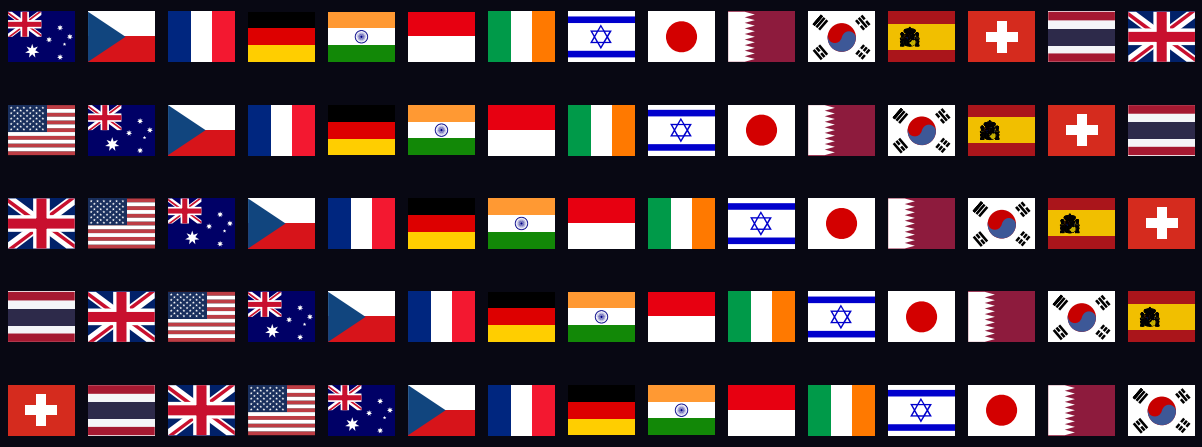
DIGITAL HEALTH

Switzerland



LEXOLOGY
Getting The Deal Through

Consulting editor
Latham & Watkins LLP

Digital Health

Consulting editors

Eveline Van Keymeulen, Oliver Mobasser, Samantha Peacock, Sara Patel, Brett Shandler

Latham & Watkins LLP

Quick reference guide enabling side-by-side comparison of local insights, including market overview; legal and regulatory framework; data protection and management; intellectual property rights, licensing and enforcement; advertising, marketing and e-commerce; payment and reimbursement; and recent trends.

Generated 27 January 2023

Table of contents

UPDATES AND TRENDS

Recent developments

Contributors

Switzerland

Peter Ling
peter.ling@lenzstaehelin.com
Lenz & Staehelin

Sevan Antreasyan
sevan.antreasyan@lenzstaehelin.com
Lenz & Staehelin

Leo Rusterholz
leo.rusterholz@lenzstaehelin.com
Lenz & Staehelin

Federico Trabaldo Togna
federico.trabaldotogna@lenzstaehelin.com
Lenz & Staehelin

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?

There is a very active investors' scene in Switzerland, composed of both traditional venture capital and private equity funds, as well as major industrial players. Academic institutions with strong technological research capabilities (eg, the École Polytechnique Fédérale de Lausanne (EPFL) or Eidgenössische Technische Hochschule in Zurich) are also major actors in the local digital health market. Supporting a practical application of science and technology, these academic institutions foster the emergence of a vivid and innovative startup ecosystem through the out-licensing of their research products to early-stage companies. Local startup incubators (eg, Fongit in Geneva, EPFL Innovation Park in Lausanne, Bio-Technopark in Schlieren, canton of Zurich) or government-driven programmes (eg, InnoSuisse), although not exclusively focused on the digital health industry, play also a vital role in this market, by providing an essential (material, human and financial) support to companies, at an early stage of their development.

Two prominent areas of innovation in the local digital health market are:

- digital medical devices (eg, medical software); and
- wearables and biosensors (eg, monitoring the health situation of the user through biosensors).

Law stated - 18 November 2022

Investment climate

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

Recent years have seen an important flux of funds in growth companies active in the healthcare industry, including in digital health technologies. The climate has been favourable to investments, with a strong local investors' scene and easy access to the Swiss market for non-Swiss investors.

The covid-19 pandemic and the uncertainties relating to the health situation seem to have only temporarily slowed down investments in digital health. Since the second half of 2020, investments have increased not only in pandemic-related health ventures, but more generally in digital health products.

