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

Switzerland


Dr. Stefan Kohler


Christian Wyss

VISCHER

1 Digital Health and Health Care IT

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

In Switzerland, digital health is not a legal term. In general, the term covers services and equipment that use information and communication technologies (ICT) in healthcare to improve healthcare and public health. In agreement with this, the Swiss government defines the term "eHealth" as the integrated use of ICT to design, support and network all processes and participants in the healthcare system.

1.2 What are the key emerging technologies in this area?

Numerous digital health solutions are currently being tested and implemented. The following solutions could become relevant in the coming years and possibly lead to disruptive innovations:

- Wearables: Mobile sensors that are worn directly on the body which continuously collect physiological data (e.g. blood pressure, temperature, pulse) and evaluate them in real time.
- Health monitoring and care using robots and sensors: Robots and/or room sensors are used to monitor and care for patients or other people in need of care (e.g. in nursing homes).
- Digital avatars and assistance systems: Computer-supported artificial and graphic representations of a person, which support people visually and/or linguistically in a task (e.g. virtual school lessons for children in hospital).
- Machine learning and predictive analysis: Based on artificial intelligence (AI), software systems process and analyse large amounts of data and automatically optimise themselves (e.g. efficient analysis of DNA sequences with AI-based mechanisms for the detection of genetic diseases).
- Online health counselling: Health-related counselling services, diagnoses and referral to doctors can be obtained on digital platforms or apps (e.g. dermatological diagnoses or health insurance counselling services).

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

According to Swiss law, personal health data are considered "particularly worthy of protection". Accordingly, data security and data protection are regularly the main issue with digital health solutions. Providers of digital health solutions, such as wearables, health apps or electronic patient records (EPR), must comply with the applicable data protection regulations, in particular the Federal Data Protection Act and – in the European context – the General Data Protection Ordinance (GDPR). In addition, other decrees may be relevant in Switzerland, such as the Federal Law on Human Genetic Testing or the Human Research Act.

Further legal issues:

- The cantons sometimes set different standards in the field of digital health, which can make it difficult to introduce digital health applications uniformly throughout Switzerland. However, for providers of digital healthcare solutions, the differences between the cantons can also provide scope for implementing an innovative business idea.
- In the field of telemedicine and other digital service areas, the billing and remuneration models are still largely unclear. The currently applicable tariff system covers digital services incompletely. Incentives for digital health solutions are missing.
- There are still uncertainties regarding the qualification of software and apps as medical devices and the conformity assessment of such solutions.

2 Regulatory

2.1 What are the core health care regulatory schemes?

- **Therapeutic Products**
  - Federal Act on Medicinal Products and Medical Devices (Therapeutic Products Act, TPA; no. 812.21).
  - Ordinance on Licensing in the Medicinal Products Sector (no. 812.212.1).
  - Ordinance on Medicinal Products (no. 812.212.21).
  - Ordinance on the Advertising of Medicinal Products (no. 812.212.5).
  - Medical Devices Ordinance (MedDO; no. 812.213).
  - Ordinance on the List of Medical Devices Subject to Prescription (no. 812.213.6).
  - Ordinance on Integrity and Transparency in the Therapeutic Products Sector (no. 812.214.31).
- **Research on Humans**
  - Federal Act on Research involving Human Beings (Human Research Act, HRA; no. 810.30).
  - Ordinance on Human Research with the Exception of Clinical Trials (Human Research Ordinance, HRO; no. 810.301).
  - Ordinance on Clinical Trials in Human Research (Clinical Trials Ordinance; ClinO; no. 810.305).

- Ordinance on Organisational Aspects of the Human Research Act (HRA Organisation Ordinance, OrgO-HRA; no. 810.308).
- Federal Act on Research Involving Embryonic Stem Cells (Stem Cell Research Act, StRA; no. 810.31).
- Ordinance on Research involving Embryonic Stem Cells (Stem Cell Research Ordinance, SCRO; no. 810.311).

