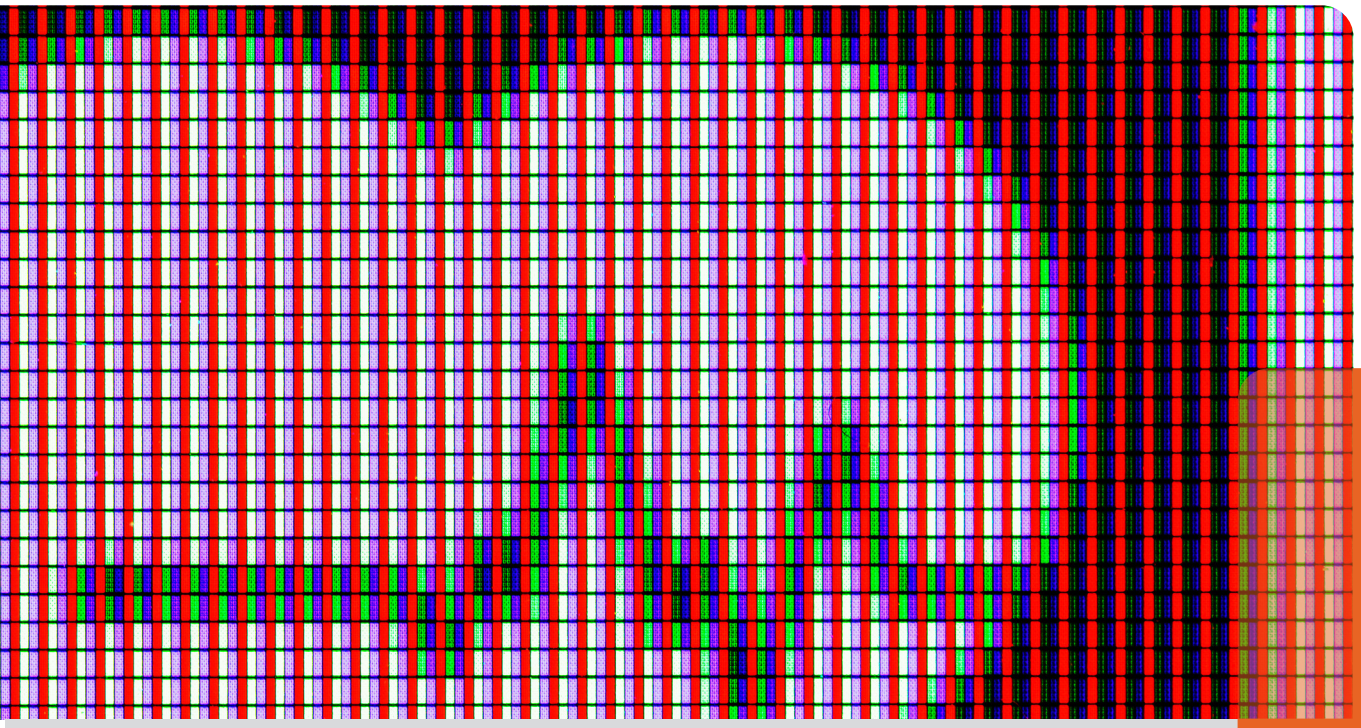
International
Comparative
Legal Guides



Digital Health

2024

Fifth Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

glg Global Legal Group

Introductory Chapter

Expert Analysis Chapters

Q&A Chapters

Switzerland


Tobias Meili


Carlo Conti


Martina Braun


André S. Berne

Wenger Plattner

1 Digital Health

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

There is no common general definition of "digital health" in Switzerland. Medicinal products (i.e. pharmaceuticals) and medical devices are subject to general regulation by the Federal Therapeutic Products Act (TPA). Detailed provisions are regulated in several ordinances. However, neither the TPA nor its ordinances contain a legal definition of the term "digital health".

The Federal Office of Public Health (FOPH), which by default acts as the competent authority for all public health matters, defines "digital health" applications and devices as products that use digital technology to accomplish their medical objectives. This includes telemedicine, telemonitoring, mobile applications and other similar applications, but not digital applications that solely assist healthcare professionals in their duties (such as controlling a device or reading and analysing data).

Swiss scholars partially use the term "digital health" as a collective term for "eHealth" (i.e., the use of ICT in healthcare) and "mHealth" (i.e., the use of mobile devices for patient care, such as smartphones or tablets).

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

Widespread use of telemedicine: Telemedicine solutions enjoy an extensive presence and are widely recognised in Switzerland. For instance, the largest medical telemedicine centre in Europe is managed by the Swiss digital health company *Medgate* in Basel, providing health insurance providers with the opportunity to serve as their policyholders' family physicians and/or gatekeepers. *SWICA*, a health insurance provider, among others, also provides telemedicine solutions, telemedical consultations and remote monitoring of vital parameters. Hence, an important part of the Swiss population has already been exposed to telemedicine.