Law stated - 18 November 2022

Recent deals

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

Among the recent deals that are worth mentioning, there is the initial public offering of SOPHiA Genetics, a Switzerland-based data-driven healthcare technology company, on Nasdaq in July 2021, and the acquisition of Consulcesi Group by Gyrus Capital in July 2022.

Law stated - 18 November 2022

Due diligence

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

A typical due diligence issue that investors should address before acquiring a stake in a digital health company, especially when the investment is a seed or series A financing, consists of the intellectual property (IP) rights protection strategy of the company. This includes, in particular:

- ensuring that the IP rights required for the company's current business and development are owned by the company (in this respect, particular attention must be given to the contractual framework between the company and its founders, employees and consultants); and
- if IP rights are in-licensed from a third party (eg, academic institutions), ascertaining that the terms of the licence will give sufficient freedom to the company to operate or, should that not be the case, requiring, as a condition precedent to the investment, a renegotiation of acceptable licensing terms.

Law stated - 18 November 2022

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?

Financing structures used by digital health ventures are generally similar to those used for companies in other sectors. Typically, a company would carry out its first financing through the issuance of convertible debt instruments and, when a proper valuation is available, traditional equity financing rounds would be used as financing tools.

Although they are not specifically related to the digital health sector (but more generally to ventures with a strong focus on innovation and R&D), Swiss federal and cantonal authorities have set up various initiatives aiming at supporting innovation and early-stage companies. For example, InnoSuisse, the Swiss federal innovation agency, has various training and coaching programmes that help ventures scale up, and provides public funding to public-private research projects.

Law stated - 18 November 2022

LEGAL AND REGULATORY FRAMEWORK

Legislation

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

The Federal Act on Medicinal Products and Medical Devices (TPA) sets the general regulatory framework for the manufacture, distribution and use of all medical devices.

The Medical Devices Ordinance contains the statutory definition of medical devices. This definition includes:

> *'instruments, apparatus, appliances, software, materials, accessories or other medical technology articles, whether used alone or in combination, including the software intended to be used specifically for diagnostic or*

therapeutic purposes and necessary for the proper application of a medical device:

that are intended for use on human beings;

that do not achieve their principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which action can be assisted by such means; and

that serves to:

diagnose, prevent, monitor, treat or alleviate diseases,

diagnose, monitor, treat or alleviate injuries or disabilities, or compensate for disabilities,

investigate or modify the anatomy, to replace parts thereof, or to investigate, modify or replace a physiological process,

control conception or make diagnoses in relation to conception.'

In addition to Swiss statutory provisions, EU regulations on medical devices must also be taken into account when examining whether software or digital health devices count as 'medical devices'.

Although the Mutual Recognition Agreement between the European Union and Switzerland (MRA) is formally still in force, the European Union is currently blocking an update of the MRA to take into account the new Medical Devices Regulation (MDR). In addition, there are fundamental differences in the interpretation of the MRA with regard to its application to CE certificates issued in Switzerland prior to the entry into force of the MDR. Unilateral recognition of CE certificates is currently warranted in Switzerland (under certain conditions). EU law on this topic therefore still plays an important role in this matter in Switzerland.

A vast array of further legislation can be relevant for certain aspects of digital health; in particular:

- the Federal Act on Data Protection;
- the Federal Act on Foodstuffs and Utility Articles;
- the Federal Act on Product Safety;
- legislation on intellectual property; and
- rules on advertisement in the Federal Act against Unfair Competition.

Law stated - 18 November 2022

Regulatory and enforcement bodies

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

Swissmedic is the Swiss authority responsible for the authorisation and supervision of therapeutic products. It is responsible, inter alia, for authorising and supervising clinical trials for medical devices and market surveillance.

The Federal Office of Public Health is the responsible authority for all issues related to the reimbursement by mandatory health insurance of the use, sale and lease of medical devices in therapeutic settings. It is also the regulatory body for the enforcement of transparency provisions in the TPA and of many laws and regulations potentially related to digital health applications (eg, stem cell research, genetic testing and protection against ionising radiation).

The Federal Data Protection and Information Commissioner is the official entrusted with supervising compliance with federal data protection legislation, applicable to data processing by federal bodies and private parties. The cantons may establish their own data protection authorities for the supervision of compliance with cantonal data protection legislation, applicable to data processing by cantonal and communal bodies.