- **Transplantation**
  - Federal Act on the Transplantation of Organs, Tissues and Cells (Transplantation Act; no. 810.21).
  - Ordinance on the Transplantation of Human Organs, Tissues and Cells (Transplant Ordinance; no. 810.211).
  - Ordinance on the National Cross-Over Living Donation Programme (no. 810.212.3).
  - Ordinance on the Allocation of Organs for Transplantation (no. 810.212.4).
- **Communicable Diseases**
  - Federal Act on Protection against Infectious Diseases in Humans (Epidemics Act, EpidA; no. 818.101).
  - Ordinance on Protection against Infectious Diseases in Humans (no. 818.101.1).
- **Medically Assisted Reproduction and Genetic Testing**
  - Federal Act on Medically Assisted Reproduction (Reproductive Medicine Act; no. 810.11).
  - Reproductive Medicine Ordinance (no. 810.112.2).
  - Ordinance on the National Ethics Committee in the Field of Human Medicine (no. 810.113).
  - Federal Act on Genetic Testing of Human Beings (no. 810.12).
  - Ordinance on Genetic Testing of Humans (no. 810.122.1).
  - Ordinance on the preparation of DNA Profiles in Civil and Administrative Matters (no. 810.122.2).
- **Requirements for Healthcare Professionals**
  - Federal law on the University Medical Professions (Medical Profession Act, MedBG; no. 811.11).
  - Medical Profession Ordinance (no. 811.112.0).
  - Cantonal implementing legislation on healthcare professionals.
- **Health Insurance and Reimbursement**
  - Federal Act on Health Insurance (HIA; no. 832.10).
  - Ordinance on Health Insurance (HIO; no. 832.102).
  - Ordinance on Benefits in the Compulsory Health Insurance (HIBO; no. 832.112.31).
  - Ordinance on the Determination of Costs and the Recording of Services by Hospitals, Birth Centres and Nursing Homes in Health Insurance (no. 832.104).

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

- **Data Protection**
  - Federal Act on Data Protection (FADP; no. 235.1).
  - Ordinance to the Federal Act on Data Protection (no. 235.11).
- **Electronic Patient Record (EPR)**
  - Federal Act on the Electronic Patient Record (EPRA; no. 816.1).
  - Ordinance on the Electronic Patient Record (no. 816.11).
  - Federal Council Ordinance on the Electronic Patient Record (no. 816.111).
  - Federal Council Ordinance on Financial Aid for the Electronic Patient Record (no. 816.12).
  - Departmental Ordinance on the Electronic Patient Record.
  - Cantonal legislation: Cantons must check their respective legal systems for compatibility with the EPRA and its implementing law and, if necessary, initiate adjustments.

2.3 What regulatory schemes apply to consumer devices in particular?

So far, there are no special legal regulatory schemes for digital health devices in Switzerland. With regard to the warranted properties and the rights of consumers in relation to defects, the rules of contract law in the Swiss Code of Obligations (no. 220) apply. The Federal Act on Product Liability (no. 221.112.944) may (additionally) be relevant for liability in cases of personal injury, and the Federal Act on Product Safety (no. 930.11) for product safety requirements.

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

- **Swiss Agency for Therapeutic Products (Swissmedic)**
  Swissmedic (with headquarters in Berne) is responsible for the enforcement of the Swiss legislation on therapeutic products. Swissmedic's remit mainly involves the granting of marketing authorisations and operating licences and market surveillance. Swissmedic's enforcement competence also includes the ordering of administrative measures and/or administrative criminal investigations.
- **Federal Office of Public Health (FOPH)**
  The FOPH is generally responsible for the health of the Swiss population, develops Swiss health policy and is committed to a health system that is efficient and affordable in the long term. Among other things, the FOPH deals with questions concerning reimbursement of medical analysis and treatments, pharmaceuticals and medical devices by health insurers. The FOPH is also responsible for the enforcement of the integrity and transparency regulations in the field of therapeutic products. The FOPH's enforcement competence also includes the ordering of administrative measures or administrative criminal investigations.
- **Cantonal Authorities**
  Cantonal Authorities are responsible for the surveillance and enforcement of the Swiss legislation on therapeutic products in specific areas (e.g. carrying out inspections and quality controls). In the course of their monitoring services, the cantons shall notify Swissmedic or the FOPH in accordance with their respective responsibilities of any events, findings or complaints.
  Cantons issue the authorisation of mail-order trade in the health sector.
- **eHealth Suisse**
  To implement the eHealth strategy in Switzerland, the Federal Department of Home Affairs (FDHA) and the Conference of Cantonal Health Directors (CDC) jointly run the eHealth Suisse competence and coordination centre. The aim of eHealth Suisse is to define common organisational, legal and technical guidelines for the development of eHealth applications, in particular the EPR.
  eHealth Suisse has no enforcement competence as such.

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

Some of the key areas of enforcement relating to digital health are as follows:

- Enforcement of notification, authorisation and/or certification obligations (e.g. for applications qualifying as medical devices; for online medical consultation).
- Enforcement of data security and data protection obligations.
- Enforcement of restrictions applicable in the field of online genetic analyses, online diagnostic tests or other online medical services.
- Enforcement of restrictions in the area of pharmaceuticals (e.g. advertising restrictions, prescription restrictions, integrity obligations).
- Enforcement of professional obligations that medical personnel must comply with.
- Enforcement of the conditions that apply to reimbursement of digital health services by health insurance companies.

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

For medical devices, including digital health solutions, the following legislation on therapeutic products is primarily relevant:

- Therapeutic Products Act (TPA; no. 812.21).
- Ordinance on Medicinal Products (no. 812.212.21).