Electronic Patient Record (EPR): In April 2017, the Federal Electronic Patient Record Act (EPRA) came into force. The purpose of the law is to ensure that, in the future, all patient records are maintained exclusively digitally and that all vital health documents (e.g., nursing and hospital reports, examination results, X-rays) are centrally stored and securely shareable among healthcare professionals. The EPRA and its implementing ordinances regulate the framework conditions for the introduction and dissemination of EPRs in Switzerland. Therefore, all hospitals are required to join a state-certified parent organisation that provides EPRs to private individuals. The use of an EPR is, nevertheless, voluntary for physicians (so far) and the general public. Consequently, implementation is currently advancing only incrementally, although there is great public interest and extensive media coverage. Therefore, and to assist the EPR in reaching a breakthrough, the EPRA is currently undergoing a revision to mandate all healthcare providers to use the EPR.

Wearables: Wearable technology monitoring personal health information in real time is fashionable and gaining users steadily. Since the COVID-19 pandemic, wearables have experienced additional expansion: the rise in interest in personal health monitoring and the adoption of remote work have both contributed to this development.

eMedication: "eMedication" refers to electronic systems that furnish data regarding the prescription, dispensation and processing of a patient's medication. This feature facilitates a multitude of operations, including the establishment of a medication schedule and a medication reminder system and is intended to increase process efficiency and patient safety. eMedication is a prevalent use case within the EPR framework. For instance, the EPR can be integrated with reminder functions that prompt patients to take their prescribed medications.

E-commerce of therapeutic products: In Switzerland, medicinal products do not necessarily have to be purchased in brick-and-mortar pharmacies or physicians' practices, but pharmacies may be permitted to engage in mail-order sales under certain conditions (Art. 27(2-4) TPA). Patients can therefore order medicinal products and certain medical devices online from a Swiss mail-order pharmacy and have them delivered at home. Over 30 mail-order pharmacies are active in Switzerland. However, following a Federal Supreme Court (FSC) ruling in September 2015, such pharmacies must request a prescription for both prescription-only and over-the-counter (OTC) medicinal products (FSC 142 II 80). Thus, prior consultation with a physician remains mandatory.

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

If a digital health technology classifies as a medical device, it must satisfy the criteria outlined in the TPA. However, this law establishes the fundamental principles governing the authorisation, monitoring and labelling of such products only in a general manner. Various other laws and ordinances at federal and cantonal level, the application of which rely on the intended area of use of digital health technology, detail these general requirements (see questions 2.1 *et seq.*). The large number of regulations to be observed make the regulatory requirements quite complex.

Furthermore, digital health technologies (such as the EPR) must comply with the provisions of the Swiss Federal Act on Data Protection (FADP). Especially in health matters, it should be noted that data relating to health, genetic and biometric data represent sensitive personal data (Art. 5(c)(2-4) FADP). To process such data, the explicit consent of the data subject is required (Art. 6(7)(a) FADP).

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

The Swiss market for digital health products and services is expanding rapidly. Diverse market size estimates exist, contingent upon the pertinent key performance indicators and the definition of digital health (see question 1.1). A study by McKinsey (see: https://www.mckinsey.com/ch/~/media/mckinsey/locations/europe%20and%20middle%20east/switzerland/our%20insights/digitization%20in%20healthcare/digitalisierung%20im%20gesundheitswesen%20%20die%2082mrdchance%20fr%20die%20schweiz%20de.pdf) assumes that the potential for utilising digital health in Switzerland amounts to around CHF 8.2 bio.

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

A considerable number of digital health-specialising companies are also engaged in other technology or health-related industries. Thus, there are no reliable data regarding what the largest digital health companies in Switzerland are. Global technology companies, including Apple, Google, Huawei, IBM, Samsung and Xiaomi, are also important players on the Swiss digital health market, as in other countries. Furthermore, several companies have established themselves in the field of telemedicine and e-commerce with therapeutic products (see question 1.2). In addition, more and more spin-offs, particularly from the two Swiss Federal Institutes of Technology in Zurich and Lausanne, are entering the market and often arise foreign investors' interest.

2 Regulatory

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

The core principles are outlined in the TPA which refers to medicinal products and medical devices as "Therapeutic Products". This also includes OTC medicinal products as well as supplements to medical devices. Due to the high export rate of such products to the European Union (EU), the Swiss legislator aims at a far-reaching conformity between Swiss and EU law.

Detailed provisions that are crucial in practice are regulated in several Ordinances, such as the Medical Devices Ordinance (MedDO). Since digital health technologies often qualify as medical devices, the requirements of the MedDO apply.

In addition, EU regulations pertaining to medical devices must be considered in conjunction with Swiss statutory provisions when it comes to digital health technologies that qualify as medical devices.

