International Comparative Legal Guides

Digital Health 2026

A practical cross-border resource to inform legal minds

Seventh Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

glg Global Legal Group

iclg

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 subsectors in your jurisdiction?

Growing use of telemedicine: Telemedicine solutions, including hybrid care combining virtual and in-person consultations, enjoy an extensive presence, are widely recognised in Switzerland and continue to further emerge. For instance, one of the largest medical telemedicine centres 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. Based on this, further telemedicine models enter the sector. 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 with the aim that 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. However, its spread has been hindered due to the voluntary nature of its use and limited funding. To accelerate digitalisation, the Federal Council (i.e. the Swiss government) decided in November 2025 to replace the existing EPR model with a newly established electronic health dossier (E-HD), designed to consolidate individual health data and mandate its use by healthcare professionals, while granting patients complete control over access. The proposed Federal Electronic Health Dossier Act, already submitted to Parliament for deliberation, shall aim to delineate roles, competencies, and funds, designating central infrastructure administration to the federal government and implementation to the Cantons. Currently, the implementation of the E-HD is aimed for completion by 2030.

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 and are increasingly being integrated with EPRs, telemedicine platforms and AI/machine learning (ML)-driven analytics.

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 (and in future the E-HD) 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 upon request be granted the permission 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 currently 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 and online offerings continue to be strictly regulated.

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

The Swiss market for digital health products and services is expanding rapidly. Several market size estimates exist,

contingent upon the pertinent key performance indicators and the definition of digital health (see question 1.1). Accordingly, recent studies estimate that in 2024, the market size of digital health in Switzerland ranged between USD 1.23 billion (Statista: https://www.statista.com/outlook/hmo/digital-health/switzerland?srsltid=AfmBOooLuQsfQNhYTRbrfv65e-eNpDuHNO-VwVe2hxkDOZeMNILOUln0) and USD 3.79 billion (Databridge: https://www.databridgemarketresearch.com/nucleus/switzerland-digital-health-market?utm), with projections suggesting strong growth to USD 14.11 billion by 2032 (Databridge).

1.4 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 important players in 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.

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

In Switzerland, there are nearly 200 companies engaged in the digital health sector, demonstrating varying rates of growth. Since revenue information is typically not disclosed to the public, a subjective evaluation is necessary. Furthermore, the varying levels of maturity among the companies must be considered: start-ups and scale-ups typically experience rapid growth; however, their overall market significance often remains quite limited.

Some notable companies include: (i) Sleepiz, a manufacturer of medicinal products focused on sleep quality; (ii) Dacadoo, a provider of health scoring and lifestyle navigation solutions; (iii) Bluespace Ventures, which offers an integrated healthcare ecosystem platform in Switzerland under the Compassana trademark; (iv) OptiChroniX, whose solutions target modifiable risk factors for cognitive health in older adults; and (v) Holmusk, a European branch of a Singaporean company specialising in data analytics and digital therapies. RetinAI and Rhovica are also notable as recent market entrants reflecting strong financing rounds, team expansion, and market activity.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

In Switzerland, the FOPH is by default the competent authority for all public health aspects, unless the cantonal (health) 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 and 82 TPA).

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The core principles are outlined in the TPA, which refers to medicinal products and medical devices as "therapeutic products" (Art. 2(1)(a) TPA, *"Heilmittel"*). 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 this context, Swissmedic has issued specific guidance referring to guidelines and publications of the EMA, FDA, WHO, CIOMS, IMDRF and ICH, aiming to clarify how such technologies are to be assessed and regulated under Swiss law. 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.

Finally, if cantonal health authorities are competent in a certain matter (e.g. in case of authorisations for medical activities), the relevant cantonal regulations apply.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

If digital health technologies or products do not comply with the provisions of the Swiss Data Protection Act (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 (Arts 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).

2.4 What regulations (and corresponding authority(ies)) 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, acting as the competent Swiss regulatory and supervisory authority for medical devices, 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 vital signs 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, including the registration obligations in the Swiss medical devices database (see question 2.5 below).

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Current Swiss legislation does not encompass AI/ML-powered digital health devices or software solutions. Consequently, the overarching principles are applicable to these products; if classified as a medical device, the relevant regulations for clinical use must be adhered to (see question 2.4 above). It is important to note that medical devices, in contrast to medicinal products (for the differentiation, see question 1.1) are not governed by a state authorisation process; instead, they adhere to the principle of self-regulation, wherein conformity is demonstrated through a declaration from the manufacturer, typically validated by a conformity assessment body. Whoever manufactures or distributes medical devices is required to establish a reporting system and notify Swissmedic of adverse effects and incidents (Art. 59 TPA), whereupon Swissmedic can take the necessary action in a particular instance, including recalls (Art. 66(2) TPA).