For the practical implementation of the legislation on therapeutic products, with particular reference to software-based medical devices, the competent Swiss authorities have published the following guidelines (as amended from time to time):

- Swissmedic Leaflet on Standalone Medical Device Software (*AW-Merkblatt Eigenständige Medizinprodukte-Software*).
- eHealth Suisse: Guide for App Developers, Manufacturers and Marketers.

Switzerland has concluded agreements on the mutual recognition of conformity assessments for medical devices (bilateral agreements or mutual recognition agreements – MRAs) with the EU Member States, the EFTA States and Turkey. The basis of these agreements is the application of the European directives for medical devices and the European CE marking. The countries concerned recognise the certificates issued by Swiss conformity assessment bodies and, in return, Switzerland recognises the conformity assessments carried out by Notified Bodies/Conformity Assessment Bodies in the countries concerned.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - Depending on their characteristics, telemedicine or virtual care platforms may qualify as medical devices. If so, the compliance of the platform with the legal requirements needs to be assessed by a Conformity Assessment Body (CAB).
  - Telemedicine or virtual care platforms as such may be subject to a notification or licensing requirement. The cantonal implementing legislation, including that on healthcare professionals, must be observed. It should be noted that the cantonal regulations in this regard are not uniform. Some cantonal legislations treat telemedicine or virtual care restrictively because they require the physician to physically meet and treat the patient.
  - The health data transferred via telemedicine or virtual care platforms are considered to be particularly worthy of protection. The platform operator must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - There are certain limits to diagnosis and treatment via telemedicine or virtual care platforms. Medical due diligence must be ensured at all times. According to the case law of the Swiss Federal Supreme Court, prescribing medicines via telemedicine or virtual care platforms requires that the patient receives personal and serious advice from a doctor. Some cantonal legislations treat telemedicine or virtual care restrictively because they require the physician to physically meet and treat the patient.
  - The responsibility and liability between the operators of the platform and the involved healthcare professionals must be clearly regulated both in the internal relationship (operator-doctor) and external relationship (operator-customers; doctors-patients).
- **Robotics**
  - Depending on their characteristics, robotic technologies used in healthcare may qualify as medical devices. If so, the compliance of the robot with the legal requirements needs to be assessed by a CAB.
  - If the robot is capable of collecting personal data, the operator must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the robot provides users with instructions or recommendations on certain behaviour. The allocation of liability issues between the parties involved (e.g. manufacturer, healthcare institution, healthcare professionals) must be contractually regulated.
  - The use of robots, especially in elderly and patient care, can affect the personal rights of those in need of care. Prior informed consent of the persons in need of care (or their legal representatives) should therefore be obtained.
- **Wearables**
  - Depending on their characteristics, wearables may qualify as medical devices. If so, the compliance of the device with the legal requirements needs to be assessed by a CAB.
  - Wearables collect and evaluate health data. The manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the wearables provide users with instructions or recommendations on certain behaviour.
- **Virtual Assistants (e.g. Alexa)**
  - Virtual assistants collect and evaluate personal data, including health data. The manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the virtual assistants provide users with instructions or recommendations on certain behaviour.
  - Virtual assistants can affect the personal rights of users. Prior informed consent of the users (or their legal representatives) should therefore be obtained.

- **Mobile Apps**
  - Depending on their characteristics, mobile apps may qualify as medical devices. If so, the compliance of the mobile app with the legal requirements needs to be assessed by a CAB.
  - If the mobile app is capable of collecting personal data, the manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the mobile app provides users with instructions or recommendations on certain behaviour. The allocation of liability issues between the parties involved (e.g. manufacturer, operator, health insurance company, healthcare professionals) must be contractually regulated.
- **Software as a Medical Device**
  - Compliance of the device with the medical device regulations needs to be assessed by a CAB.
  - The manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the device provides users with instructions or recommendations on certain behaviour. The allocation of liability issues between the parties involved (e.g. manufacturer, operator, health insurance company, healthcare professionals) must be contractually regulated.
- **AI-as-a-Service**
  - Depending on its characteristics, AI-as-a-service may qualify as a medical device. If so, the compliance of the service with the legal requirements needs to be assessed by a CAB.
  - Given the large amounts of data from a variety of sources used in AI systems, AI systems are prone to errors. The establishment and maintenance of a continuous and effective quality assurance concept is indispensable. The liability issues associated with AI in healthcare need to be carefully, contractually allocated between the parties involved (e.g. manufacturer, operator, health insurance company, healthcare professionals).
  - AI systems require large amounts of data from sources such as electronic health records, pharmacy records, insurance claims records, or patient-generated information. The operators of AI systems must ensure compliance with data protection legislation (including that on cybersecurity).
- **IoT and Connected Devices**
  - If the IoT and/or connected devices are capable of collecting personal data, the manufacturer must ensure that the legal requirements for data security (including cybersecurity) and data protection are met.
  - Particular questions of liability may arise if the IoT and/or connected devices provide users with instructions or recommendations on certain behaviour. The allocation of liability issues between the parties involved (e.g. manufacturers, operators, etc.) should be as far as possible contractually regulated.
- **3D Printing/Bioprinting**
  - Suppliers of the CAD files required for 3D printing must consider whether their print commands are subject to copyright protection. The external design of 3D printed products may be subject to third-party trademark or design protection, and their technical functionality may be subject to third-party patent protection.
  - The question of who is liable in the event of damage from defective 3D printing products can be complex and should be clarified in advance.
- **Natural Language Processing**
  - Natural language processing involves the processing and analysis of large amounts of natural language data. If these data can be attributed to a specific person (i.e. are not anonymised), the data protection legislation is relevant.