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

In addition to the TPA, the data protection requirements of the FADP (see question 1.3) and the requirements of the EPRA must be complied with as part of the implementation of the EPR (see question 1.2). Economic considerations, as well as cost control and affordability of digital health technology, are dealt with by the Federal Health Insurance Act (HIA). The cantonal health laws, of which there are 26, might also apply to digital health technology. Furthermore, other regulatory schemes, such as the Federal Product Safety Act, the Federal Foodstuff and Utility Articles Act, the Federal Cartel Act, the Federal Unfair Competition Act (UCA) and IP legislation may apply, depending on the circumstances.

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

Although a distinct national framework for "consumer healthcare devices" does not exist, several laws and regulations do apply to such items (see questions 2.1–2.2). Both the TPA and the MedDo explicitly state that software may qualify as a medical device if used for medical purposes (Art. 4(1)(b) TPA & Art. 3(1)(c) MedDO).

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

In Switzerland, the FOPH is by default the competent authority for all public health aspects, unless the cantonal authorities are in charge. In the area of Therapeutic Products, however, neither the FOPH nor the cantonal health authorities, but rather the Swiss Agency for Therapeutic Products (Swissmedic) acts as the competent Swiss regulatory and supervisory authority for medicinal products, including OTC products as well as medical devices (Arts 68, 69 & 82 TPA).

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

If digital health technologies or products do not comply with the provisions of the FADP, the cantonal criminal authorities may impose fines of up to CHF 250,000 on offenders in accordance with the penal provisions of chapter 8 FADP.

Digital health technologies or products that qualify as medical devices according to the TPA must comply with the regulations of the TPA and MedDO. Failure to comply with the regulations of the TPA or the MedDO may qualify as a criminal offence (Art. 86 and 87 TPA). For example, intentional introduction, export or use of non-compliant medical devices, or the use of medical devices without meeting the necessary technical and operational requirements, may be sanctioned by imprisonment of up to three years or a fine (Art. 86(1)(d) TPA).

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

Digital health solutions qualify as medical devices when they i) are intended to be used for human beings, and ii) serve to fulfil medical purposes, such as: a) diagnosis, prevention, monitoring, treatment or alleviation of diseases, injuries or disabilities; b) investigation, replacement or modification of the anatomy or of a physiological or pathological process or state; c) providing information by means of *in-vitro* examination of specimens derived from the human body, including organ, blood and tissue donations; and/or d) control or support of conception (Art. 3(1)(c) MedDO).

According to Swissmedic, software or apps are not considered medical devices if their sole purpose is related to fitness, well-being, nutrition (such as diets), hospital resource planning, reimbursement, management of doctors' visits, statistical analysis of clinical or epidemiological studies or registers, functioning as a diary, replacing paper-based health data, or serving as electronic reference works containing general non-personalised medical information. In September 2018, the Swiss Federal Administrative Tribunal (FAT) ruled in a landmark decision that an app designed to assess a woman's fertility by analysing her personal data meets the criteria to be classified as a medical device (FAT C-669/2016).

Thus, the term "medical device" is interpreted comprehensively. Hence, if software has a medical purpose, regardless of whether it has a proven medical effect, it may qualify as a medical device. In such a case, the software must adhere to the regulatory requirements that apply to medical devices.

