
- Conflicting interests between vendors and customers' use of the data.
- Drafting a proper and tailored definition of the training data set.
- Defining in an accurate and tailored manner the uses of the licensed data.

9 Liability

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

As mentioned above, digital health is developing in Mexico but the laws surrounding it are yet to be decided. The rules of common civil law would apply. Digital health service providers should be diligent in checking any changes to the law to be informed about any potential liabilities in the event of adverse outcomes when using digital health technologies.

9.2 What cross-border considerations are there?

In general, the applicable regulation in Mexico concerning health products (i.e. medical devices) require marketing authorisation holders (MAH) to appoint a legal representative in Mexico (a company who has to comply with regulatory duties on behalf of the MAH):

- The local and legal representative (a company) has to be located in Mexico.
- The MAH must grant sufficient authority to the legal representative, who should have a broad scope of activities, since this representative must be able to comply with any kind of MAH's duties, such as labelling, technovigilance and/or pharmacovigilance and quality control responsibilities.

In addition, the NOM 240, which regulates technovigilance, requires the MAH of medical devices to inform of any adverse effect occurring abroad if the device involved is also commercialised in Mexico.

10 General

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

Mexican law regulates the processing of PII in services, applications, and infrastructure in cloud computing. That is, the external provision of computer services on-demand that involves the supply of infrastructure, platform, or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared. For these purposes, the data controller may resort to cloud computing using general contractual conditions or clauses.

These services may only be used when the provider complies at least with the following:

- it has and uses policies to protect personal data similar to the applicable principles and duties set out in the Law and these Regulations;
- it makes subcontracting that involves information about the service that is provided transparent;
- it abstains from including conditions to providing the service that authorises or permits it to assume the ownership of the information about which the service is provided;
- it maintains confidentiality with respect to the personal data for which it provides the service; and
- it has mechanisms at least for:
  - disclosing changes in its privacy policies or conditions of the service it provides;
  - permitting the data controller to limit the type of processing of personal data for which it provides the service;
  - establishing and maintaining adequate security measures to protect the personal data for which it provides the service;
  - ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it; and
  - impeding access to personal data for those who do not have proper authority for access or in the event of a request duly made by a competent authority and informing data controller. In any case, the data controller may not use services that do not ensure the proper protection of PII.

No guidelines have yet been issued to regulate the processing of PII in cloud computing.

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

The key issues that should be considered by non-healthcare companies before entering today's digital healthcare market are mainly the regulatory requirements of the healthcare products and services, the speed of development of the field, the Mexican reimbursement systems (public and private sector), the regulation for data collection, use, processing, and sharing, and tax and corporate compliance requirements.

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

Digital health is a relatively new industry in which many of the businesses operating are start-ups or scale-ups. Any investor should consider the risks that could accompany such types of businesses, such as poor management structure or inadequate processes.

Another important consideration when making a decision to invest is how the market perceives digital health services. In Mexico, digital health services are still developing and therefore investment may be slow. Also, the digital health sector shifts rapidly and therefore investors must consider whether a certain company will provide long-term profits.

Finally, data security and privacy breaches may decide the success and survival of a company. In Mexico, data protection laws largely follow similar laws of other countries, and digital health service providers must follow such laws. Also, if processing or transferring data internationally, companies must

ensure they comply with international laws on data protection such as the GDPR; the EU–US Privacy Shield, or any other future regulations substituting these. Any investor must be sure these laws are being fully complied with by Mexican digital health service providers before investing, to avoid any risks in losing their investment if a breach occurs.

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

The principal key barrier holding back widespread clinical adoption of digital health solutions is that digital health is still relatively new in Mexico and its application in real-life settings is still limited, so the legislation in this field is still developing in Mexico.

10.5 How critical is it for a digital health solution to obtain formal endorsement from physician certification bodies (e.g., American College of Radiology, etc.) as a driver of clinical adoption?

The formal endorsement from physician certification bodies would be of great importance, because it would generate an impulse for the development of laws and provisions in this area.

Abraham Díaz co-chairs the Privacy and IT Industry group and has a wealth of knowledge across the IP spectrum. Abraham focuses his practice on copyright, trademarks and unfair competition, litigation, licensing and prosecution matters. He counsels clients on any IP-related matters, and handles matters involving trademarks, trade dress, product configuration, unfair competition, advertisement-related matters, false advertising, trade secrets, plant breeders' rights, vegetal varieties and Internet-related IP issues. His Internet experience includes handling domain disputes under the UDRP, as well as counselling clients concerning the development of websites and the protection of the content thereof.

He also counsels clients with regard to the correct implementation, monitoring and auditing of privacy management programmes, and crisis and data breach management.

Because of his broad background, Abraham is perfectly placed to advise clients on a range of subjects and is able to assess the legal needs within this sector from a 360° standpoint.

OLIVARES
Pedro Luis Ogazón 17
San Ángel 01000
Ciudad de México
Mexico

Tel: +55 5322 3000
Email: abraham.diaz@olivares.mx
URL: www.olivares.mx

Ingrid Ortíz is a member of the Life Sciences & Pharmaceutical law group and works on related matters, such as digital health, at OLIVARES. Her practice is mainly focused on Intellectual Property Litigation, Regulatory and Administrative Litigation; as well as Regulatory and Compliance advisory concerning, among others, digital health. Her main areas of practice allow her to interact with the Mexican sanitary agency, among others, the Federal Commission for Protection against Sanitary Risks (by its acronym in Spanish COFEPRIS), the Mexican Patent and Trademark Office (by its acronym in Spanish "IMPI"), and the Courts of law, such as the Federal Court of Tax and Administrative Affairs, the Federal District Courts and the Federal Circuit Courts.

OLIVARES
Pedro Luis Ogazón 17
San Ángel 01000
Ciudad de México
Mexico

Tel: +55 5322 3000
Email: ingrid.munoz@olivares.mx
URL: www.olivares.mx

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
Outsourcing
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
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group