3.2 What are the key issues for digital platform providers?

The key legal issue with digital platforms is the question of whether the platform provider or the user (uploader) is responsible and liable for the uploaded content. There is no specific legal basis on this issue in Switzerland. Relevant in this regard are, on the one hand, the provisions of the Federal Law against Unfair Competition (no. 241) and, on the other hand – if statements that violate personality rights are in question – the civil and criminal law provisions on the protection of personality rights (in particular Art. 28 of the Swiss Civil Code: no. 210). According to Swiss legal practice, it is undisputed that the uploader is responsible for the uploaded content. Under certain circumstances, however, the platform provider may be held responsible for the content of the platform users as well. Accordingly, the Swiss Federal Supreme Court confirmed in its (attorney-criticised) decision no. 5A_792/2011 the joint responsibility of the provider in the case of a violation of personality rights committed via the platform (Art. 28 ZGB). Digital platform providers must therefore be aware that they do not have a general liability privilege in Switzerland for user content on the platform. Platform providers should exclude the respective liability risk as far as possible with suitable contractual agreements.

Another important issue is data protection and data security. Platform providers are required to implement the relevant requirements of data protection legislation on their platform.

4 Data Use

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

Data that is truly anonymised does not fall under data protection laws. As a result, it can be freely used for any purpose, including medical research. However, when large amounts of data are analysed, anonymisation reaches its limits. The comparison of anonymised data with other data entails the risk of reidentification of the previously anonymised data. Health data in particular is highly individualised, which makes effective anonymisation difficult. Using personal data for digital health applications means that all requirements of the applicable data protection laws must be complied with.

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

Swiss data protection law is technology-neutral. Note that all listed hospitals execute cantonal performance mandates and thus fall within the scope of cantonal data protection laws. Not only public listed hospitals but also private listed hospitals have to comply with cantonal data protection law unless there is special legislation that provides for an exemption. For hospitals without cantonal performance mandates and for all private digital health providers, the Swiss Federal Data Protection Act applies.

In addition, the GDPR also applies to Swiss digital health providers offering their services in EU countries.

4.3 Which key regulatory requirements apply?

The processing of data relating to specific or identifiable persons is subject to the Data Protection Act and under certain circumstances to the GDPR. In contrast to European law, Swiss law does not prohibit processing subject to permission as long as the processing is carried out lawfully and in accordance with the data processing principles of Arts 4, 5 and 7 FADP (*cf.* Art. 12 para. 2 lit. a FADP). These are:

- Principle of transparency: The collection of personal data and in particular the purpose of their processing must be identifiable to the data subject (Art. 4 para. 4 FADP).
- Principle of purpose limitation: Personal data may only be processed for the purpose that was stated at the time of acquisition, is apparent from the circumstances or is provided for by law (Art. 4 para. 3 FADP). As soon as the data processing goes beyond the purpose, justification, a legal basis or consent is necessary.
- Principle of proportionality: The processing of personal data must be proportionate, i.e. must not go further than the purpose of the processing requires (Art. 4 para. 2 FADP).
- Principle of data integrity: The processor must ensure the accuracy of the personal data and destroy incomplete or inaccurate personal data (Art. 5 para. 1 FADP).
- Principle of data security: Personal data must be protected against unauthorised processing by appropriate technical and organisational measures (Art. 7 para. 1 FADP).

Consequently, Swiss law does not require the consent of the person concerned or any other justification for the lawfulness of the processing of health data. It is sufficient for the person concerned to be informed of the purpose of the processing and the processor to comply with the purpose limitation principle and the other processing principles.

As already mentioned above, the GDPR has extraterritorial effects; therefore, Swiss service providers may also be affected.

The GDPR contains stricter regulations than the current FADP. Thus, the principle of prohibition subject to permission applies here. Permission can arise from the law or from the consent of the person concerned. However, the total revision of the FADP, where the draft is currently being discussed in parliament, will bring it into line with the GDPR. For example, according to the new draft, data managers and processors will have to take appropriate measures to reduce the risk of personal injury as early as the planning stage of data processing. In addition, they are obliged to ensure, by means of appropriate default settings, that only personal data that is relevant for the respective purpose is used (such as pseudonymisation, where knowledge of the data subject is not necessary for the processing). The new E-FADP is expected to enter into force in 2021.