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

See question 2.6 above.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care:** Telemedicine and virtual care are well established practices in Switzerland (see question 1.2 above). Except for specific cantonal regulations, telemedicine is not governed by any legal provision. However, telemedicine is permitted to a certain extent by the regulations that govern the professional obligations of physicians so long as it satisfies the obligations of the duty of care.
- **Robotics:** Depending on their intended use, robotics in healthcare may be classified as medical devices and, thus, subject to the relevant medical device regulations (especially TPA and MedDO).
- **Wearables, Mobile Apps, Virtual Assistants (e.g. Alexa):** Wearables, mobile apps and virtual assistants can collect and process personal health data; therefore, they must comply with the FADP. Additionally, if these devices qualify as medical devices due to their potential for medical applications (refer to question 2.6), they must comply with regulatory requirements applicable to medical devices.
- **Software as a Medical Device:** See question 2.6.
- **Clinical Decision Support Software:** See question 2.6.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions:** See questions 8.1–8.3.
- **IoT (Internet of Things) and Connected Devices:** Depending on their intended use, IoT and connected devices in healthcare may be classified as medical devices.
- **3D Printing/Bioprinting:** A fact sheet pertaining to the 3D printing of medical devices was released by Swissmedic. Swissmedic distinguishes in this regard between adaptable medical devices, mass-produced/patient-matched medical devices and custom-made devices (Art. 10 MedDO). Bioprinting technology may give rise to several regulatory and legal concerns pertaining to transplantation, gene technology, intellectual property and liability law.
- **Digital Therapeutics:** The term "digital therapeutics" encompasses a wide range of device-controlled therapy measures. Digital therapeutics, specifically, could potentially be impacted by both the regulatory requirements applicable to medical devices, as well as the data protection provisions outlined in the FADP.
- **Digital Diagnostics:** In Switzerland, like in the EU, the regulatory obligations pertaining to *in-vitro* diagnostics are regulated in a specific legal statute, which is the *In Vitro* Diagnostic Medical Devices Ordinance (IvDO). The latter sets forth that it applies *inter alia* to software or systems, whether used alone or in combination, intended by the manufacturer to be used *in-vitro* for the examination of specimens derived from the human body (Art. 3(1)(a) IvDO). Thus, digital diagnostics must meet the requirements of the IvDO. Depending on the manufacturer's intent, additional regulatory or legal requirements may apply (see also questions 2.1, 2.3 and 2.6).
- **Electronic Medical Record Management Solutions:** See question 1.2, Electronic Patient Record (EPR).
- **Big Data Analytics:** The regulatory approach on big data analytics is caught in a dilemma: while this technology raises significant concerns regarding data protection, the purpose of a medical treatment using big data may only be achieved through transparency. Furthermore, there may be situations where legal requirements are in direct opposition to one another.
- **Blockchain-based Healthcare Data Sharing Solutions:** Blockchain-based healthcare data sharing technology has the potential to streamline and increase the transparency of processes within the healthcare sector. However, Swiss healthcare regulatory authorities have not yet explicitly designated this technology as a target of regulation. Like other technologies, its legal or regulatory issues are thus contingent upon its specific objective. Accordingly, blockchain technologies that meet the criteria for medical devices might also be subject to their regulatory requirements.
- **Natural Language Processing:** Natural language processing (NLP), i.e. the computer-based capability to comprehend spoken and written language in a manner analogous to that of humans, is not generally classified as a medical device. NLP may, notwithstanding, be susceptible to regulatory requirements applicable to medical devices, provided that the manufacturers explicitly designate it for medical use. Moreover, adherence to data protection requirements may be necessary.

3.2 What are the key issues for digital platform providers?

In Cantons where digital platform providers are permitted to establish operations, the competent cantonal authority must issue an operating licence to such digital platform providers who wish to offer digital health services. This necessitates, *inter alia*, that the individual bearing the ultimate medical responsibility meets the prerequisites for ordinary physicians and that he/she directly and personally practises his/her profession. Nevertheless, delegation is permissible, specifically to practice assistants with sufficient training and oversight. The competent authority has the authority to exercise discretion in determining the personnel that is necessary for the digital health activity.

Furthermore, it is mandatory to uphold medical confidentiality and ensure the safeguarding of patient records to prevent unauthorised access. Depending on the location of the digital platform provider, other and/or additional key issues may arise. Thus, a case-by-case assessment is always necessary.

4 Data Use

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

The FADP governs the processing of personal data by private persons and federal bodies. Data processing activities of cantonal bodies are subject to the respective cantonal data protection legislation.

Personal data is defined as all information relating to an identified or identifiable natural person. Data of legal entities are not considered personal data. The FADP recognises so-called sensitive personal data for which stricter rules apply in certain aspects. Among others, health data is considered as sensitive personal data.

The FADP outlines several principles to be observed for the processing of personal data: processing must be lawful, conducted in good faith and proportionate. Personal data may only be used for the purposes for which it was collected, and those purposes must be made transparent to the data subjects. If personal data is no longer necessary for processing, it must be either destroyed or anonymised. Additionally, the processed personal data must be accurate and protected through appropriate technical and organisational measures. Finally, the law provides for several further obligations of data processors and for rights of the concerned data subjects.

It is important to note that in contrast to the EU GDPR, the FADP does not require a justification for every data processing activity by private persons. Therefore, data processing by private persons is in principle permitted unless explicitly prohibited by law.

In addition to the requirements stipulated by data protection legislation, healthcare professionals and their auxiliaries must adhere to professional confidentiality obligations, the breach of which is subject to criminal penalties.

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

The FADP distinguishes between private processors and federal bodies. Federal bodies are subject to more stringent requirements. Data processing by cantonal bodies is governed by the respective cantonal data protection legislation (see question 4.1). For example, healthcare professionals employed by cantonal hospitals are subject to the cantonal data protection legislation in question.

4.3 Which key regulatory requirements apply?

The general data processing principles apply (see question 4.1).

As stated, the FADP provides for several obligations of data processors. In particular, the data controller is required to fulfil information obligations when collecting personal data and when using automated individual decision-making processes. Further, the data controller must implement appropriate technical and organisational measures and ensure privacy-friendly settings. Subject to certain exceptions, a data controller is obliged to maintain a record of data processing activities. Also, under certain circumstances, the data controller must conduct data protection impact assessments and report breaches of data security. Additionally, the data controller must ensure the data subjects' rights.