Law stated - 18 November 2022

Licensing and authorisation

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

Digital health products are considered medical devices if they have a medical purpose; that is, they serve to:

- diagnose, prevent, monitor, treat or alleviate diseases;
- diagnose, monitor, treat or alleviate injuries or disabilities, or compensate for disabilities;
- investigate or modify the anatomy, to replace parts thereof, or to investigate, modify or replace a physiological process; or
- control conception or make diagnoses in relation to conception.

It is necessary and sufficient that the device has a medical purpose, irrespective of whether it actually has a (demonstrable) medical effect.

Pursuant to a Briefing Note of Swissmedic , software or apps do not qualify as medical devices if they are intended solely for fitness, well-being or nutrition (eg, diets), for hospital resource planning, reimbursement, management of doctors' visits, for the statistical analysis of clinical or epidemiological studies or registers, for use as a diary, to replace paper-based health data or if they constitute electronic reference works containing general non-personalised medical information. Nonetheless, the term 'medical device' is to be understood broadly. In a decision of 2018, the Swiss Federal Administrative Court decided that an app designed to measure the fertility of a woman by analysing her personal data qualifies as a medical device. In a further decision in 2022, the Federal Administrative Court confirmed that the same mobile app had to be classified as a Class IIb (under the then applicable provisions) medical device, in line with the practice of the EU authorities.

If the digital health product does not qualify as a medical device, it may still qualify as a utility article and be subject to the relevant legislation (the Federal Act on Foodstuffs and Utility Articles).

If the digital health product qualifies as a medical device, it needs to comply with the statutory requirements set out in the TPA and the Medical Devices Ordinance. If, among several modules or functionalities of a digital health product, only one is considered a medical device, only that module or functionality has to comply with the requirements applicable to medical devices.

The specific licensing and authorisation requirements depend on the classification of the relevant medical device. Depending on the classification, the manufacturer needs to work with a notified body to obtain a CE mark and, in some cases, needs to perform clinical evaluations or investigations.

Digital health services

There is a wide spectrum of digital health services and the regulatory rules applicable to them depend on each individual case. As a general rule and subject to individual circumstances, the provision of general information on health issues based on predefined reference materials is not specifically regulated in Switzerland. Conversely, providing medical advice in the individual case (eg, telemedicine) constitutes the exercise of a medical profession, which is reserved for persons who are allowed to exercise medical professions (ie, registered with the Swiss Register of Medical Professionals) and having sufficient knowledge of the relevant language.

The marketing of health services in general, and digital health services in particular, can be subject to special

regulations regarding advertisement, as well as strict obligations with regard to transparency and the prohibition of offering or accepting undue advantages.

Law stated - 18 November 2022

Soft law and guidance

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

Swissmedic adopted Information Sheet Medical Device Software in 2021, last updated in 2022, that provides guidance on the definition, classification and certification requirements for medical device software.

Among the non-governmental issued guidelines, it is worth noting the Swiss Medtech Code of Ethical Business Practices . This document is issued by Swiss Medtech (a Swiss association representing more than 600 companies) and aims at promoting an ethical medical technology industry.

Law stated - 18 November 2022

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?

Digital health products and services are subject to the general rules on contractual and tort liability.

Digital health products are subject to the Federal Act on Product Safety, which institutes a strict liability regime (ie, irrespective of any negligence or wilful misconduct on behalf of the manufacturer). Under the Act, the manufacturer of products is liable for death, personal injury and property damage that is a consequence of a faulty product. Not only the actual person or entity who manufactured the product, but also anyone who pretends to be the manufacturer, who puts its name or trademark on the product or imports the product for resale, lease or any other commercial purpose is deemed a manufacturer under this Act.

Law stated - 18 November 2022

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

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

According to established legal doctrine and court practice, health data is any information that (directly or indirectly) allows the drawing of conclusions on the physical or mental state of the health of an individual (namely, any medical findings following an examination and also if such finding is below the threshold of an actual diagnosis). As such, medical bills for treatments received or in certain instances also bills for medicines constitute health data. Under the Federal Act on Data Protection (FADP), which – together with the corresponding Data Protection Ordinance (DPO) – generally governs data processing by private parties and federal bodies, data on health is considered sensitive personal data. Under the revised FADP (which will enter into force on 1 September 2023, together with the revised DPO), genetic data and biometric data (which unequivocally identify an individual) will be added to the definition of sensitive personal data.

