PANORAMIC

DIGITAL HEALTH

Switzerland

LEXOLOGY

Digital Health

Contributing Editor
Abeba Habtemariam
Arnold & Porter

Generated on: April 10, 2025

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2025 Law Business Research

Explore on **Lexology**

Contents

Digital Health

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations
Investment climate
Recent deals
Due diligence
Financing and government support

LEGAL AND REGULATORY FRAMEWORK

Legislation
Regulatory and enforcement bodies
Licensing and authorisation
Soft law and guidance
Liability regimes

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'
Data protection law
Anonymised health data
Enforcement
Cybersecurity
Best practices and practical tips

INTELLECTUAL PROPERTY

Patentability and inventorship
Patent prosecution
Other IP rights
Licensing
Enforcement

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing
e-Commerce

PAYMENT AND REIMBURSEMENT

Coverage

UPDATES AND TRENDS

Recent developments

Contributors

Switzerland

Walder Wyss Ltd

walderwyss attorneys at law

Anne-Catherine Cardinaux anne.cardinaux@walderwyss.com

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

In Switzerland's local digital health market, key players encompass various entities contributing to innovation and development. These players include:

- Academic institutions: for example, the Swiss Federal Institute in Lausanne (EPFL) and the Federal Institute of technology in Zurich (ETH Zurich) are prominent in driving innovation. They foster a conducive environment for research and development, aiding in the emergence of startups through technology transfer initiatives.
- Startup incubators: Institutions such as the EPFL Innovation Park in Lausanne, the Bio-Technopark in Schlieren or the Digital Health Center in Bülach provide essential support and resources to digital health startups, facilitating their growth and development, and help connect startups with investors and other key players within the venture ecosystem.
- Government-driven programmes: Initiatives such as InnoSuisse play a vital role in providing support to companies in the digital health sector, particularly in their early stages.
- Investors: Switzerland boasts an active investor scene comprising traditional venture capital (pre-seed, seed and post-seed stage, mostly by 'angels', family offices, traditional venture capital funds and the like), private equity funds and large industrial companies. These investors provide crucial financial backing, fostering innovation and growth in the digital health market. Corporate venture investors contribute by sharing know-how and granting access to industrial networks as well.
- Regulatory agencies: Regulatory agencies such as Swissmedic play a crucial role in ensuring the safety and efficacy of digital health products and services in Switzerland.

Prominent areas of innovation in the Swiss digital health market include telemedicine and remote patient monitoring, healthcare data analytics and artificial intelligence (AI), digital therapeutic and wearable health technologies. The Digital Health Center Bülach has compiled a helpful list of podcasts for those wishing to stay up to date with the digitalisation of Swiss healthcare.

Law stated - 2 März 2025

Investment climate

How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

The investment climate for digital health technologies in Switzerland is generally positive, supported by various factors that attract investors. These factors include a strong innovation ecosystem, government initiatives supporting digital health startups and research projects, and access to a diverse range of funding sourcing in a stable economy.

The SIX Swiss Exchange is a prominent stock exchange in Europe, leading in the life science sector. About 35 per cent of the capital of European life sciences companies is traded on the SIX Swiss Exchange, highlighting Switzerland's long-standing connection to this field. Switzerland has the highest per capita concentration of bio and medtech companies globally, demonstrating its strong ecosystem for innovation and growth in these industries.

According to a PwC analysis, although global M&A deal volumes experienced a downturn in Q3 2024, Swiss Health Industries saw a more moderate decline of 17 per cent compared to Q3 2023. This relative resilience is due to the market's insulation from broader macroeconomic challenges and consistently strong buyer interest.

However, despite the favourable investment climate, there are also a few challenges in the Swiss digital health sector. Navigating the regulatory landscape can be complex and time-consuming, particularly for startups and early-stage companies. Labour in Switzerland is expensive and compliance with data protection regulations can also present challenges for companies developing digital health technologies (even if less stringent compared to EU regulations).

Law stated - 2 März 2025

Recent deals

What are the most notable recent deals in the digital health sector in your jurisdiction?

The notable recent deals in the digital health sector include:

- In Q1 of 2024, Arga Medtech , developer of a cardiac ablation system for treating cardiac arrhythmias, announced the closure of a €54 million oversubscribed Series B funding. The round was led by the existing investors, Advent Life Sciences (UK) and Earlybird Health (Germany), as well as new investor Gilde Healthcare (the Netherlands) and an undisclosed strategic investor.
- In Q1 of 2023, NanoFlex Robotics, a pioneer in magnetically controlled medical soft robotics, secured over US$12 million in Series A funding. The financing round was led by Ascend Capital Partners and supported by European-based family offices, including Kinled Holding Ltd and Mountain Labs Ltd.
- In Q4 of 2022, Swiss-based medical technology company MedAlliance announced having entered into an agreement with Cordis, a global developer and manufacturer of interventional cardiovascular technologies, for an acquisition.
- In Q1 of 2022, MindMaze, a digital neurotherapeutic platform, secured a US$105 million financing round. The investors were Concord Health Partners and others.
- In Q1 of 2022, DistalMotion, the medical technology company behind the Dexter robotic system, secured a US$ 90 million Series E financing led by Revival Healthcare Capital, with participation from existing and new investors.
- In Q1 of 2022, Sonova Holding, a Swiss-based leading provider of hearing care solutions, has successfully completed the acquisition of Alpaca Audiology LLC, a large independent networks of audiological care clinics in the US.
-

In Q3 of 2021, SOPHiA Genetics, a Swiss-based creator of a global data pooling and knowledge sharing platform, announced the closing of a US$234 million initial public offering and US$20 million private placement.

Law stated - 2 März 2025

Due diligence

What due diligence issues should investors address before acquiring a stake in digital health ventures?

Before acquiring a stake in digital health ventures, investors should conduct due diligence on several key areas, industry-related and general:

- Regulatory compliance (ensuring adherence to healthcare and data protection regulations).
- Intellectual property portfolio (assessing the company's patents, trademarks, trade secrets and other IP-related topics).
- Clinical validation and efficacy (evaluating scientific evidence supporting the effectiveness of the product) and the existence of relevant approvals and/or permits for commercialisation.
- Market demand and competition (assessing demand, target demographics and competitive landscape).
- Technology infrastructure and security (reviewing data security measures and technology protocols).
- Business model and revenue generation (understanding how the company plans to generate revenues and reach profitability).
- Team expertise and experience (evaluating the leadership team's track record in the industry).
- Financial viability and projections (reviewing financial statements, business plan, fundraising history and future cash flow planning).
- Customer adoption and retention (examining adoption rates, satisfaction levels and churn rates).
- Partnerships and collaborations (assessing existing and potential partnerships for growth).
- General legal due diligence topics (including assessment of company and share structure, ownership over shares and assets, validity of material agreements, compliance with laws and regulations, insurance coverage, tax, labour, pension and disputes or litigation).

Law stated - 2 März 2025

Financing and government support

What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

While digital health ventures commonly employ financing structures similar to those used across various sectors, given the typical absence of robust valuation data for early-stage digital health companies, debt securities (instead of shares), typically in the form of convertible notes, are used first to avoid any under-pricing. Such convertible notes convert into shares as part of a future qualified equity financing round, typically at a certain discount to the cash price to be paid by equity investors (said discount in this industry usually being between 10 and 30 per cent, occasionally in addition to any interest payments, typically being between 2 and 10 per cent). Importantly, such debt is 'subordinated' under Swiss law and thus cannot be repaid in cash if the company has no distributable equity. As the company progresses and attains a solid valuation, traditional equity financing rounds become prevalent. For such rounds, customary features are used for digital health venture companies, such as preferred shares (the financial preference often being a 1 × non-participating liquidation preference, unless in financial distress where investors usually ask for more aggressive terms), board seat, anti-dilution protection (Swiss venture standard being weighted average and not full ratchet!), drag-along and similar rights.