As of 1 July 2026, registration of all medical devices, systems and treatment units placed on the Swiss market will be mandatory in the Swiss medical devices database (swissdamed), which is based on the EU database EUDAMED. Voluntary registration has been possible since August 2025.

Nevertheless, comprehensive regulation of AI/ML in Switzerland is not anticipated, as the Federal Council declared in February 2025 that sector-specific AI regulations will be implemented into existing legislation, rather than a general horizontal AI legislation.

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

See question 2.2 above.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

See question 2.6 above.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Digital health products are typically classified as medical devices (see question 2.4 above) as regulated by the TPA and the MedDO. Due to their nature as federal laws, the Cantons lack legislative authority but play a role in the law's enforcement: on the one hand, Swissmedic operates with the Cantons' involvement (Art. 68(1) TPA), as the Cantons have the right to nominate members to the Swissmedic Agency Council (Art. 72(2) TPA); on the other hand, the Cantons are tasked with regulating points of sale, particularly medical practitioners, and issuing retail trade licences for the sale of therapeutic products, including digital health products, in establishments such as pharmacies and drugstores, as well as overseeing the related inspection system.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

See question 2.6 above.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Telemedicine and virtual healthcare 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**
  Wearables collect and process vital signs (heartrate, blood pressure, etc.), which from a legal perspective qualify as personal data. Accordingly, the collection and processing of such data 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.
- **Virtual Assistants (e.g. Alexa)**
  See question 3.1, Wearables.
- **Mobile Apps**
  See question 3.1, Wearables.
- **Software as a Medical Device**
  See questions 2.2 and 2.6.

- **Clinical Decision Support Software**
  See question 2.6.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  See questions 2.5, 8.1 and 8.2.
- **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 and the data protection provisions outlined in the FADP. See also question 2.5.
- **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: whilst this technology raises significant data protection concerns, the purpose of a medical treatment using big data can only be achieved through transparency. Furthermore, there may be situations where legal requirements are in direct contradiction to each other.
- **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 manufacturer explicitly designates it for medical use. Moreover, data protection requirements must be observed.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

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 power 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, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

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 sanctions.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As outlined above, the FADP governs the processing of personal data by private persons and federal bodies, whilst data processing activities of cantonal bodies are subject to the respective cantonal data protection legislation (see question 4.1). This also applies to personal health data.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The FADP distinguishes between private data 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. Further, the FADP recognises so-called sensitive personal data (e.g., health data), for which stricter rules apply in certain aspects (see question 4.1).

4.4 How do the regulations define the scope of personal health 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 data controller must (a) anonymise the personal 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 personal 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 personal data only for non-personal purposes, and (c) publish the results in a way that prevents the identification of the data subject.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

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 data processor, it is necessary to establish a written data processing agreement (DPA). A DPA should in particular set forth the rights and obligations of the parties, including the controlling rights of the data controller. Further, the data processor must undertake to implement and maintain adequate technical and organisational measures, which must be described in detail. For joint or independent data controllers, a contractual agreement is not mandatorily required, unlike under EU GDPR. However, it might nevertheless 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 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The principle applies that only accurate personal data may be processed. Every data subject has the right to have inaccurate personal data corrected. Furthermore, the constitutional prohibition of discrimination 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 automated decision-making, the data 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-making be reviewed by a natural person.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The FADP and cantonal data protection laws set forth the principles governing the collection and use of personal health data. The Swiss Federal Health Insurance Act (HIA) imposes strict limits on how insurers can use health data, ensuring it is only processed for specific purposes, namely the provision of insurance services. In November 2025, a project for an E-HD with central data processing to be implemented by 2030 has been presented (see question 1.2, EPR). More generally, the eHealth Switzerland initiative aims at facilitating the secure exchange and management of health information, whilst giving patients control over who accesses their data. Finally, the Swiss Medical Association (FMH) has issued several guidelines directed at healthcare professionals, which outline the applicable data protection principles, and emphasise patient confidentiality and the necessity of informed consent.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

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 confidentiality obligations), 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

confidentiality obligations, 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. Personal data may only be transferred to countries that afford 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 comparatively 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, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

See questions 5.1 and 5.3.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), 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 questions 4.4 and 5.1). 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 disregard 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.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

As laid out, the FADP imposes requirements on the collection, processing and sharing of personal health data (see question 5.1). The HIA regulates the exchange of data between those responsible for implementing, monitoring or supervising the implementation of said act (see also question 4.7). The eHealth Strategy, overseen by the FOPH, aims at establishing an interoperable digital healthcare ecosystem that promotes secure and efficient data exchange. In particular, the EPRA shall be revised comprehensively and facilitate secure data sharing across healthcare providers, with patient consent as a central principle (see question 1.2, EPR). Further, see also question 5.5.