With regard to medical research, further provisions of the Human Research Act must be observed. The Human Research Act allows the anonymisation of data and their subsequent use for research on humans only if it is not biological material or genetic personal data, or if the person concerned has been informed in advance and has not submitted his or her veto (Art. 32 para. 3 HRA).

Furthermore, a recent judgment in which the Federal Administrative Court had to assess the procurement of data by the supplementary health insurance provider from the compulsory health insurance within the same group showed that, in addition to the FADP, the data transfer provisions of Art. 84a of the Federal Health Insurance Act are also highly relevant for digital health providers.

4.4 Do the regulations define the scope of data use?

On the basis of the principle of proportionality pursuant to Art. 4 para. 2 FADP, the processing of data may not go beyond what is necessary for the purpose of processing. Accordingly, no data may be collected in stock.

4.5 What are the key contractual considerations?

Art. 4 para. 4 FADP provides that the data collection and the purpose of the processing must be identifiable for the data subject. According to Art. 4 para. 3 FADP, the processing of personal data may only be carried out for the purpose stated at the time of collection, which is apparent from the circumstances or is provided by law. Explicit consent is required for the collection of particularly sensitive personal data, such as data on health. However, such consent is only valid if the person has been adequately informed and has subsequently given his or her informed consent voluntarily. In addition, the consent can also be withdrawn at any time, whereby the burden of proof for the existence of the consent lies with the data processor in each case. For the information to be considered appropriate to the data subject, it must at least cover the type, scope and purpose of the data processing, the names of the data processors and, if applicable, the risks of the data processing (informed consent). Due to these requirements regarding the adequacy of information, blank consent to any future form of processing is only possible if it is carried out with clear limits. In principle, it is also possible to integrate data protection provisions into general terms and conditions if the data subjects are adequately informed about the scope of their consent and the data protection provisions are presented clearly enough. Here too, however, explicit consent is required for data on health. In addition, Art. 8 of the Federal Act Against Unfair Competition prohibits general terms and conditions that, against the principles of good faith, provide for a significant and unjustified disproportion between a consumer's contractual rights and obligations to the detriment of the consumer. Data subjects of health data qualify as consumers. Thus, general terms and conditions must not only ensure that the data subjects explicitly consent to having their health data processed, but must also provide for a reasonable balance of the data subject's contractual rights and obligations.

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

Data has become a raw material that enables the development of new products, services and value chains. Accordingly, securing rights to data can be crucial to business success. Under current law in Switzerland, there is no independent law governing the ownership of data. Whoever has de facto control over data can prevent the use by third parties by not disclosing them and keeping them secret. In addition, there is always the possibility of regulating the use of data by agreement.

5 Data Sharing

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

Art. 10a FADP allows the use of data processors unless prohibited by legal or contractual confidentiality obligations. The data subject must be informed, however, in the case of a transfer of

the personal data to a country that does not have an adequate level of data protection.

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

The duty to provide information and the right of access to personal data may vary depending on whether the personal data were obtained from the data subject themselves or not. If the personal data have not been obtained from the data subject, the responsible person must also provide the contact details of the data protection officer and the categories of personal data processed. In addition, the data subject must be provided with information on the source of the data and whether these sources are publicly available.

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

The disclosure of particularly sensitive data (health data) to third parties always requires justification (Art. 12 para. 2 lit. c FADP). If the justification lies in the consent of the data subject (Art. 13 para. 1 FADP), this must be given voluntarily and explicitly after appropriate information (Art. 4 para. 5 FADP). The data subject then always has the opportunity to object to the processing (Art. 12 para. 2 lit. b FADP).

According to the new draft of the FADP, the list will extend the existing list of particularly sensitive personal data. Genetic and biometric data (e.g. fingerprints), which uniquely identify a natural person, have recently also been taken into account.

6 Intellectual Property

6.1 What is the scope of patent protection?

Inventions are subject to patent protection, i.e. new technical solutions to technical problems, whereas private use, research and teaching are excluded from the protective effect of a patent. What is unique to Switzerland is that there is no official examination for novelty or an inventive step. The scope of protection is defined in the patent claims and the period of protection is a maximum of 20 years, whereby a Swiss patent automatically also applies in Liechtenstein. Switzerland is a member of all major regional and international patent treaties, including the European Patent Convention (EPC) and the Patent Cooperation Treaty (PCT).