While not specifically targeted at the digital health sector, Swiss federal and cantonal authorities have implemented initiatives to bolster innovation and support early-stage companies. Notable among these is InnoSuisse, the Swiss Innovation Agency. An example on a cantonal level is the Zurich University Hospital's (USZ) Health Innovation Hub. Although these initiatives aren't exclusive to digital health, they aim to foster innovation and R&D, thereby indirectly benefiting ventures in the digital health space.

Law stated - 2 März 2025

LEGAL AND REGULATORY FRAMEWORK

Legislation

What principal legislation governs the digital health sector in your jurisdiction?

There is no bespoke digital health legislation in Switzerland. Instead, health-related information technologies are typically categorised within each regulatory framework according to the objectives of the respective regulations.

Swiss laws seldom address specific technologies directly. Depending on their functionalities, attributes and assertions, digital health products and services may fall under various regulatory considerations, including:

- regulations pertaining to medical devices (Therapeutic Products Act (TPA); Medical Devices Ordinance (MedDO); Ordinance on In Vitro Diagnostic Medical Devices (IvDO);
- obligations regarding data protection and professional confidentiality (Federal Act on Data Protection (FADP); Data Protection Ordinance (DPO); specific laws, stemming from the Federal Constitution's mandate to protect health, including the

Human Research Act (HRA); articles 321 and 321-bis of theCriminal Code address professional secrecy cantonal laws);

- liability regulations (product liability);
- professional practice and licensing requirements (federal and cantonal laws);
- restrictions on advertising (federal and cantonal laws);
- rules regarding the provision of benefits to healthcare professionals (HCPs), healthcare organisations (HCOs) or patient organisations (TPA; Health Insurance Act (KVG));
- telecommunications regulations; and
- public procurement provisions.

Law stated - 2 März 2025

Regulatory and enforcement bodies

Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

Switzerland operates as a federal state comprising 26 cantons, with one central federal government. The federal government holds responsibility for various sectors including health insurance, medicinal products, medical devices and public health. Conversely, the cantons oversee hospital planning, licensing of service providers and possess significant autonomy in organising their respective healthcare systems. Typically, cantonal health authorities are tasked with enforcing both local and national health laws. In this system, various regulatory and enforcement bodies have jurisdiction over the digital health sector:

At the federal level:

- Swissmedic: This authority is responsible for the authorisation and supervision of therapeutic products. Swissmedic's responsibilities are defined in the Therapeutic Products Act (TPA) and multiple ordinances. Swissmedic oversees clinical trials for medical devices and conducts market surveillance (quality defects, incidents, illegal trade).
- Federal Office of Public Health (FOPH): The key health-related requirements are anchored in the Federal Constitution. Based on these principles, the FOPH oversees more than 20 laws and numerous ordinances. Accordingly, its responsibilities cover a wide spectrum, including social health and accident insurance. Inter alia, the FOPH handles issues related to reimbursement by compulsory health insurance for medical devices used in therapeutic settings. The FOPH also enforces integrity and transparency provisions.
- Federal Data Protection and Information Commissioner (FDPIC): Responsible for supervising compliance with federal data protection legislation, this office oversees data processing by federal bodies (ie, the federal administration, federally affiliated companies, such as SBB, Swiss Post and Swisscom) and private parties. The oversight of data processing by municipal and cantonal authorities falls under the

jurisdiction of the data protection supervisory bodies of the respective cantons or municipalities.

At the cantonal level:

- Cantonal health authorities: These entities oversee medical professional practice and enforce professional licensing requirements. They are responsible for implementing and enforcing both cantonal and national health laws.
- Regional ethics committees: Alongside Swissmedic, these committees authorise certain categories of human clinical trials with medical devices under the Swiss Clinical Trials Ordinance.
- Cantonal data protection authorities: Entities designated as 'public bodies' at the cantonal level are governed by cantonal data protection laws and are monitored by the respective cantonal data protection authorities. Many healthcare organisations fall into the category of 'public bodies.'

Law stated - 2 März 2025

Licensing and authorisation

What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

The licensing and authorisation requirements depend on the type of the digital health product or service.

Digital Health Products

Digital health applications are of great interest. Swiss law currently lacks an official legal definition for them. The Federal Office of Public Health (FOPH) defines 'digital health applications' in its Fact Sheet on the Reimbursement of Digital Health Applications under Mandatory Health Insurance as products that are used (1) to promote health, (2) to support and inform patients or (3) for medical purposes and that utilise digital technologies. A digital health application can be software, an app, a mobile device (eg, sensors for recording body parameters and software for digital evaluation or transmission) or a combination of these. It can also be used in combination with a non-digital physical product (ie, bathroom scales) and can be intended for self-use by patients or healthy individuals or for use by specialised staff. Artificial intelligence can also be used.

- Digital health applications with a health-promoting purpose are used by largely healthy people, particularly in the areas of general health, fitness, well-being or self-development. They can monitor body parameters (eg, pulse, sleep rhythm, etc) or personalise recommendations for healthy behaviour (eg, nutrition tips, meditation, relaxation tips, etc). They are not specifically intended to prevent, diagnose, monitor or treat an illness or its consequences. They are sometimes also referred to as 'lifestyle' or 'wellness' applications. This category includes fitness watches or nutrition, exercise and wellness apps. As a rule, these applications are not subject to Swiss medical device law.

- Digital health applications for patient support and information are used to support patients with a specific disease or symptoms in their everyday lives by providing general, disease-related information and behavioural recommendations (improving understanding of the disease, self-management skills). These can also include the option of digitally documenting symptoms and disease progression (eg, patient diary) or include exercise videos, quizzes or interactive learning with feedback. Depending on the range of functions, these digital health applications are not necessarily subject to Swiss medical device law. However, the documentation of symptom recording can also provide helpful information for healthcare professionals (eg, blood pressure diary, bladder diary, food diary, etc.). This part of the digital application can therefore also be a monitoring with a medical purpose and thus define as a digital health application with a medical purpose (see below).
- Digital health applications with a medical purpose are used for the early detection, prevention, diagnosis, monitoring, prognosis, treatment or alleviation and care of diseases or their consequences or are used during maternity. Based on digitally documented data, medical analyses can be made and individual recommendations for action can be made. Examples of this category include app-based therapy for diagnosed diseases, telemedical monitoring of people with chronic diseases and intelligent diagnostic devices with decision support systems for specialists in the treatment of diseases. They may be covered under mandatory health insurance. These digital health applications are placed on the market as medical devices and in this case must fulfil the requirements of Swiss medical device law (Therapeutic Products Act (TPA); Medical Devices Ordinance (MedDO)).