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

Federated models of healthcare data sharing must navigate complex regulatory considerations and technical challenges. Interoperability standards are the basic prerequisite to enable seamless data exchange across decentralised systems. Security measures, including encryption, access controls and audit trails, are essential to protect sensitive health information. Contractual frameworks, such as DPAs, clarify responsibilities and liabilities, particularly in the event of data breaches. To promote the digital transformation in the healthcare sector, the Federal Council has launched the so-called "*Digisanté* Project", being implemented since 2024 onwards. This project aims at creating a nationwide digital healthcare system for the secure and seamless exchange of data, including a medical register (see question 1.2, EPR above). All stakeholders shall obtain access to the relevant health information in accordance with data protection legislation. Data entry shall be performed in a uniform and standardised system, the "Swiss Health Data Space", which shall improve the quality and safety of the entire treatment chain, from prevention to diagnostics, treatment and care. Secure access to standardised data shall also help to promote academic and industrial medical research and the professional and political management of the healthcare system.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact 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. No specific requirements exist 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). However, computer-implemented inventions, which solve a technical problem, are patentable.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The Swiss Federal Copyright Act (CopA) protects literary and artistic intellectual creations of individual character, irrespective of their value or purpose. Computer programs are explicitly recognised as copyright-protected works. Digital health software can therefore be protected by copyright if the requirements are met. 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 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are protected by provisions of the Federal Unfair Competition Act and the Swiss Criminal Code. 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 How do intellectual property laws in your jurisdiction impact 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?

No, in principle only individuals can be named as inventors. Whilst a device or AI may contribute to the invention process, only a human being may be named as inventor. Nevertheless, there is an ongoing debate in Switzerland regarding whether it is necessary for an inventor to be a natural person. A notable case regards the AI system DABUS: on 26 June 2025, the Swiss Federal Administrative Court ruled that when applying for a patent, a natural person must be named as the inventor (FAT B-2532/2025).

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

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.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Several key precedents in the realm of intellectual property rights concern digital health innovation. The Swiss Federal Patent Court has issued several rulings clarifying the scope of patentability for digital health technologies. Finally, an example relating to trademark law regards the rejection of the registration of the trademark "ID NOW" for medical devices by the Federal Administrative Court, based on the grounds that said sign was considered descriptive of the respective goods (FAT B-1776/2023). The ruling clarifies the high standards of distinctiveness required for trademarks and reiterates that trademarks must not give rise to misleading expectations as to the functionality or performance of the respective products, which also applies in the area of medical devices. See also question 6.6.

7 Commercial Agreements

7.1 What contractual and strategic 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 activities. As a starting point, the involved parties need to 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 intellectual property rights be protected. Additionally, publication rights, marketing rights, regulatory responsibility and product liability ought to be contractually agreed upon.

7.2 What contractual and strategic 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 question 2.1 *et seq.*), particular attention must 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 contractual and strategic 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 ML 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 contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

See questions 8.3, 8.4 and 9.3.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

See questions 2.5, 2.6 and 2.8.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

See questions 2.4 and 2.8.

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

Intellectual property may only be created by a natural person (i.e., a human being) in accordance with Swiss copyright and patent law (Art. 6 CopA; Art. 3(1) Patent Act). As a result, advancements achieved through ML without explicit human intervention do not qualify as inventions protected under Swiss intellectual property 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 or through an algorithm.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

When procuring data for ML, it is crucial to consider significant commercial factors. These include, but are not limited to: (i) establishing data ownership and intellectual property 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 ML in digital health technologies may potentially involve sensitive personal data, which raises several obligations under the FADP (see question 1.3).

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

As far as can be seen, no established practice has yet emerged among regulatory bodies overseeing AI/ML technologies to differentiate between standard AI and generative AI technologies and products.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction?

Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

See question 8.5 above.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

If AI/ML models are trained on data for which the developer lacks the appropriate data rights, the developer may face legal consequences under the FADP (see question 4.1 *et seq.*). Any person may request from a data controller information about the processing of personal data concerning him or her, which he or she has provided to the data controller, in a commonly used electronic format, if (i) the controller processes the data by automated means, and (ii) the data are processed with the consent of the data subject or in direct connection with the conclusion or performance of a contract between the controller and the data subject (Art. 28(1) FADP).

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).