Although there is no statutory definition of anonymised (health) data, anonymisation is commonly understood to refer

to an irreversible process after which the data can no longer be linked to a specific individual (without disproportionate effort).

Several further federal acts and ordinances specifically govern the processing of health data, such as the Federal Act on Research involving Human Beings (HRA). The HRA, which applies to research concerning human diseases and the structure and function of the human body, defines health-related personal data as information concerning the health or disease of a specific or identifiable person, including genetic data (defined as information on a person's genes, obtained by genetic testing).

The HRA defines anonymised health-related data as health-related data that cannot be traced to a specific person (without disproportionate effort). The Human Research Ordinance further specifies that for the proper anonymisation of health data, all items that, when combined, would enable the data subject to be identified without disproportionate effort (in particular, the name, address, date of birth and unique identification numbers), must be irreversibly masked or deleted.

Law stated - 18 November 2022

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?

According to the FADP, health data benefits from a higher level of protection than regular personal data, as health data is considered sensitive personal data. Under the FADP, the processing of sensitive personal data is governed by special rules:

- private parties must register their data files (prior to operational use) with the Federal Data Protection and Information Commissioner (FDPIC) (as further set out in the DPO) if, among others, they regularly process sensitive personal data;
- disclosing sensitive personal data to third parties requires a justification (by, eg, express consent, overriding public or private interest or law); and
- active information duties apply if sensitive personal data are obtained or processed (such duties also apply where the data is collected from third parties).

Under the revised FADP, the duty to notify data files to (and register with) the FDPIC will be abolished and replaced by a general duty to maintain records of processing activities. Further, extensive processing of sensitive personal data will be determined as likely to lead to a high risk to an individual's personality or fundamental rights and thus, will require performing a data protection impact assessment (DPIA). If the DPIA indicates that the contemplated processing may be of a high-risk nature despite any measures taken, the FDPIC must be consulted prior to such processing.

Under the revised DPO, if sensitive personal data are processed on a large scale by automated means and if preventive measures cannot guarantee data protection, data logs must be kept (logging at least the saving, modification, reading, disclosure, deletion and destruction of the data). The log must provide information on the identity of the person who carried out the processing, the type, date and time of processing and, if applicable, the identity of recipients. The logs must be kept for at least one year and separately from the system in which the personal data is processed. The logs must further be accessible only to the bodies and persons responsible for verifying the application of the data protection provisions or preserving or restoring the confidentiality, integrity, availability and traceability of the data, and the logs may only be used for such purposes.

Also under the revised DPO, processing regulations for processing by automated means must be issued (and regularly

updated), if sensitive personal data are processed on a large scale. Such regulations must provide information on the internal organisation, data processing and control procedures as well as measures to ensure data security.

Under the HRA, if health-related personal data is further used for research, the consent of the persons concerned must be obtained at the time of collection, or they must be informed of their right to object. The HRA contains detailed provisions on such further use of genetic data and non-genetic health-related personal data as well as a transfer for purposes other than research, export and storage of health-related personal data. The Human Research Ordinance further contains detailed provisions on storage, measures for collection and further use of health-related personal data.

Law stated - 18 November 2022

Anonymised health data

Is anonymised health data subject to specific regulations or guidelines?

To the extent health data is truly anonymised (namely, subjected to an irreversible process after which the data can no longer be linked to a specific individual – without disproportionate effort), respective output data is no longer considered to constitute personal data. Consequently, general data protection laws no longer apply. This understanding is further corroborated by the revised FADP, which provides that personal data no longer needed should be destroyed or anonymised. However, the procedure of anonymising health data (or any other personal data for that matter) as such entails data processing and is thus, subject to the relevant data protection rules. That being said, contrary to European doctrine (according to which the anonymisation itself is considered to be a change of processing purpose requiring a justification), anonymisation (without retention of a copy of the original non-anonymised data) is treated in the same manner as a deletion (and thus requires no justification). Under the revised FADP, which explicitly treats destruction and anonymisation in the same manner and that further provides that personal data may be processed for purposes compatible with the initial purpose, anonymisation (even if a copy of the original non-anonymised data is retained) requires no justification (as such 'compatibility' with the initial purpose may be assumed in the case of anonymisation).