There is no official authorisation process for medical devices. Switzerland aligns with the European Union's (EU) compliance assessment and certification system for these devices . Evaluation of adherence to globally accepted standards is carried out by private organisations. Medical devices are classified into different risk categories, each requiring specific assessment procedures. CE-marked medical devices may in principle be placed on the market in Switzerland. They may be imported into Switzerland subject to the legal requirements in force, and may be sold and distributed here. Because the agreement on mutual recognition of conformity assessments (MRA) between Switzerland and the EU has not been updated, registration of economic operators (CHRN) and of medical devices is carried out directly by Swissmedic. Manufacturers are subject not only to the device registration requirements stated in the MedDO but also to the obligations and modalities associated with articles 27, 29 and Annex VI of the (EU) 2017/745 (MDR). The aforementioned articles in the MedDO enter into force on 1 July 2026. Swissmedic published an information sheet (current version dated 1 January 2025) outlining the roles and obligations of the Swiss authorised representative, the importer and the distributor.

Digital Health Services

Healthcare professionals engaged in delivering digital health services may need professional licences from relevant health authorities, based on the nature of the service provided. On a federal level, the Medical Professions Act (MedBG), the Health Professions Act (GesBG) and the Psychology Professions Act (PsyG) delegate the issuance of professional practice permits and the supervision of compliance with professional duties of specialists who practise their profession independently to the cantons.

The practice of these professions in Switzerland requires authorisation even when it is conducted using digital technologies (the same goes for professions solely regulated on a cantonal level). Of course, not every activity performed by these professionals is to be considered a practice requiring professional license (eg, a psychotherapist participating in online group meetings alongside coaches from other disciplines as part of a programme solely for patient support and information). This distinction can be challenging in practice and requires careful consideration.

When healthcare services are provided across borders, a key question is when Swiss authorities consider a healthcare profession to be practised in Switzerland, and thus when Swiss health regulations should apply. There is no consistent approach to this matter across the cantons. As soon as patients residing in Switzerland are treated, careful assessments should be carried out.

Cantonal health regulations may contain provisions that make digital services more difficult. For example, in the Canton of Zurich, Paragraph 12(1) of the Health Act (GesG) should be observed, which states that professional practice must be carried out personally and, in principle, directly with the patient. This generally excludes telemedicine; however, exceptions may be made if patient safety is ensured. There is currently a discussion in the Canton of Zurich about relaxing this requirement for direct contact.

Law stated - 2 März 2025

Soft law and guidance

Is there any notable 'soft' law or guidance governing digital health?

Digital health products

Guidance governing digital health products include the following:

- Swissmedic released a guidance document regarding standalone medical device software, which encompasses applications installed on wearable devices (- Information Sheet on Medical Device Software, current version 3 from April 2024). The document also provided illustrations of non-medical software. In particular, Swissmedic refers to MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) and MDCG 2019-16 Guidance on Cybersecurity for medical devices, issued by the EU Medical Device Coordination Group.
- In 2022, the Swiss Competence and Coordination Centre of the Confederation and the Cantons (eHealth Suisse) released the Guide for App Developers, Manufacturers, and Distributors, along with accompanying checklists. This resource aims to assist in the differentiation between 'lifestyle/wellness' products and medical devices.
- In 2024, the FOPH published a Fact Sheet on the Reimbursement of Digital Health Applications under Mandat ory Health Insurance.
- In 2025, after 20 years, Swissmedic revised its Schweizerische Gute Praxis für die Instandhaltung von Medizinprodukten (GPI). This guideline describes the requirements for the maintenance of medical

devices in general. Its application is mandatory for all hospitals. For the safety of network-enabled medical devices and the maintenance of medical technology applications (eg, software, distributed alarm systems), close collaboration between IT, medical informatics, medical technology, engineering and procurement is crucial. These aspects are addressed in Chapters 8.6 and 8.7 of this guideline. For healthcare facilities that do not meet the legal definition of a hospital, such as independent medical practices or group practices without inpatient treatments, this guideline can serve as a reference for maintenance but is not mandatory (the maintenance of medical devices by these healthcare facilities is not overseen by Swissmedic, but by the cantonal health authorities). In technical terms, the guidelines primarily contain recommendations on encryption and key management. For organisational aspects, they mainly provide guidelines for drafting contracts. The guidelines generally recommend for patient data to be encrypted to the greatest extent possible and key management to either lie with the client or for contractual safeguards to ensure that the contractor can only access patient data with explicit consent of the client or only to the extent indispensable.

Digital health services

Healthcare professionals who wish to practise their profession partly or primarily through digital means find no specific soft law in their professional associations' statutes on navigating the various legal requirements. For example, the Swiss Medical Association (FMH) states in article 7 of its professional code only in a general sense that consultation or treatment via information and communication technologies is possible, provided that the required medical diligence is ensured and, in particular, the obligations regarding informed consent and documentation are met (this provision is rather new; it came into effect in November 2023).

The professional associations support their members primarily through non-binding guidance. For instance, FMH provides several publications on 'E-Health' (eg, on e-prescriptions, medical practice IT, data protection and security, and interoperability standards) on its website. Concerning teleradiology and telemedicine in general, it was reported in the media at the end of 2024 that several healthcare stakeholders are reassessing the practice of outsourcing medical services abroad. Medical associations are looking to revise their guidelines on the matter.

Law stated - 2 März 2025

Liability regimes

What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

Swiss legislation does not include specific liability regulations pertaining to digital health. Instead, general civil liability principles are applicable, notably tortious liability, contractual liability and product liability.

Product safety regulations, which encompass digital health products, establish a standard of strict liability. Accordingly, the manufacturer bears responsibility for any instances of death, personal injury or property damage resulting from product defects. The scope of manufacturer, as defined by the Product Safety Act, extends to individuals claiming manufacturer status or whose name or trademark appears on a product. Additionally, those importing products for resale, rental or other commercial purposes are also regarded as manufacturers.

While product safety regulations are subject to the principle of territoriality, the question of applicable private law claims in cross-border situations is governed by conflict of laws.

Law stated - 2 März 2025

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

What constitutes 'health data'? Is there a definition of 'anonymised' health data?

Health-related personal data

The Federal Act on Data Protection (FADP) lists health data, biometric and genetic data as sensitive personal data. While the FADP does not define 'health data', article 3 lit. f of the Human Research Act (HRA) defines it as 'information concerning health or disease of a specific or identifiable person, including genetic data.' Distinguishing health-related personal data from mere lifestyle data can be challenging. The same information may be classified as health data or not, depending on the context (eg, the number of steps taken per day).

The Swiss privacy landscape in the health sector is governed by a combination of general and specific laws. The general framework is set by the FADP. Specific laws, stemming from the Federal Constitution's mandate to protect health, include the Federal Act on Medicinal Products and Medical Devices (the Therapeutic Products Act, TPA) and the Federal Act on Research involving Human Beings (the Human Research Act, HRA). Additionally, articles 321 and 321-bis of the Criminal Code address professional secrecy. In the case of conflict, the specific law takes precedence over the general one.

Anonymised health-related data

Anonymised health-related data, according to the HRA, is health-related data that cannot (without disproportionate effort) be traced to a specific person.

Law stated - 10 April 2025

Data protection law

What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Processing of particularly sensitive personal data does not per se require consent

The Swiss concept is fundamentally different from the opposite concept of the GDPR. The Swiss Data Protection Act is based on the principle of permission with the reservation of prohibition. Accordingly, processing is generally permissible provided that the processing principles and data security are adhered to, personal data is not processed contrary to the express declaration of intent of the person concerned, and third parties are not given access to particularly sensitive personal data. Otherwise, this constitutes an infringement of privacy, which, among other things, can be justified by the consent of the person concerned. Processing of particularly sensitive personal data, including health data, does not per se require consent, even if the opposite is sometimes argued. ***If*** consent is required for the processing of particularly sensitive personal data, for high-risk profiling by a private individual or for profiling by a federal body, it must be given explicitly (article 6(7) FADP).