4.4 Do the regulations define the scope of data use?

Personal data may only be processed for the specific purpose for which it was collected, and which purpose is transparent to the individuals whose data is being processed, unless there exist grounds for justification (e.g., the data subject's consent, an overriding private or public interest, or an explicit legal basis). Moreover, federal bodies may only process personal data if there is a statutory basis for doing so.

The FADP contains a list of circumstances in which the controller may have an overriding interest. This may be the case, among others, if the data controller processes personal data for non-personal purposes, such as research, planning or statistics, provided that the following requirements are satisfied: in such cases, the controller must (a) anonymise the data as soon as the processing purpose allows, or if anonymisation is not feasible or requires disproportionate effort, implement appropriate measures to prevent the identification of the data subject, (b) disclose data that includes sensitive personal data (such as health data) to third parties in a manner that renders the data subject unidentifiable, and if this is not possible, guarantee that the respective third parties process the data only for non-personal purposes, and (c) publish the results in a way that prevents the identification of the data subject.

4.5 What are the key contractual considerations?

The roles and responsibilities of the parties involved in data processing must be defined. In the case of the assignment of data processing to a third-party processor, it is necessary to establish a written data processing agreement (DPA). For joint controllers or independent controllers, a contractual agreement is not mandatorily required, unlike under the EU GDPR. However, it might be advantageous in many instances to define at least the basic responsibilities of each party regarding the respective data processing activities in writing.

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

Swiss law does not recognise any proprietary rights to personal data. However, the FADP grants data subjects the right to request and obtain information from the data controller on whether personal data relating to them is being processed. Also, the FADP provides for a right to data portability, subject to certain conditions.

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

The principle applies that only accurate data may be processed. Every data subject has the right to have inaccurate data corrected. Furthermore, the constitutional prohibition of discriminations also applies to the processing of personal data by federal bodies.

If a decision, which produces legal effects for a data subject or significantly affects a data subject, is based on an automated decision, the controller shall, upon request, provide the data subject with the opportunity to make a statement. The data subject may also request that the automated decision be reviewed by a natural person.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Currently, there are no specific legal or regulatory issues in Switzerland that pertain exclusively to generative AI companies. However, the Federal Council (i.e., the Swiss government) is examining regulatory approaches to AI, suggesting that there may be potential legal and regulatory challenges ahead.

5 Data Sharing

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

Under the FADP, it is crucial to distinguish between sharing personal data with a data processor and sharing it with a third party. Subject to statutory or contractual confidentiality obligations (such as, for example, medical professional secrecy), the sharing of personal data with a data processor is generally permitted, requiring only a DPA, assurance of the data processor's data security and informing data subjects about the categories of recipients receiving their personal data. If the data controller is bound by professional secrecy, generally the consent of the data subject is necessary.

If personal data is shared with third parties, stricter rules apply when it comes to the disclosure of special categories of personal data such as health data. The disclosure of such data by private processors requires either consent of the data subject, an overriding private or public interest or justification by law. Moreover, federal bodies may only disclose personal data (irrespective of whether sensitive or not) to third parties if there is a statutory basis for doing so, or if one of the statutory exceptions apply (see question 5.2).

Another critical consideration is the location where the shared data is processed. Data may only be transferred to countries that offer a level of protection which is deemed adequate from a Swiss law perspective. If personal data is disclosed to countries with data protection legislation of a lower standard, this is permissible only (a) with the data subject's consent, (b) under contractual agreements ensuring a level of data protection equivalent to Swiss standards, or (c) if any of the other statutory exceptions apply.

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

Here again, a distinction is made as to whether the data controller is a private person or a federal body.

For the processing of personal data (including disclosure) by a data controller who is a private person, see question 5.1.

Personal data may only be processed and disclosed to third parties by a federal body if there is a statutory basis or if one of the statutory exceptions apply (see question 4.4). Additionally, personal data may be disclosed in the context of public information if it pertains to a public duty and there is an overriding public interest. The data subjects may object to the disclosure of certain personal data by federal bodies if they can demonstrate a protected interest. However, the federal body may refuse the objection if there is a legal duty to process the data or if fulfilment of the respective body's tasks would otherwise be jeopardised.

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

When it comes to processing (including sharing) of health data, often the consent of the data subject is necessary (see questions 5.1 *et seq.*).

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

A project called "DigiSanté" aims to promote digitisation in the healthcare sector and facilitate the seamless exchange of health data. To achieve the digitisation, strategies are being developed in the period 2023–2024, which will be implemented in stages starting in 2025.