Pursuant to a provision in the HRA, the HRA does not apply to anonymously collected or anonymised health-related data.

Law stated - 18 November 2022

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 FDPIC is the federal data protection authority in Switzerland. Cantons may establish their own cantonal data protection authorities (which may supervise data processing by cantonal and communal bodies).

The FDPIC has no direct enforcement (or criminal or administrative sanctioning) authority. However, the FDPIC investigates on its own initiative or at the request of a third party if:

- methods of processing are capable of breaching the privacy of a large number of persons;
- data files must be registered; or
- there is a duty to provide information in connection with a cross-border data transfer.

To this end, the FDPIC may request files, obtain information and arrange for processed data to be shown. Based

thereon, the FDPIC may recommend that a certain method of data processing be changed or abandoned. Such recommendations are not binding but if they are not complied with or are rejected, the FDPIC may refer the matter to the Federal Administrative Court and, on appeal, to the Federal Supreme Court for a decision. Any such final decision is binding on the parties.

Under the revised FADP, the FDPIC will initiate, ex officio or upon notification, an investigation if there are sufficient indications that a specific data processing could violate data protection rules (unless such breach is of minor significance), and if such investigation reveals a violation, render binding administrative measures, including:

- that processing is fully or partially adjusted, suspended or terminated;
- that personal data is fully or partially deleted or destroyed; and
- in certain cases, disclosure abroad is deferred or prohibited.

Unlike most other European data protection authorities, the FDPIC still cannot impose any (administrative) fines.

Private parties are liable to a fine of up to 10,000 Swiss francs if they, among others, wilfully:

- fail to notify data files or in so doing provide false or incomplete information;
- provide the FDPIC with false information in the course of an investigation or refuse to cooperate;
- fail to inform on the collection of sensitive personal data; or
- breach the duty to keep sensitive personal data confidential.

Under the revised FADP, these (and many further) violations are subject to a fine of up to 250,000 Swiss francs.

Since the investigative possibilities of the FDPIC are limited (and fines can only be imposed by a court of law of competent jurisdiction), there are very few significant investigations (or sanctions) related to data protection violations. Accordingly, there have been very few notable 'enforcement' actions in relation to digital healthcare technologies.

One case in point is the Helsana+ case, in which the FDPIC recommended to a health insurance company that its app-based bonus program called Helsana+ (in which participants could perform activities to gather plus points, which could then be converted into cashbacks and other non-cash benefits) should not be used to collect or process any basic insurance data or to obtain consent to such collection and processing and that cashbacks should not be offered to participants who only had concluded the mandatory basic insurance. Since the recommendations were declined, the FDPIC brought the case before the Federal Administrative Court. The Court ruled that the consent obtained to collect personal data from the basic insurance service providers was not compliant with data protection law. However, the use of data lawfully obtained from policyholders who only concluded the mandatory basic insurance was found not to breach the FADP.

Another recent example is the FDPIC's investigation into the National Organ Donation Register (NODR) (an online register where registered users can enter their will for or against organ donation in the event of their death) operated by Swisstransplant, the Swiss Foundation for Organ Donation and Transplantation. Following a complaint by the persons responsible for a Swiss investigative TV programme, the FDPIC opened a formal fact-finding procedure concerning the NODR's electronic registration process. After it became apparent early on in the investigation that it was possible to register with the NODR under another person's name, Swisstransplant discontinued registration (initially with the intention of replacing it with a more secure online process but later indefinitely in light of the federal register that will replace the NODR, presumably by 2024). The NODR would still have been accessible to hospitals for a transition period, but registered users would no longer have had the possibility to change their expression of will and would only have been able to delete their accounts. The FDPIC had already issued its report when Swisstransplant decided not to accept any new registrations, making some of the recommendations obsolete. With the exception of two

recommendations to improve technical security, Swisstransplant accepted all remaining recommendations, which would have significantly reduced the operational risks associated with the NODR. The two rejected recommendations primarily referred to the abandoned registration process but a residual risk remained in relation to the account deletion process (accounts could have been deleted by unauthorised third parties). However, since Swisstransplant finally decided to permanently cease all operations of the NODR entirely, even such residual risk was no longer relevant.