Human research

The HRA provides a comprehensive and relatively restrictive framework for the use of personal data in human research. It generally requires the consent of the individuals for the secondary use of their health-related personal data and biological material. Because in medical research, it is often not yet clear at the time of data collection which research projects the data may be used for, the HRA provides for certain exceptions to informed consent and allows for a general consent under specific conditions.

The HRA differentiates between two scenarios for the re-use of data:

- Reuse of non-genetic personal data (article 33 HRA): if the researchers have access to identifiable data, informed consent is required; for pseudonymised data (coded data), patients only have a right to object, and if no objection is made, the data is included in the project; and anonymised data can be freely re-used (ie, patient's consent is not required nor do they have a right to object).
- The procedure for the re-use of genetic data or biological material is stricter (article 32 HRA): the re-use of unencrypted or pseudonymised data requires informed consent; and re-use of anonymised genetic data or biological material is subject to the right of objection.

The current HRA regime presents several challenges. Obtaining informed consent for secondary use can be burdensome, especially when dealing with large datasets, data collected years ago, or individuals who are difficult to contact. This complexity often leads researchers to rely on an exception clause (article 34 HRA) intended for rare cases. This exception has become the norm in practice.

Other protections in case of automatic processing on broad scale

If sensitive personal data is processed automatically on a large scale, this may trigger specific obligations:

- article 4(1) DPO regarding logging;
- article 22(2)(a) FADP regarding data protection impact assessments (see the Federal Data Protection and Information Commissioner (FDPIC)'s Factsheet on the data

protection impact assessment (DPIA) in accordance wit h articles 22 and 23 FADP);

- article 5(1)(a) DPO regarding processing regulations; and
- article 24(a) DPO regarding the register of processing activities.

Professional and official confidentiality requirements

Healthcare professionals (HCPs) and practitioners in healthcare organisations (HCOs) are bound by professional and/or official confidentiality requirements:

1. The federal medical confidentiality rules (Swiss Criminal Code) apply to healthcare professionals such as doctors, dentists, chiropractors, pharmacists, midwives, psychologists, and their auxiliary staff, including nurses, medical practice assistants, and occupational and physical therapists. For other professional groups handling health data, cantonal confidentiality obligations may apply. Health professions not covered by article 321 of the Swiss Criminal Code (naturopaths, acupuncturists, etc.) are nevertheless subject to the duty of confidentiality under article 62 of the FADP. The definitions of 'assistants' and 'confidentiality' correspond to those in article 321 Swiss Criminal Code.
2. Public authorities and their members, as well as public officials are bound by official secrecy obligations (Swiss Criminal Code). This applies to both institutional and functional public officials (those performing public duties). These confidentiality obligations may also extend to health data processed by employees of public hospitals.

Revealing confidential information to third parties is not allowed unless legally mandated, permitted (for research purposes, see article 321-bis(2) Criminal Code), or with the informed consent of the patient (consent may be express or tacit; consent may also be given by behaviour implying consent, see the FDPIC's publication on patient data disclosure).

Auxiliary personnel, including IT providers (see the FDPIC's publication on patient data disclosure), are also subject to professional confidentiality.

Law stated - 10 April 2025

Anonymised health data
Is anonymised health data subject to specific regulations or guidelines?

Truly anonymised health data is not considered personal data. General data protection laws do not apply to such data.

However, the process of anonymising health data itself is subject to relevant data protection rules:

- in general, transparent information must therefore be provided about the implementation and purpose (in particular, secondary use) of anonymisation (principle of transparency and purpose limitation);

- the Federal Act on Data Protection (FADP) stipulates a research privilege, which is also included in most cantonal data protection laws. This privilege facilitates the processing and anonymisation of personal data for non-personal purposes, particularly in research, without the need for the data subject's consent;
- however, the research privilege under the FADP and cantonal data protection laws is ineffective in matters that fall within the scope of the Human Research Act (HRA). The HRA requires consent (to varying degrees, see above). The doctrine criticises this regulation, stating that it is outdated in relation to the realities of research. In its 2023/2024 activity report, the Federal Data Protection and Information Commissioner (FDPIC) addressed this issue and reaffirmed the primacy of the HRA.

Law stated - 10 April 2025

Enforcement

How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The Federal Data Protection and Information Commissioner (FDPIC) is designated to oversee federal bodies, provide guidance to private entities, and enforce federal data protection legislation. Cantonal 'public bodies' (as defined in the cantonal data protection laws) are governed by cantonal data protection regulations and are supervised by cantonal data protection authorities. Many healthcare organisations (HCOs) fall under the category of 'public bodies'. These authorities' jurisdiction, resources and determination are not equivalent to those of their European counterparts.

Violations may result in sanctions for the company as well as fines for natural persons. The authorities may conduct investigations or issue orders to restrict, amend or cease processing. The disclosure of data in the context of professional secrecy may result in additional sanctions. Fines (up to 250,000 Swiss francs) may be imposed on persons responsible for an offence. A criminal investigation is possible, and the offence may be recorded in the criminal register. In contrast to the regulation under the General Data Protection Regulation, only certain offences are punishable by law, and even these are only punishable if committed intentionally.

- In 2024, a Swiss Federal Audit Office's (SFAO) audit of the Federal Office of Public Health (FOPH)'s oversight of insurers highlighted the need for clearer roles and better coordination between the FDPIC and the FOPH. Health insurers must comply with both social security and data protection laws and are therefore supervised by both authorities. As an initial step, the FDPIC and FOPH revised Circular No. 7.1 on health insurance supervision. They later established regular communication to enhance supervision, leveraging the FOPH's on-site inspections and the FDPIC's strengthened legal powers under the revised FADP. This coordination covered: new insurance apps and models; outsourcing of health data; implementation of revised Circular No. 7.1; mandatory invoice copies for insured persons; insurer access to employment contracts in home care; GP access to insurance medical advisers; data protection

in integrated care centres; and Insurance certificates for tax authorities (excluding health service details).

- In 2023, the data protection officer of the Canton of Zurich examined Zurich's retirement and nursing homes and found that many homes lack the required special authentication measures.
- In 2022, the FDPIC conducted and concluded an investigation into the national organ donor register operated by the Swisstransplant Foundation. The FDPIC identified deficiencies in the online authentication process. Shortly after the FDPIC submitted its final report, Swisstransplant decided to permanently shut down the register. By December 2022, the register was officially closed, and all data was deleted. That same year, Swiss voters had approved the principle of presumed consent for organ donation and the establishment of a federally maintained register with a similar function to Swisstransplant's. The new register is expected to launch in 2025.
- In 2022, the FDPIC launched a case investigation into the breast implant register managed by the Swiss Plastic Surgery Association. The register records all breast plastic surgery operations involving implants along with any difficulties encountered during the operations and serves several purposes. On the one hand, it aims to improve the quality of service by sharing information on any incidents. It also allows the tracking of implants to facilitate product recalls in the case of defects found in a series of implants. On the other hand, the data collected is also used for the compiling of industry statistics. The FDPIC launched an investigation after a flaw was reported in the register's IT architecture that allowed anyone to access patient records in a few simple steps. In addition to personal details (first name, last name, date of birth etc.), medical information regarding operations was also accessible. While the FDPIC was preparing his report, meanwhile, the register has been taken offline.
- In 2022, the FDPIC conducted an investigation into a database of private covid-19 test centres that presented security issues. In his final report, he pointed out that the data was exposed to significant security risks due to a known vulnerability. However, the data controllers promptly took appropriate action when the flaw was detected, minimising the risk to the data subjects, so that the FDPIC was able to close the investigation without the need to issue any recommendations.