5.5 What are the key issues to consider with respect to federated models of healthcare data sharing?

The restrictions imposed by applicable Swiss data protection legislation apply.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

Digital health products regularly encompass both software and hardware elements. Patents for inventions are granted for new inventions applicable in industry. There exist no specific requirements for innovations in the digital health sector. However, exclusions from patentability cover, among others, methods for treatment by surgery or therapy and diagnostic methods practised on the human or animal body. Also excluded are computer programs as such, which are protected by copyright law (see question 6.2). Computer-implemented inventions, that solve a technical problem, are patentable.

6.2 What is the scope of copyright protection for digital health technologies?

The Swiss Federal Copyright Act (CopA) protects literary and artistic intellectual creations with individual character, irrespective of their value or purpose. Computer programs are explicitly defined as copyright-protected works. Digital health software can therefore be protected by copyright if the requirements are satisfied. It is worth mentioning that there are no specific formal requirements to obtain copyright protection in Switzerland. Copyrights are automatically established upon the creation of the respective work.

6.3 What is the scope of trade secret protection for digital health technologies?

Trade secrets are protected by provisions of the UCA and Criminal Law. Furthermore, the Swiss Code of Obligations stipulates that an employee may not utilise or disclose to others any facts to be kept secret, in particular manufacturing and business secrets, of which he or she becomes aware in the service of the employer. No specific provisions apply to digital health technologies.

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

Based on the laws described above, universities and colleges issue their own regulations concerning the utilisation of intellectual property in the context of university activities.

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

See questions 6.1–6.4.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

In principle, only individuals can be considered inventors. However, there is currently a debate in Switzerland regarding whether it is necessary for an inventor to be a natural person.

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

The Federal Act on the Promotion of Research and Innovation sets the legal basis for the promotion of research and of aspects of innovation in Switzerland. Together with the Federal Act on Funding and Coordination of the Swiss Higher Education Sector it defines the legal framework for scientific activities in Switzerland.

7 Commercial Agreements

7.1 What considerations should parties consider when dealing with collaborative improvements?

In practice, collaborative agreements are frequently entered into with universities, non-university research institutions and/or other industrial partners, in addition to internal research and development. As a starting point, the involved parties must determine whether they are interested in engaging in a research collaboration or in conducting contract research. Research cooperation agreements are frequently considerably more complex than mere research agreements due to various regulations governing the transfer of IP rights and their compensation.

Furthermore, to facilitate the commercial exploitation of the work results from such collaboration, it is essential that the respective party's IP rights be protected. Additionally, publication rights, marketing rights, regulatory responsibility and product liability ought to be contractually agreed upon.

7.2 What considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

In addition to the aforementioned aspects (see question 7.1) and the core healthcare regulatory schemes to be complied with (see questions 2.1 *et seq.*), particular attention should be given to ensuring that healthcare companies and their employees do not obtain undue benefits (Art. 55(1) TPA). The existence of an undue benefit must be determined on a case-by-case basis: benefits of modest value (up to CHF 300 annually) or in support of research, further education or training, contingent upon fulfilling specific criteria are, for example, not considered as "undue" (Art. 55(2)(a)(b) TPA).

7.3 What considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Federated learning (FL) in healthcare is the process of developing machine learning models over datasets that are distributed across various data centres (e.g., hospitals, clinical research labs and mobile devices) without exchanging the data itself. Companies dealing with agreements establishing such collaboration and data sharing must determine whether they are members of a FL consortium in which all other parties are trustworthy prior to proceeding (i.e., whether attempts to corrupt the model or intentionally extract sensitive information can be excluded). Furthermore, by definition, FL systems prevent the exchange of health-related data among participating institutions. However, through reverse engineering, the shared information may still indirectly expose private (highly sensitive) health data (i.e., leakage risk). Mitigation of the results from all these risks is required.

7.4 What considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

See questions 8.1–8.3 and 9.3.

8 Artificial Intelligence and Machine Learning

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

Machine learning is a sub-discipline of AI and describes an automated process (learning process) for the continuous enhancement of an application. Switzerland's digital health sector is significantly and dynamically influenced by machine learning, which is utilised in numerous research projects. Various domains are encompassed by the application of machine learning in digital health in Switzerland, which contributes to the enhancement of healthcare management, personalised medicine, treatment planning and diagnostics.

8.2 How is training data licensed?

In general, training data licensing ought not to be regarded differently from that of other types of information or data: if the training data constitutes an original work of literature or art, it may qualify as protected intellectual property under the CopA. Compilations of pure facts that possess individual characteristics may qualify as collected works (Art. 4 CopA) if they express individual characteristics. Thus, the training data are licensable in the same manner as any other copyright.

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

Intellectual property may only be created by a natural person

(i.e., a human) in accordance with Swiss copyright and patent law (Art. 6 CopA; Art. 3(1) Patent Act). As a result, advancements achieved through machine learning without explicit human intervention do not qualify as inventions protected under Swiss IP law. Nevertheless, dissenting views exist regarding the allocation of credit to the algorithm's owner (e.g., programmer) for works and inventions generated by algorithms. However, ownership cannot be acquired by an algorithm.