6.2 What is the scope of copyright protection?

Literary and artistic intellectual creations (including computer programs) with an individual character are subject to copyright protection, irrespective of their value or purpose. Such creations automatically become protected at the moment of creation. The author has the exclusive right to his own work and the right to recognition of his authorship. The author has the exclusive right to decide whether, when, how and under what author's designation his own work is published for the first time. The period of protection is up to 70 years after the death of the author (50 years for computer programs). What is unique to Switzerland are the collective rights management organisations such as SUISSIMAGE. Moreover, various international agreements on copyright, such as the Revised Berne Convention (WCT), ensure that Swiss authors receive the same protection as foreign authors.

6.3 What is the scope of trade secret protection?

Though Switzerland lacks specific trade secret laws, many aspects of trade secret protection are adequately covered. For instance, there are provisions on certain aspects of trade secrets protection in the Unfair Competition Act (no. 241; e.g. prohibition of exploitation or use of trade secrets that were unlawfully obtained), the Criminal Code (i.e. anyone who divulges a trade secret that he is under a statutory or contractual duty not to reveal, or anyone who exploits for himself or another such a betrayal, is liable to criminal sanctions), and the Code of Obligations (i.e. employment law: employees must not exploit or reveal confidential information – such as trade secrets – obtained while in the employer's service). As a consequence of the diversity of legal provisions on trade secrets, there is no unique protection theory on trade secrets in Switzerland.

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

Most public research and educational institutions and university hospitals (PROs) in Switzerland have professionally organised bodies that ensure technology transfer with the private sector. Uniform regulations on this technology transfer are drawn up by the Swiss Technology Transfer Association (swiTT). The following main principles apply:

- Partnership: The cooperation between private enterprise and PROs rests on the basis of partnership. PROs are entitled to an appropriate financial share of the revenues generated by the cooperation partner through commercialisation of the intellectual property rights.
- Intellectual Property: As a rule, the PROs claim the intellectual property rights created by them within the scope of the cooperation for themselves, but grant the industrial partner exclusive rights of use.
- Freedom of Publication: The publication of scientifically interesting research results remains a central task of PROs. Before publication, adequate time for the preparation and submission of a patent application is contractually provided.

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

Under the prevailing Swiss doctrine, the term "software" is a generic term comprising both the computer program and the development and user documentation. Accordingly, for software as a medical device, copyright protection is paramount. Copyright law thus protects the concrete implementation, i.e. the program code, but not a process underlying a computer program.

The software used in a medical device as such cannot be protected by patents. However, computer programs used to implement a technical invention, so-called "computer-implemented inventions", are patentable under certain conditions (in particular, they must meet the requirement of technical character).

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

Collaborative improvements are a frequent source of dispute if the allocation of potential improvements has not been designed diligently enough. Partners with complementary expertise or

products usually need access to collaborative improvements of their own expertise or products, which can be used independently from the other partner's expertise or products. Collaborative improvements that are inseparably linked to both partners' expertise or products usually require the development and negotiation of a new business model that can be structured as collaboration and licence agreements (that may include cross-licences), joint ventures, or co-marketing agreements.

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

Healthcare companies are used to a strict regulatory framework and they must require their partners to meet these requirements whenever they apply. Non-healthcare companies may be used to a much more liberal environment and overlook or underestimate regulatory requirements. Therefore, it is key that agreements do not only clearly allocate regulatory responsibilities, but also provide for adequate collaboration and control mechanisms that allow and incentivise the non-healthcare company to identify and meet relevant regulatory requirements in due time.

8 AI and Machine Learning

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

Machine learning is expected to dramatically improve prognosis and diagnostic accuracy. It is also expected that machine learning will displace significant parts of the work of radiologists and anatomical pathologists. These physicians focus largely on interpreting digitised images, which can be fed directly to algorithms instead. Massive imaging data sets, combined with recent advances in computer vision, will drive rapid improvements in performance. Radiologists and anatomical pathologists will become much more AI-literate to assure quality and further improve AI-based prognosis and diagnostic tools.

8.2 How is training data licensed?

Training data is rarely licensed on an exclusive basis, but digital health providers that obtain one of those rare exclusive licenses to quality training data will certainly have an advantage over the competition. Also, training data pools are often dynamic and further data will be added or data quality will be improved over time. Thus, for digital health providers, it is key to ensure that they get access to such amended or improved versions of training data. Finally, certain government entities, such as the Federal Office for the Environment, offer open access to digital data for AI applications.

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

In Switzerland, copyright protection arises automatically upon creation of a work, regardless of any formality. Such a work must be an "intellectual creation" and must therefore have a human origin. As a result, a work generated by means of AI will only be eligible for copyright protection if a human being is involved in the process of its creation. In addition, the authors of a work obtained with AI can only be humans who have provided creative inputs that are linked to and reflected in the final work. In that sense, a "creative causal link" must be perceptible between the creative work of the author(s) and the resulting work. The occurrence and extent of human intervention remains decisive in appreciating the authorship. Whether or not this is the case has to be assessed on a case-by-case basis. Authors may be, for example, individuals who provide the AI with decisive input in the process of creating a work by training a model to learn automatically or persons who have defined the goal to be achieved by the AI by specifically parameterising the AI.