Law stated - 10 April 2025

Cybersecurity

What cybersecurity laws and best practices are relevant for digital health offerings?

Relevant cybersecurity laws

Data protection legislation is central to cybersecurity for digital health offerings. The processing of data by public entities is regulated by the FADP for federal bodies, which also applies to private organisations carrying out federal public functions, such as health insurers and pension funds. Entities designated as 'public bodies' at the cantonal level are governed by cantonal data protection laws (eg, Zurich's Information and Data Protection

Act). Many healthcare organisations fall into the category of 'public bodies.' The Federal Act on Data Protection (FADP) governs personal data protection and data security, which is a fundamental aspect of cybersecurity in Switzerland. Data security covers all measures taken to ensure the confidentiality, integrity and availability of data. The legislature adhered to a 'technologically neutral' stance. This approach prevents a gap between technological advancements and the legal framework, ensuring greater long-term adaptability. However, it also has the downside that the legislation may sometimes lack sufficient precision.

- Legally, there is no requirement to adhere to specific technical standards. However, in practice, companies often refer to international standards as benchmarks or best practice guidelines.
- Switzerland does not have a 'reasonable security' test or a specific framework governing this standard.
- Controllers and processors must take 'appropriate technical and organisational measures' to ensure data security commensurate with the risk. The greater the risk of a breach of data security, the higher the requirements for the measures to be taken. This is generally interpreted as a requirement to use state-of-the-art technologies, as outlined in the FDPO.
- The FADP mandates breach notification if the incident is likely to pose a high risk to the data subject's personality or fundamental rights. The notification must be sent to the Federal Data Protection and Information Commissioner (FDPIC) as soon as practicable and should include details on the nature of the breach, its consequences and the measures taken or planned.

Switzerland has not implemented any comprehensive cybersecurity legislation thus far. The only clear exception is the Information Security Act (ISA), which came into effect on 1 January 2024, together with its four implementing ordinances. The ISA governs the structuring of the federal administration in terms of safeguarding against cyber risks. The ISA establishes a competence hub – the National Cyber Security Centre (NCSC) – and addresses various compliance requirements for external service providers engaging with the federal administration. On 1 April 2025, a new reporting obligation(as adopted in parliament on 29 September 2023) for operators of critical infrastructures came into force. The authorities and organisations subject to the reporting obligation must report cyberattacks to the NCSC within 24 hours under certain circumstances. The reporting obligation will be in effect for six months before non-compliance becomes punishable from 1 October 2025. The Cybersecurity Ordinance (provisional version available here) contains the implementing provisions for the reporting obligation and, in particular, regulates the exceptions. The list of operators of critical infrastructures includes:

- healthcare facilities on the cantonal hospital lists (in addition to hospitals, also maternity centres and nursing homes);
- medical laboratories with a licence under the Epidemics Act;
- companies that manufacture, place on the market or import medicinal products;
- social insurers;
- manufacturers of hardware or software whose products are used by critical infrastructures and have remote maintenance access or are used to control and

monitor operational systems and processes or to ensure public safety (examples include laboratory equipment such as automated microscopes or analytical tools).

In addition to these frameworks, there are additional rules and requirements for regulated industries, including in the health space (eg, article 74 MedDO, article 51(2) Medicinal Products Ordinance (VAM); article 12 Ordinance on the Electronic Patient Record).

Best practices

The FADP permits the certification of data processing systems, software, and entities (both private individuals and federal bodies) that handle personal data. Although such certifications are rare in practice, they effectively necessitate compliance with ISO 27001 as a prerequisite.

Relevant Swiss guidelines include the following.

- In July 2022, the NCSC issued 'Recommendations on cybersecurity in the healthcare sector'. The NCSC recommends that all healthcare providers implement the minimum cybersecurity requirements set out in this paper. The NCSC considers them to be best current practice.
- In May 2022, the Swiss Conference of the Cantonal Ministers of Public Health (GDK) supplemented its existing recommendations on hospital planning with a recommendation on data protection and information security (recommendation 16). Among other things, this recommends that hospitals have an information security management system (ISMS) and take certain ISMS measures.
- Swissmedic released a guidance document regarding standalone medical device software, which encompasses applications installed on wearable devices (- Information Sheet on Medical Device Software, current version 3 from April 2024). The document also provided illustrations of non-medical software. In particular, Swissmedic refers to MDCG 2019-16 Guidance on Cybersecurity for medical devices, issued by the EU Medical Device Coordination Group.
- In January 2024, the FDPIC published its Guide to Technical and Organisational Data Protection Measures (TOM). In this guide, the FDPIC refers to the Federal Office for National Economic Supply (FONES)'s minimum standard for improving 'ICT resilience'. It is aimed in particular at operators of critical infrastructures but is basically applicable for any company or organisation and freely available.
- For medical device software, Swissmedic refers to EU Medical Device Coordination Group 2019-16 Cybersecurity for medical devices.
- There are numerous recommendations aimed primarily at the federal administration.

Debate on cloud services (including public-cloud services)

Cloud services can play an important role in healthcare; for example, in data processing and storage, AI-assisted diagnoses or personalised medicine, image processing and diagnostics, secure communication, and identity and access management. Whether cloud providers, particularly those based abroad, can be recognised as auxiliary personnel under Swiss law is

a matter of debate. The requirement for obtaining consent when engaging a cloud provider is also controversial, both in relation to Swiss cloud services and those with international ties.

The recent contributions to this discussion are aimed at public bodies or public authorities. As already stated, many healthcare organisations (HCOs) in Switzerland qualify as cantonal public bodies. They do not specifically address health data, but deal with sensitive data in general. The most recent contributions include the following.

- The recommendations in the fact sheet Cloud-Specific Risks and Measures- , published in a revised version on 14 February 2022 by Privatim, the influential conference of Swiss data protection commissioners. The fact sheet addresses the use of cloud services by public bodies. Privatim considers potential access by foreign authorities as the key cloud-specific data protection risk. Privatim differentiates in its recommendations between normal and sensitive personal data. Criticism has been raised against this distinction (see the commentary re the privatim fact sheet on datenrecht.ch).
- The Canton of Zurich conducted a consultation on the 'Law on Digital Basic Services' in 2024. The law is aimed at cantonal and municipal authorities. Among other points, the previously proposed version stated that information should generally be stored in Switzerland or the EU, and that for sensitive personal data or confidential or secret information, encryption is required to prevent access by the cloud provider without the involvement of the public authority; this would essentially have allowed hosting services. This point faced strong criticism. In the new version of the 'Law on Digital Basic Services' soon to be debated in the cantonal parliament, a permission provision is included if the data centres are located outside a region with adequate protection. This will generally require the conclusion of standard contractual clauses and the conduct of a Transfer Impact Assessment that evaluates these clauses, the other technical and organisational measures (TOMs), and the residual risk of foreign lawful access (see the commentary re the new version of the 'Law on Digital Basic Services' on dat enrecht.ch).
- In the past, several cantons had published guidelines on the use of cloud services by public bodies. In technical terms, they primarily contained recommendations on encryption and key management.