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

When procuring data for machine learning, it is crucial to consider significant commercial factors. These include, but are not limited to: i) establishing data ownership and IP rights; ii) defining financial terms, including fees and royalties; iii) addressing concerns related to data security and confidentiality; and iv) ensuring adherence to applicable laws and regulations, with particular emphasis on privacy. The application of machine learning in digital health technologies may potentially involve sensitive personal data, which raises several obligations under the FADP (see question 1.3).

9 Liability

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

Digital health solutions are subject to the general rules on contractual and tort law liability. In addition, the regulations governing therapeutic products stipulate that whoever manufactures or distributes therapeutic products (including but not limited to digital health solutions) is required to establish a reporting system and notify Swissmedic of adverse effects and incidents that i) are attributable to the therapeutic product itself, its use or improper instructions for use, or ii) may endanger the health of consumers, patients, third parties or animals (Art. 59(1) TPA). Furthermore, quality issues must be reported to Swissmedic (Art. 59(2)(3) TPA).

Violation of the reporting obligation primarily triggers criminal law consequences (Art. 87(1)(c) TPA). However, civil liability may also be triggered based on i) the Swiss Product Liability Act, which is based on the EU product liability directive, ii) contract law, and/or iii) tort law. In addition, a manufacturer may be held jointly and severally liable with any authorised representative in Switzerland of a person injured by digital health solution that qualifies as a defective medical device (Art. 47d(2) TPA).

A certificate of conformity (CoC) for a digital health solution that qualifies as a medical device may be an indicator that the product is not defective. However, such CoC does not exempt a manufacturer of the respective product from potential product liability claims.

9.2 What cross-border considerations are there?

Anyone who manufactures a digital health solution that qualifies as a medical device in Switzerland or who makes it available in Switzerland must report any adverse reactions suspected of being associated with this medical device to Swissmedic (Art. 66(1) MedDO). The response to such alerts is entirely up to Swissmedic's discretion. However, recalls in the US and/or the EU might encourage Swissmedic to consider similar administrative measures in Switzerland as well.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

When deploying generative AI in Swiss digital health solutions: i) compliance with the FADP; ii) assurance of transparency and informed consent from users; as well as iii) maintenance of accuracy and dependability via routine validation and documentation should take precedence. The incorporation of professional oversight and human intervention mechanisms are crucial in the healthcare decision-making processes. User agreements should incorporate unambiguous liability disclaimers and limitations, which underscore the technology's supportive nature. Furthermore, it is imperative to enforce strict cybersecurity protocols and to ensure ongoing training for healthcare professionals.

10 General

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

Cloud-based digital health services and their interfaces are usually hosted on external systems and sometimes even spread across several platforms. Therefore, when sharing data with other parties, key concerns are data security, namely the potential for unauthorised disclosure of personal data, the encryption and interoperability of data, the coordination of access and incident management, as well as data protection issues since cloud-based services for digital health store substantial quantities of very sensitive data (see question 1.3). In addition, it is necessary to ascertain whether the cloud-based services for digital health meet the criteria to be classified as a medical device (see questions 2.3 and 2.6).

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

Digital health products and/or services are subject to rigorous regulation and oversight. Therefore, regulatory and data protection considerations necessitate a thorough assessment of the intended business model and the intended products and/or services. A comprehensive compliance organisation considering the aforementioned factors, among others, should be established prior to the entry of non-healthcare companies into the digital healthcare market. Ultimately, it might be useful to evaluate whether Swiss compulsory health insurance may potentially cover the cost of the digital health products and/or services in question (see questions 2.2 and 10.6).

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

Key topics that should be considered before investing in digital healthcare ventures are the adherence to the constantly evolving data protection requirements, the necessity for comprehensive title-chain documentation, the ramifications of employee stock

option plans, and the identification and adherence to relevant healthcare regulatory schemes (see questions 2.1 *et seq.*).

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

High market-entry barriers, a complex procedure for registering new products or services for reimbursement by compulsory health insurance, and a complex regulatory framework are the key barriers holding back a wider use of digital health solutions in Switzerland. In addition, Switzerland is a federal state composed of 26 Cantons, each of which may have its own regulatory requirements on certain healthcare aspects. Moreover, the presence of four official languages in Switzerland may necessitate the employment of multilingual staff depending on the business model, products or services.

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

The Swiss Medical Association (FMH) is the professional association of all Swiss physicians and issues the FMH Code of Ethics and its appendices, which must be observed by all physicians. Given that the implementation of digital health solutions is essentially governed solely by law, the FMH's influence is limited to political advocacy work for its members' interests and those of patients to influence the respective legislative process.