Law stated - 18 November 2022

Cybersecurity

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

Switzerland has no dedicated cybersecurity laws. However, under the Federal Act on Data Protection (FADP), any personal data must be protected against unauthorised processing through adequate technical and organisational measures, as further specified in the Data Protection Ordinance (DPO), including:

- general measures to ensure confidentiality, availability and integrity of data to ensure an appropriate level of data protection. In particular, systems must be protected against unauthorised or accidental destruction; accidental loss; technical faults; forgery, theft or unlawful use; and unauthorised alteration, copying, access or other unauthorised processing. In assessing the adequacy of measures, the purpose of the data processing; the nature and extent of data processing; an assessment of the possible risks to data subjects; and the current state of the art must be taken into account. The measures must be reviewed periodically;
- special measures to be implemented, in particular for automated processing, including entrance, data carrier, transport, disclosure, storage, usage, access and input controls, each as further described in the DPO. Also, data files must be structured in a manner that data subjects are able to assert their rights of access and to have their data corrected;
- record-keeping, among others, with respect to automated processing of sensitive personal data if preventive measures cannot ensure data protection, in particular, if it would not otherwise be possible to determine whether data has been processed for the purposes for which it was collected or disclosed. The records must be stored for one year in a state suitable for auditing and be accessible only to those whose duty it is to supervise compliance with data protection regulations, and may be used only for this purpose;
- issuance of processing policy (if automated data files subject to registration with the Federal Data Protection and Information Commissioner (FDPIC) are used) describing internal organisation and data processing and control procedures and containing documents on planning, realisation and operation of the data file and information technology used – to be updated regularly and made available to the FDPIC (or the data protection officer, as applicable) upon request in a comprehensible form; and
- in the case of disclosure, notification of data recipient or recipients as to how up-to-date and reliable the personal data disclosed is, unless such information is evident from the data itself or the circumstances.

Under the revised FADP and revised DPO, the necessary level of protection must be determined and suitable technical and organisational measures (to be reviewed and adapted, as required) be implemented in a risk-based approach. Thereby, the types of processed data, purpose, type, extent and circumstances of data processing, risks to personality and fundamental rights, the current state of the art and implementation costs shall be considered. The revised DPO includes detailed provisions on the foregoing.

The FDPIC published the Guide for technical and organizational measures , which addresses data access (security of premises, server rooms and workspaces, identification and authentication, access rights), life cycle (data entry, recording, pseudonymisation and anonymisation, encryption, device security, data backup and destruction, outsourcing

of processing, security and protection) and transfer (network security, encryption and signing of messages, handover of devices, recording of data transfers) and access rights (individual right of data subjects concerned and replicability of procedures).

Law stated - 18 November 2022

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?

The disclosure of sensitive personal data requires the express consent of the data subjects concerned (or a justification by an overriding private or public interest or law). Since for most applications of digital health solutions, no justification seems apparent, a clear process should be established for obtaining express (and informed) consent from any individuals whose health data are disclosed. Further, internal policies should be put in place to address any requests made by individuals with respect to their health data and to set out how health data may be processed by employees or contractors of the digital health solution provider.

Although there is no respective legal requirement, to the extent an operational data protection officer (who meets the requirements set out in the FADP and the DPO) is appointed, the controller of data files is not required to declare its files to the FDPIC. Under the revised FADP, to the extent a data protection adviser (who meets the requirements set out in the revised FADP) is appointed, the consultation of such data protection adviser may replace the consultation of the FDPIC following a data protection impact assessment (DPIA), as applicable.