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

Companies wishing to use data in machine learning have an interest in developing their AI systems with the best possible data. This creates a tension between their business interests and the legal data protection framework. As a result, the training data must be carefully selected. In addition, especially in the case of particularly sensitive personal data such as data on health or criminal prosecutions within the meaning of Art. 3 lit. c FADP, the ways in which the algorithm processes the data must stay within pre-defined limits. For example, it must be clarified whether the data may be further developed into complete data packages which could reveal additional sensitive information about the persons concerned.

Detailed quality data for use in machine learning is likely to have roughly the same commercial value as initial algorithms designed to solve a specific problem. Thus, we expect that whoever provides such detailed data on an exclusive basis for machine learning applications will negotiate for an important equity stake, upfront or milestone payments, royalties or other adequate compensation.

9 Liability

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

There are no specific liability rules addressing digital health. The civil liability rules generally apply, in particular Art. 41 *et seq.* (liability in tort) and Art. 97 *et seq.* (contractual liability) of the Swiss Code of Obligations (no. 220) as well as the Federal Act on Product Liability (no. 221.112.944, as based on the European Union's Directive 85/374/EEC).

The basic prerequisites of liability in tort are:

- damage;
- illegality;
- causality between damage and illegality; and
- misconduct attributable to the defendant.

The basic prerequisites of contractual liability are:

- breach of contract;
- damage;
- causality between the breach and the damage; and
- misconduct attributable to the obligor.

Product liability according to the PLA:

- The "producer" is strictly liable for personal injuries and death as well as damage to property caused by a product which did not provide the safety which could reasonably be expected.
- There is a broad definition of "producer".
- An injured person may raise additional claims based on other legal grounds.

In addition, legal violations with digital health applications can lead to criminal sanctions and/or administrative disciplinary measures, which find their basis, *inter alia*, in the Therapeutic Products Act or Data Protection Act.

9.2 What cross-border considerations are there?

In international situations, the applicable law is determined by the Swiss Private International Law (CPIL; no. 291). Concerning torts, the international tort law includes product liability as well as personal injury. Arts 134-139 CPIL provide special conflict-of-law rules for these specific categories of torts. In the case of such special tort, it must also be questioned whether a subsequent choice of law according to Art. 132 CPIL is permissible. If the parties do not choose the law and if there is no specific tort pursuant to Arts 134-139 CPIL, the law applicable to the pre-existing legal relationship between the counterparties (Art. 133 para. 3 CPIL) may be considered. If no such pre-existing relationship exists, and the damaging party and injured party have their habitual residence in the same country, the law of this country is applicable according to Art. 133 para. 1 CPIL. Only as the last possible connection does the traditional general principle of the connection to the place of tort (*lex loci delicti commissi*) come into play (Art. 133 para. 2 CPIL).

With regard to punitive, exemplary, moral or other non-compensatory damages, which are not available under Swiss law, Swiss courts refuse to award such damages even if the applicable foreign law provides for such damages (*cf.* Article 135 II CPIL).

The Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (no. 0.275.12) regulates the jurisdiction, recognition and enforcement of judgments between the Member States of the European Union, Switzerland, Norway and Iceland.

In contrast to civil law, the Swiss administrative law does not provide for specific conflict of law rules. The principle of territoriality applies: a situation occurring in a given territory must be assessed by the competent authorities of that territory in accordance with the law applicable there, and any exercise of sovereign powers or the use of coercive means is reserved to the relevant organs of the state, unless there are different intergovernmental arrangements.

International criminal law distinguishes between the principle of active personality (applicability of the law of the State of which the offender is a national) and the principle of passive personality (applicability of the law of the State of which the victim is a national). According to the real or protective principle, the law of the State whose interests have been harmed by the crime is to be applied; this is a special case of the effect principle.

10 General

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

In healthcare, patient data is subject to medical professional secrecy. "Swiss Cloud" providers based in Switzerland are also covered by Art. 321 of the Swiss Penal Code as vicarious agents of the physician or other medical professional. Thus, medical professional secrecy is maintained.

Patient data can be stored with foreign cloud providers if these cannot read the patient data (i.e. the patient data is encrypted and the cloud providers do not have the key). Technically, this requires that the patient data is encrypted in Switzerland before being transferred to the foreign cloud.

Finally, certain health data might not qualify as patient data covered by the medical professional secrecy. Digital health providers may process such data in Swiss or foreign cloud-based services subject to the usual data protection requirements. This might include, in particular, stating explicitly that these applications or uses are not intended for patient data covered by medical professional secrecy.

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

Non-healthcare companies entering the digital healthcare market must become familiar with the extensive regulatory requirements in the healthcare sector and integrate the cost of compliance in their business models. For example, if an app is subject to medical device regulation, increased requirements for quality management and documentation apply to development, programming, validation, testing and version management. A market launch in Switzerland also requires a CE mark and, in most cases, must be reported to Swissmedic.