Law stated - 10 April 2025

Best practices and practical tips

What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Managing the ownership, use and sharing of user data, including raw and anonymised data, as well as the output from digital health solutions, requires careful attention to legal compliance.

It is important to note that raw data is not necessarily anonymised by definition. Raw data can include personally identifiable (health) information if it has not undergone anonymisation processes and thus constitutes (sensitive) personal data under the Federal Act on Data Protection (FADP) resulting in a higher level of protection. Anonymised health data, however, has already been processed to remove any identifiable information and thus does no longer constitute sensitive personal data under the FADP. As discussed above, the process of anonymising health data itself is subject to relevant data protection rules.

The following best practices should be considered:

- Clarify ownership and consent: define data ownership clearly in contracts and obtain explicit, informed consent from users. Offer granular consent options for specific uses of data.
- Ensure legal compliance: follow relevant data protection laws, integrate privacy by design, and apply data minimisation principles.
- Anonymisation and de-identification: use robust anonymisation techniques and regularly audit them. Define clear retention periods for data.
- Data sharing: set clear terms when sharing data with third parties, implement strict access controls and maintain transparency with users about data usage.
- Security protocols: employ strong encryption, conduct security audits and use multi-factor authentication to protect data.
- Handling data use and outputs: ensure data outputs are accurate, define usage guidelines and provide users access to their data.
- Transparency and empowerment: allow users to correct or delete their data.
- Breach response: have a response plan for data breaches, ensuring timely notifications to users and regulators.

Law stated - 10 April 2025

INTELLECTUAL PROPERTY

Patentability and inventorship

What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Patentability

For an invention to be patentable, it must meet certain criteria under the Patents Act (PatA). First, it must be novel, meaning it has not been disclosed before in any public form. Second, the invention must involve an inventive step; it cannot be something that would be obvious to someone skilled in the field. Additionally, the invention must have industrial applicability, meaning it should have a practical use, such as in healthcare or consumer

health. Furthermore, Swiss patent law requires that the invention have a technical character. This means that it must provide a technical solution to a problem, such as a hardware device used in the healthcare field. Inventions that are purely abstract, like mathematical models or business methods, without any technical implementation, are not patentable.

There are also exclusions to what can be patented. For example, abstract ideas or mathematical models or software that are not integrated are not eligible for patent protection, unless they form part of a broader technical solution, such as a diagnostic tool using artificial intelligence. Inventions related to medical methods for treating the human body by surgery or therapy are excluded from patentability under the European Patent Convention (EPC), which also applies in Switzerland. However, medical devices, diagnostic tools and other healthcare technologies that have a technical character are patentable. Biotechnological inventions, like those involving genetic material or human embryos, face restrictions.

Inventorship

When it comes to inventorship, the person who makes a substantial contribution to the conception of the invention is considered the inventor. In digital health, this can include contributions from both technical experts, such as software engineers, and healthcare professionals who apply the technology clinically. In many cases, employee inventions are governed by employment contracts, meaning the rights to the patent may belong to the employer unless otherwise agreed upon: if it is a contractual obligation and the invention is created during the course of their work, the invention belongs to the employer provided nothing else is stated in the employment contract (article 332 Code of Obligations (CC)). Inventions created during the course of work but which are not part of the employee's contractual obligations must be reported to the employer if this has been agreed in writing. The employer can then decide whether they want to obtain the invention in question. A similar provision exists for computer programs protected by copyrights according to the article 17 Copyright Act (CopA) . Digital health inventions often involve joint inventorship, where multiple individuals contribute to the invention. Proper attribution of inventorship is essential to avoid disputes, particularly in interdisciplinary teams consisting of engineers, software developers and healthcare professionals.

Under Swiss copyright law, databases are only eligible for protection if they are considered original. To meet the originality requirement, a database must represent an intellectual creation due to the selection or arrangement of its content. If a database is purely comprehensive and serves its intended purpose, it does not meet the originality criteria. As a result, most databases are not protected by copyright, even if significant investments were made in their creation.

In Switzerland, the allocation of rights to AI-generated inventions and creative works is guided by existing intellectual property laws, which generally require human inventorship and authorship. Because AI is not recognised as a legal person, AI-generated inventions are attributed to the person or entity that developed the AI or made significant contributions. Ownership typically belongs to the inventor or employer, depending on employment contracts. For copyright protection, works generated solely by AI may not be eligible unless a human played a significant role in shaping the output. If AI is used as a tool, the work is considered human-created, and rights go to the creator or employer. However, if AI acts autonomously, Swiss law does not yet address ownership, potentially requiring legal reforms.

Law stated - 2 März 2025

Patent prosecution

What is the patent application and registration procedure for digital health technologies in your jurisdiction?

While there are no specific prosecution procedures for digital health inventions, the distinction in patenting between Swiss national patents and European patents remains important, with different examination processes.

Switzerland is a member of the European Patent Convention (EPC) and the European Patent Office (EPO) is responsible for granting European patents, which are valid in Switzerland if designated during the application process. Patent applications can be filed directly with the Swiss Federal Institute of Intellectual Property (FIIP) for national patents. However, as of current regulations, Swiss national patents are granted without an examination of novelty or inventive step, which contrasts with the more rigorous examination process under the EPO for European patents. This means that while a Swiss national patent may be easier to obtain in terms of procedural requirements, it does not undergo the same scrutiny as a European patent application. A third party can, however, challenge in court at any time whether the invention was novel. If necessary, the patent can be declared invalid. The FIIP published a brochure on patent applications in Switzerland, currently available in German, French and Italian only.

There are no specific prosecution procedures for digital health technologies before either the FIIP or the EPO. Digital health inventions are treated under the same general procedures as other technologies, with the key considerations being whether the invention meets patentability criteria such as novelty, inventive step and industrial applicability.

Law stated - 2 März 2025

Other IP rights

Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Several intellectual property (IP) rights are crucial for digital health offerings, beyond just inventorship and copyright.

- Trademarks protect logos, names or signs used to identify digital health products or services. These can be secured by filing an application with the FIIP, ensuring they are distinctive and not similar to existing trademarks.
- Designs safeguard the visual appearance of products, such as the user interface of health apps or wearable devices. Design rights can be obtained by filing an application with the Swiss Federal Institute of Intellectual Property (FIIP) or the European Union Intellectual Property Office (EUIPO) if seeking wider European protection.
- Trade secrets protect confidential business information like algorithms or proprietary data. While no formal registration is required, trade secrets are secured through

confidentiality measures, such as non-disclosure agreements (NDAs) and restricted access.

Law stated - 2 März 2025

Licensing

What practical considerations are relevant when licensing IP rights in digital health technologies?

Both registered and unregistered IP rights can be the subject of a licensing agreement. Swiss statutory law does not provide specific provisions for creating or regulating the terms of a licensing relationship. Mandatory aspects of Swiss contract law (such as limitations on liability) and competition or regulatory laws may impose certain restrictions on contractual freedom. There is no requirement for the licensing agreement to be in writing, registered or approved, with one exception: licenses for collective marks are only valid if they are registered. However, in Switzerland, the registration of a license is possible for registered intellectual property rights (such as patents, trademarks and designs), and this registration allows the license to be enforced against third parties who later acquire the licensed IP. Swiss law does not require the licensing agreement to include specific terms to be binding.