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

The possibility of reimbursement by mandatory health insurance for the use, rental or sale of digital health solutions is governed by the HIA (see question 2.2). The FOFP is the competent authority in all matters relating to this. Several digital health solutions already exist in Switzerland, which are reimbursed by mandatory and/or private insurances. Nevertheless, the approaches utilised for this are highly dependent on the structure of this digital health solution. For instance, in most Cantons, the reimbursement application for a telemedicine solution can be submitted together with the request to carry out such an activity. Therefore, a case-by-case assessment is recommended.

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

In addition to the issues already mentioned, the evolution of Swiss regulatory (digital) health policy is to be seen in conjunction with the one of the EU. Given that Switzerland's largest trading partner is the EU, and that Switzerland exports a significant quantity of therapeutic products to EU Member States, the Swiss legislator strives for a comprehensive harmonisation of Swiss and EU legislation. Consequently, developments in Swiss digital health are also profoundly impacted by EU regulatory developments.

Tobias Meili is a partner in the Corporate and Commercial Law, Life Sciences and Health Law practice groups and on the IP and IT team. He advises clients in the areas of corporate and commercial law, corporate governance (including responsible business conduct matters), mergers and acquisitions and contract law. In addition, he provides support to our clients in the areas of data protection and IT law.
Due to his extensive experience as a private practitioner, as well as an inhouse counsel in senior roles (Accenture; Syngenta), he combines an authentic, pragmatic and solution-oriented approach to giving advice with solid legal expertise and skills as a negotiator.

Wenger Plattner
Aeschenvorstadt 55
4010 Basel
Switzerland

Tel: +41 61 279 70 00
Email: tobias.meili@wenger-plattner.ch
LinkedIn: www.linkedin.com/in/tobiasmeili

Carlo Conti is an of counsel in the Life Sciences and Health Law practice group. He advises institutions and organisations on questions of life sciences and health law and on matters of governmental and administrative law. He is a member of a number of boards of directors.
He has many years of professional experience and deep knowledge of all areas of life sciences and health law, as well as governmental and administrative law. He held executive positions in the pharmaceutical industry for more than 15 years. Carlo Conti then served as a member of the State Council for the Basel-Stadt Canton where he was head of the public health department. He was also president of the Swiss Conference of Public Health Ministers and chairman of the board of Swiss DRG AG and vice-chairman of the agency council of Swissmedic.

Wenger Plattner
Aeschenvorstadt 55
4010 Basel
Switzerland

Tel: + 41 61 279 70 00
Email: carlo.conti@wenger-plattner.ch
URL: www.wenger-plattner.ch/en/specialists/17/conti-carlo

Martina Braun is an of counsel and a member of the IP and IT team. She advises and represents companies, foundations and individuals on all aspects of IP law and IT, with a particular focus on copyright, trademarks and data protection. Her key area of expertise is advising on contract law. She specialises in particular in licensing and sponsorship agreements in the sports and entertainment sector. She also deals with various questions related to personality rights.
Martina Braun completed her doctoral thesis on copyright law and recently completed a CAS in international sports law.

Wenger Plattner
Seestrasse 39
P.O. Box, 8700 Küsnacht-Zürich
Switzerland

Tel: +41 43 222 38 00
Email: martina.braun@wenger-plattner.ch
LinkedIn: www.linkedin.com/in/martina-braun-81930b20

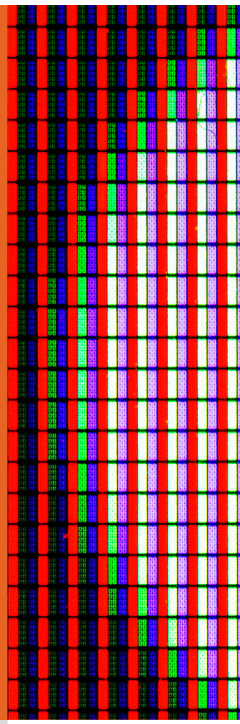
André S. Berne is an associate and mainly deals with commercial law and various regulatory matters. His primary practice areas consist of life sciences and health law, competition law and general contract law. Furthermore, he advises companies and organisations on matters pertaining to Swiss corporate and commercial law and administrative law, as well as EU law. He regularly publishes in his fields of expertise.

Wenger Plattner
Aeschenvorstadt 55
4010 Basel
Switzerland

Tel: +41 61 279 70 00
Email: andre.berne@wenger-plattner.ch
LinkedIn: www.linkedin.com/in/andr%C3%A9-s-berne-866b0199

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.



Digital Health 2024 features one introductory chapter, two expert analysis chapters and 22 Q&A jurisdiction chapters covering key issues, including:

- Digital Health
- Regulatory
- Digital Health Technologies
- Data Use
- Data Sharing
- Intellectual Property
- Commercial Agreements
- Artificial Intelligence and Machine Learning
- Liability

The International Comparative Legal Guides are published by: glg Global Legal Group