Violations of the reporting obligations primarily trigger criminal law consequences (Art. 87(1)(c) TPA). However, civil liability may also apply 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 a 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 may 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 AI/ML (including standard AI and 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.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Swiss civil law may hold entities accountable under contractual and non-contractual theories for harm caused by negligent or improper use of AI/ML models, including medical malpractice claims if AI decisions lead to medical errors or harm. Furthermore, under the FADP, misuse can lead to violations of privacy rights and data protection, especially if sensitive health data is processed without consent or adequate safeguards. Additional liability provisions may apply.

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 4.1). 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 question 2.3).

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 respective company's business model and its intended use of products and/or services. A comprehensive compliance organisation considering, among others, the aforementioned factors should be established prior to the entry of non-healthcare companies into the digital healthcare market. Ultimately, we recommend evaluating 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 in general are the key barriers for new digital health solutions in Switzerland. In addition, Switzerland is a federal state comprising 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 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 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe 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 and its ordinances. 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 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

In Switzerland, certain due diligence gaps within the healthcare ecosystem for evaluating digital health solutions may create challenges for stakeholders in maintaining safety, compliance and ethical standards. Identified gaps encompass: (i) data governance, characterised by insufficient clarity regarding data ownership, consent management and compliance with data protection requirements, especially for sensitive health data; (ii) algorithm transparency, marked by limited understanding of AI/ML models' decision-making processes, which may give rise to liability and unfair competition risks; (iii) regulatory oversight, with the absence of specific regulations for AI/ML in healthcare (see question 2.5), resulting in uncertainties related to compliance with medical device regulations and standards for safety and efficacy; (iv) interoperability, emphasising challenges in ensuring secure and effective integration of digital health solutions with existing healthcare systems and standards; and (v) clinical validation, indicated by the lack of robust frameworks for the ethical evaluation and clinical validation of AI/ML models in medical contexts, potentially undermining trust and effectiveness.

10.8 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 mentioned above, the evolution of Swiss regulatory (digital) health policy is to be seen in conjunction with similar EU policy. 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 influenced by EU regulatory developments.

A recent development further reinforcing this alignment is Switzerland's association with key EU programmes, such as Horizon Europe and the Digital Europe Programme, retroactively applied from early 2025. This participation strengthens opportunities for Swiss researchers and innovators in digital health to collaborate with EU partners, secure funding, and engage in EU-wide initiatives, thus fostering innovation and regulatory alignment.

Tobias Meili is a Partner in the practice groups Governance & Compliance, Life Sciences & Health Law, and M&A/Corporate. He advises clients, particularly in the life sciences sector, on commercial and corporate law, especially on corporate governance (including corporate responsibility issues), restructuring, M&A, and contract and technology law. His area of activity also includes internal investigations as an examiner or investigator appointed by FINMA or companies.
Due to his many years of experience in a leading position in the legal department of a formerly SMI-listed multinational corporation and an international consulting and technology company, Tobias Meili is familiar with the structures, processes, and challenges of large companies. In his legal practice, he combines an authentic, pragmatic, and solution-oriented advisory approach with solid legal expertise and negotiation skills.

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 Of Counsel in the field of Life Sciences and Health Law. He advises institutions and organisations on issues related to life sciences and health law, as well as on constitutional and administrative law matters. He is president or member of various boards of directors.
He has many years of professional experience and profound knowledge in all areas of life sciences and health law, as well as in constitutional and administrative law. For more than 15 years, he held executive positions in the pharmaceutical industry. Subsequently, Carlo Conti became a member of the state government in Basel-Stadt and 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, as well as vice president of the board of Swissmedic (the Swiss Agency for Therapeutic Products).

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/team/conti-carlo

Martina Braun is a Partner and a member of the practice groups IP, IT & Data Protection as well as Sports Law. She advises national and international companies and start-ups as well as associations, foundations and private individuals comprehensively on contractual matters and represents them in complex negotiations.
Her focus lies in copyright, trademark, personality and data protection law. She has extensive experience in the commercialisation of intangible assets and specialises particularly in licensing and sponsorship agreements in the sports and entertainment industries.
Martina Braun has written a dissertation on copyright law and completed a CAS in international sports law. She also publishes regularly on IP law and is active in professional organisations.

Wenger Plattner
Seestrasse 39, 8700 Küsnacht-Zurich
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 a Senior Associate and primarily handles commercial law and various regulatory issues. His main areas of focus include life sciences law, health law, competition law, data protection law, and general contract law.
He also advises companies and organisations on Swiss commercial and corporate law, administrative law, and EU law, and represents them before courts and authorities in German and French.
In addition to his advisory and litigation activities, André S. Berne prepares expert opinions in his areas of specialisation. He regularly publishes and lectures in these fields.

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

iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 59 practice areas.

Digital Health 2026 features an introductory chapter, four expert analysis chapters and 18 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