At the app developer's expense, Swissmedic may carry out checks to determine whether an app qualifies as a medical device and whether the conditions for placing it on the market are met. If these conditions are not met, Swissmedic may withdraw the app from the market and prohibit further marketing in Switzerland and the EU.

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

When looking at the business model of a digital healthcare venture, a key issue is whether the venture's final product or service will be reimbursed by national health insurance plans, sold to patients without such reimbursement, sold to healthcare providers such as hospitals, or marketed to pharmaceutical or medical device companies to enhance their existing products or services. Another key issue is how the venture stands out from the competition, i.e. if there is solid patent, trademark or copyright protection or whether the concept is to be faster and better than the (potential) competition.

Legal issues to consider during due diligence are: who developed and who owns which parts of the software; who tested the software with what kind of data; and whether real-life data was used in the tests as well. Further legal issues are timing and costs for the regulatory pathway to comply with healthcare and data protection legislation.

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

A key barrier for widespread clinical adoption is switching the financing of digital health solutions from project-based financing to a sustainable financing through hospitals' ordinary budgets, health insurance providers, and patients. While it is relatively easy to get initial financing via research grants, industry collaborations, foundations, innovation budgets or similar sources, the switch to sustainably financing the costs of digital health solutions is a real challenge. Healthcare financing is not only controlled by market forces, but – to a large extent – by both federal and cantonal politics. Financing schemes and incentives differ substantially between publicly owned and privately owned hospitals, between hospitals and outpatient healthcare facilities,

and – to a lesser extent – between big university hospitals and smaller hospitals without academic affiliation. Unlocking the full potential of many digital health solutions, however, often requires not just a few, but a majority of players adopting a particular solution.

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?

Two issues play a crucial role in driving clinical adoption. First, the adoption and endorsement by a small number of leading clinicians, i.e. key opinion leaders in top hospital positions with a strong track record and presence both in the clinic and in academic research, who could at least potentially move to other hospitals both in Switzerland or internationally. Digital health solutions tested or even regularly used by them will quickly catch the attention of both their peers and hospital management. Second, hospital management, health insurance providers, governments and legislators need to understand the value of a digital health solution for the entire ecosystem and adopt appropriate rules and regulations to pay for the solution and split the costs between hospitals, health insurance providers, and patients. Endorsement from physician certification bodies usually follows while or after the above two processes are completed. However, the advantages of a digital health solution that has been successfully tested and used by early adopters in the clinic must be almost self-evident both to clinicians and payors. Thus, we do not see endorsement from physician certification bodies as a main driver of clinical adoption.

Dr. Stefan Kohler has extensive experience in IP/technology law and regulated markets such as healthcare, pharma, medtech, biotech, cosmetics and foodstuffs. He regularly represents Swiss and foreign companies before Swiss courts and administrative authorities. He first studied science at the ETH in Zurich which enabled him to accurately and legally classify technical-scientific facts.
Stefan is an associate judge at the Swiss Federal Patent Court, president elect of the board of the Swiss Licensing Executives Society (LES), board member of BioLawEurope, board member of Swiss Healthcare Startups (SHS) and a member of the Forum for Genetic Research of the Swiss Academy of Sciences. He is a lecturer at the entrepreneurship programme to boost the success of eHealth companies at the Università della Svizzera Italiana (USI) and teaches aspiring patent attorneys at the Swiss Institute for Intellectual Property in the field of licensing agreements, R&D agreements and technology transfer.

VISCHER
Schuetzengasse 1
P.O. Box
8021 Zurich
Switzerland

Tel: +41 58 211 34 19
Email: skohler@vischer.com
URL: www.vischer.com

Christian Wyss specialises in drafting and negotiating contracts for clients from the Life Sciences and Information Technology industries. Christian has extensive experience with technology transfer and licence agreements, research, development or marketing co-operations, clinical trial agreements, contract manufacturing agreements and distribution agreements. He regularly works with clients in financing rounds, acquisitions, or joint ventures and assists with intellectual property-related issues in M&A transactions. Christian also advises on implementing compliance with the Swiss data protection laws.
Christian's clients range from start-ups, over VC financed development stage companies, to industry leaders. Christian is familiar with balancing each project's technology-driven aspects and the requirements of industry partners, investors, or other constituencies.
Christian received his law degree from the University of Basel, Switzerland, and his LL.M. from Wake Forest University School of Law in Winston-Salem, North Carolina. He was admitted to the Bar in Switzerland in 2002.

VISCHER
Aeschenvorstadt 4
P.O. Box 329
4010 Basel
Switzerland

Tel: +41 58 211 33 39
Email: cwyss@vischer.com
URL: www.vischer.com

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