Parties have the freedom to negotiate royalty rates (including agreeing to a free license) as well as the contract's duration and termination conditions. In contracts with consumers, there are restrictions on clauses related to choice of law, jurisdiction and the use of general terms and conditions. Under Swiss law, co-ownership can take two forms: joint ownership (article 646 Civil Code), where each co-owner holds a specific share of the right, or ownership in common (article 652 Civil Code), where all co-owners collectively own the entire property. To ensure clarity in intellectual property rights, it is advisable to define ownership allocation through contractual agreements, such as in R&D contracts, specifying the rights and obligations of each party.

Law stated - 2 März 2025

Enforcement

What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

Enforcing IP rights in digital health technologies follows standard IP enforcement procedures:

- IP owners can enforce their rights through civil litigation, seeking to prevent or stop infringements and claim damages. Courts may grant injunctions to halt ongoing or imminent violations, award compensation for financial losses, or require the infringer to surrender unlawfully gained profits. Additionally, infringing goods may be ordered for destruction, and courts can mandate the publication of judgments to inform the public about the ruling. Depending on the canton, cases are brought before

commercial or regular civil courts. In urgent situations, rights holders can request preliminary injunctions to swiftly stop unauthorised use of their IP.

- The Federal Patent Court has exclusive jurisdiction in civil matters relating to both the validity and the infringement of patents. Non-patent IP disputes are initially heard by the High Court or Appeals Court of the relevant canton. The Federal Supreme Court serves as the appellate instance for all IP proceedings.
- For domain name disputes, Switzerland follows the Uniform Domain-Name Dispute-Resolution Policy (UDRP) for .ch domains. The UDRP procedure in Switzerland is conducted by the World Intellectual Property Organisation (WIPO), which is headquartered in Geneva.

In a recent case before the Federal Supreme Court involving a patent for a ventilator used in intensive care, the court had to determine whether a unique feature of the invention, namely, an animated representation of the ventilated lung displayed on a screen, contributes to solving a technical problem and thus affects the inventive step. The Court ruled in favour of the patent holder.

Law stated - 2 März 2025

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

The promotion of digital health products and services in Switzerland is subject to strict regulations, especially for medical devices, pharmaceuticals and healthcare services. Key legal frameworks include the Therapeutic Products Act (TPA), the Medical Devices Ordinance (MedDO), the Medicinal Products Advertising Ordinance (AWV), the Federal Act Against Unfair Competition (UCA), professional and ethical regulations set by HCPs professional associations as well as data protection laws.

- Medicinal Products: direct-to-consumer advertising for prescription medicines is prohibited. Only healthcare professionals may be targeted in advertising. Over-the-counter (OTC) medicines may be advertised to the public, but claims must be truthful, non-misleading and scientifically substantiated. The key criterion for direct-to-consumer advertising is its suitability for promoting sales, with the focus on how the public is addressed. Even general information about medicinal products may constitute advertising if it can influence consumer behaviour. Non-promotional information, such as general health or disease-related content that does not refer to specific products, is allowed. However, distinguishing between permissible information and prohibited advertising is difficult, especially with outdated case law and Swissmedic guidelines. Swiss legal doctrine generally allows corporate advertising for pharmaceutical companies (understood as primarily targeting shareholders, analysts, potential investors and media professionals). The Federal Administrative Court recently confirmed this (BVGer C-1080/2022, 26 September 2024), marking the first Swiss case law distinguishing unlawful direct-to-consumer advertising from permissible corporate advertising. However, the Court's ruling shows

a restrictive stance on corporate advertising. Until higher court clarification, it is advised to design corporate advertising restrictively.

- Medical devices: medical devices intended solely for use by healthcare professionals must not be advertised to the public. Claims for devices must only contain statements that correspond to the product information. Misleading statements, particularly concerning the intended purpose, safety and performance of a device, are prohibited. If a digital health product qualifies as a medical device, the same rules as above apply.
- The Therapeutic Products Act (TPA) prohibits the acceptance or granting of undue benefits. If healthcare professionals are paid for marketing services, the payment must be reasonable and proportionate.
- As a general rule, healthcare professionals in Switzerland advertise very cautiously. Their professional regulations require them to strictly separate this activity from their core professional duties.
- Non-medical wellness and fitness apps are not subject to medical advertising laws but must comply with unfair competition and data protection rules.
- General Advertising Rules and Restrictions: the UCA prohibits misleading, deceptive or aggressive marketing. Any health-related advertising must be fact-based and should not exploit fears or false expectations. Endorsements by doctors or health professionals in marketing are highly restricted. Healthcare professionals must comply with their professional and ethical regulations. The UCA prohibits unfair advertising practices, in particular the sending of unsolicited electronic advertising without prior consent (opt-in). There is one exception: The person contacted is a customer of the company and the promotion concerns similar products or services from the same company. This exception only applies if a sale has been made or a service has been used. Simply opening an online account is not sufficient. In any case, the identity of the sender must be indicated and there must be a simple and free way to opt out of further advertising. Both case law and legal doctrine favor a narrow interpretation of the exception. 'Similar products or services' refer only to those that are closely related to what the customer originally purchased or used.
- Digital health services collecting patient data must comply with the Federal Data Protection Act (FADP). If sensitive personal data is processed automatically on a large scale, this may trigger specific obligations. This may apply to marketing based on patient data profiling.

Law stated - 2 März 2025

e-Commerce

What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

Contracts can be established electronically, necessitating mutual agreement between parties on the essential elements of the contract. The acceptance of an offer must mirror the terms of the offer, ensuring customers are fully informed about the product and price.

The Federal Act Against Unfair Competition (UCA) outlines obligations for companies offering goods or services online. These include:

- disclosing full identity and contact details, including an email address, in a clear manner;
- detailing the technical steps required to complete the transaction, such as a step-by-step purchase procedure;
- providing the opportunity and means to correct input errors before finalising the order; and
- promptly confirming the order through electronic communication, such as a confirmation email.

Law stated - 2 März 2025

PAYMENT AND REIMBURSEMENT

Coverage
Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Swisshealthcare insurance system

Basic health insurance is mandatory under the Health Insurance Act. It offers the same range of services and benefits to all insured people. Digital health applications with a medical purpose, and in some cases, digital health applications for supporting and informing patients (self-management), can fall within the scope of the Health Insurance Act. A prerequisite for reimbursement under the compulsory healthcare insurance (OKP) is compliance with the WZW criteria (the acronym derives from the German words and stands for effectiveness, appropriateness and efficiency).

- TARMED, the tariff system in place since 2004 for outpatient medical services, will be replaced on 1 January 2026 by the new fee-for-service tariff structure TARDOC and a tariff structure for flat rates. At its meeting on 19 June 2024, the Federal Council partially approved both tariff structures and set out requirements for their introduction.
- Medical devices, medications, laboratory tests, aids, dental procedures and maternity or preventive healthcare prescribed by medical professionals are specified in comprehensive positive lists. Any services or products not listed are not covered by compulsory health insurance and do not require reimbursement, following a closed catalogue system. The lists include tariffs, rates and maximum reimbursement levels.
- SwissDRG (a flat rate tariff) is the tariff system that regulates the remuneration for services in inpatient acute care.

Supplementary insurance is optional and subject to the Insurance Contracts Act (VVG), covering a higher level of comfort or additional services and benefits.

Reimbursement of digital health applications

Outpatient sector

According to the 'Fact sheet on the reimbursement of digital health applications (dgA) under compulsory healthcare insurance' (current version dated November 2024), the reimbursement eligibility of dGA varies depending on their type and user group:

1. For dGA used by doctors for the diagnosis, treatment or monitoring of diseases classified as medical services there is a legal presumption of mandatory benefits; they may be reimbursed by compulsory health insurance (OKP) even without explicit inclusion in Annexes 1 and 2 of the Ordinance on Health Insurance Benefits (KLV). The prerequisite for this is that the service is not listed on the negative list (Annex 1 KLV). The prerequisite for this is that the service is not listed on the negative list (Annex 1 KLV). The obligation to cover medical services for prevention, maternity and dental treatments is excluded from the principle of trust. These services are exhaustively listed in articles 12–19 KLV. Ensuring correct tariff classification is the responsibility of the tariff partners (tariff autonomy).
2. dGA used by non-medical healthcare professionals, such as nurses, in the course of their professional duties may be reimbursed under certain conditions. Only services provided by non-medical healthcare providers who are authorised as service providers under the OKP in accordance with the Health Insurance Ordinance (KVV) are reimbursed. Their OKP-covered services are exhaustively listed in the KLV. If the dGA constitutes a new service that is not part of an already listed service in the KLV, an application must be submitted to the Commission for General Benefits and Fundamental Questions (ELGK) for its inclusion in the mandatory benefits. The decision on whether the service is covered by compulsory health insurance (OKP) falls within the competence of the Federal Department of Home Affairs (EDI), which is advised by the ELGK.
3. dGA that patients use independently to support self-treatment or monitor chronic conditions may also be reimbursed, provided they are listed in the List of Aids and Devices (MiGeL). For OKP coverage, the application must be medically necessary and prescribed by a doctor. To include a new service in the MiGeL, an application must be submitted to the Federal Commission for Analysis, Means, and Devices (EAMGK). The inclusion or modification of positions in the MiGeL is made through a decision by the Federal Department of Home Affairs (EDI), which seeks advice from the EAMGK. Any significant changes to the medical purpose of an application require reassessment to ensure continued compliance with medical standards. Similar products are grouped together in a MiGeL position, for which a maximum reimbursement amount is set. If the actual price of a dGA exceeds the maximum reimbursement amount set in the MiGeL, the additional costs must be borne by the patients themselves. The maximum reimbursement amounts in the MiGeL correspond to the average price of similarly suitable products available on the market. The foreign price is also taken into account.

The reimbursement of services provided by both medical (1) and non-medical (2) healthcare providers is regulated within the framework of tariff agreements. Taking into account the WZW criteria, the tariffs also include the dGA used by the service provider. The economically appropriate tariff classification of services is the responsibility of the tariff partners (tariff

autonomy). The tariffs must comply with legal requirements and adhere to the principles of cost-effectiveness and fairness. Currently, there is a lack of an adequate representation of the dGA service in the applicable tariff agreements. The KVG does not have a compensation model for dGA services that can be used for tariff determination. Consequently, even for WZW-compliant dGAs, there are still obstacles to OKP reimbursement.

Inpatient sector

Digital applications that are used solely to support the activities of healthcare professionals (eg, reading and analysing data or controlling a device) in the inpatient sector are reimbursed as part of the SwissDRG flat rate tariff. Only if they are genuine additional services (this mainly concerns 'innovative additional medical services') are they reimbursed separately (ie, through supplementary insurance).

Reimbursement under supplementary insurance

The legal relationship between supplementary insurance and the insured is of a private law nature and is governed by the VVG. Supplementary insurances have the freedom to design their additional medical services catalogues. Services that provide a benefit falling within the scope of compulsory health insurance must not be included in the list of benefits provided by supplementary health insurance.

At the end of 2020, the Swiss Financial Market Supervisory Authority (FINMA) required insurers to only accept billing for actual additional services outside of the OKP (see press release). As a result, the Swiss Insurance Association (SVV) developed an industry framework for 'Additional Services VVG', which the majority of supplementary insurers have committed to and which is to form the basis for future tariff agreements. Each service provider must specify the relevant benefit level of the OKP and, based on this, the VVG additional services. The specific service packages and prices (ie, tariff points) for additional services are negotiated individually between hospitals, doctors and supplementary insurers to ensure compliance with competition law requirements. On the service provider side, the FMCH (the FMCH is the umbrella organisation of 16 specialist societies and three professional organisations for specialists in invasive and acute medicine in Switzerland) has developed a catalogue that describes and delineates categories of additional and supplementary medical services in the VVG area (the VVG catalogue or additional services catalogue). The catalogue is primarily applicable to the inpatient and outpatient hospital sector.

This makes benchmarking difficult for manufacturers. Although there are platforms with calculation tools for additional services, even on these platforms, no price can be determined (only a relative evaluation of medical services based on points).

Discussion on telemedicine by doctors licensed in Switzerland during their stay abroad

Article 34(2) of the Health Insurance Act stipulates that services are generally only covered by health insurance if they are provided in Switzerland (principle of territoriality). It is an open secret, and has already been reported in Swiss media, that doctors working for Swiss telemedicine providers also practice from abroad. The coverage of these services under Swiss mandatory health insurance is legally disputed.

Law stated - 2 März 2025

UPDATES AND TRENDS

Recent developments

What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

On 26 May 2021, the updated Medical Devices Ordinance (MedDO) came into effect, followed by the introduction of the new Ordnance on In Vitro Medical Diagnostic Devices on 26 May 2022. These changes were aimed at aligning Switzerland's regulations with EU Regulations (EU) 2017/745 (MDR) and (EU) 2017/746. Under previous regulations (the European Medical Device Directive and the former Swiss MedDO), medical devices placed on the Swiss market could also be sold in Europe, and vice versa, due to the mutual recognition agreement (MRA). However, the MRA has not been updated to reflect the new regulations. As a result, Switzerland is now considered a third country under the MDR, leading to the cessation of mutual recognition. The third-country status significantly impacts market surveillance in Switzerland. With Swissmedic losing access to EUDAMED, manufacturers, authorised representatives and importers must register with Swissmedic to obtain a Swiss Single Registration Number, similar to the SRN used in Europe. This is essential for establishing a market surveillance system in Switzerland. Additionally, devices will need to be registered in swissdamed, the Swiss Database on Medical Devices, with details and deadlines for registration expected to be determined in the future.

On 27 April 2022, the Federal Council announced to the public that the Electronic Patient Record (EPR) would undergo further development. It is intended to be integrated as a component of compulsory health insurance. All healthcare providers operating in outpatient settings will be required to maintain an EPR. Additionally, the Federal Council intends to grant access to research endeavours with the consent of individuals involved. Furthermore, there are plans to utilise the technical framework of the EPR for supplementary services (for more information regarding the further development of the EPR, see here). At its meeting on 28 June 2023, the Federal Council submitted the proposal for the comprehensive revision of the Federal Act on the Electronic Patient Record (EPRA) for consultation. The consultation on the draft of the comprehensive revision of the EPRA lasted from 28 June to 19 October 2023. It will take several years for the amendments to come into force.

On 14 February 2025, the Swiss Federal Council decided to ratify the Council of Europe's AI Convention. This decision includes aligning Swiss legislation with international AI standards, ensuring data protection, transparency and non-discrimination. The Federal Council emphasised innovation while protecting fundamental rights. Further legislative changes and non-binding measures will be developed by 2026, with input from various stakeholders (official press release).

Law stated - 2 März 2025