Since many new duties will be introduced by the revised FADP, it seems reasonable to already apply them to new digital health solutions, including:

- implementing privacy by design and by default (setting up technical and organisational measures to meet data protection regulations and data processing principles from the planning of the processing, which shall be appropriate with respect to the state of the art, type and extent of processing and associated risks; and ensuring through appropriate predefined settings that data processing is limited to the minimum required by the purpose, unless the data subject instructs otherwise);
- keeping records of processing activities (containing all relevant information and at least such information explicitly set out in the revised FADP);
- implementing a process for automated individual decisions, if any (inform individuals of any decisions solely based on automated data processing and having legal effects or significantly affecting him or her, whereby the affected individual may generally request to express his or her point of view and have the decision reviewed by a person);
- implementing processes to conduct DPIAs (whenever it appears that an envisaged processing activity is likely to lead to a high risk to an individual's personality or fundamental rights (eg, in the case of extensive processing of sensitive personal data, which will often be the case with respect to digital health solutions) and consult with the FDPIC (prior to such processing if the DPIA indicates that the contemplated processing may be of a high-risk nature despite any measures taken);
- implementing a process to address data breaches (data breaches that are likely to lead to a high risk to the personality or fundamental rights of the individual concerned must be notified to the FDPIC as quickly as possible. Where necessary for the protection of the individual or if requested by the FDPIC, the controller must also notify the respective individuals);
- implementing technical capabilities to retain data logs, as necessary;
- drawing up processing regulations, as necessary; and

- reviewing and adapting, as necessary, the technical and organisational measures in place.

The FDPIC published on its website guidelines on the processing of personal data in the medical field , which address the doctor-patient relationship including:

- processing and sharing of health data, access rights and data security (in particular access, device, transport, disclosure, storage, usage and input controls as well as logging or recording of automated processing and virus protection);
- electronic processing of medical records;
- electronic health cards;
- maintenance of hard and software containing health data; and
- processing of medical data for research, planning and statistics purposes.

The FDPIC further published guidelines on biometric recognition systems .

Law stated - 18 November 2022

INTELLECTUAL PROPERTY

Patentability and inventorship

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

With regard to digital health-related inventions, two main issues need to be taken into account. First, 'software as such' is, in principle, not patentable in Switzerland. To be patentable, the claimed software needs to have a technical effect that goes beyond normal physical interaction between software and hardware. Second, the European Patent Convention (to which Switzerland is a party) explicitly excludes 'methods for treatment of the human or animal body by surgery or therapy and diagnostic methods practised on the human or animal body', except for 'products, in particular substances or compositions, for use in any of these methods'. Given that a single step of treatment by surgery or therapy is sufficient to disqualify the invention from being patentable, a high degree of diligence is required when drafting the patent claims.

Inventions created by employees 'in the course of their work for the employer and in performance of their contractual obligations' belong automatically to the employer without further compensation being payable. Inventions created in the course of the employee's work – but not in the performance of his or her obligations – can be acquired by the employer if this was set out in the employment agreement and against payment of special compensation.

Law stated - 18 November 2022

Patent prosecution

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

Switzerland is a signatory State of the European Patent Convention and the vast majority of patents in force in Switzerland are granted by the European Patent Office (EPO). It is also possible to file patent applications in Switzerland with the Federal Institute of Intellectual Property (FIIP); however, under the rules currently in force, Swiss national patents are granted without being examined for novelty and inventive step.

There are no special prosecution rules for digital health technologies before the FIIP or the EPO.

Law stated - 18 November 2022

Other IP rights

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

The main IP right relevant in the context of digital health is copyright. The Federal Act on Copyright and Neighbouring Rights (CA) provides for the protection of literary and artistic works, which extends to software. Copyright in a work exists, and vests in its author, as from its creation without the need (or even possibility) to register it. The ordinary term of copyright protection is 70 years after the death of the author; copyrights in software expire 50 years after the death of the author.

Swiss law does not contain any provision regarding the ownership of copyrighted works created by employees, except for copyright in software. Therefore, in the absence of (explicit or implicit) contractual provisions, the general rule is that the copyright vests in the author of the work (ie, the employee). As regards software, the CA provides that the employer has the exclusive right to use any software that has been created by its employees in the course of discharging their professional duties or fulfilling their contractual obligations. However, employers and employees are free to agree on a different allocation of copyrights in employment agreements, subject to the general limitations on the assignment of moral rights (such as the right to be named as author).

Trade secrets and know-how are important assets in the context of digital health offerings (as in any technology sector), although they are not considered IP rights per se in Switzerland as they are not absolute rights. Note, however, that certain provisions in Swiss law prohibit specific conduct with respect to trade secrets and know-how (such as the Federal Act against Unfair Competition, Labour Law, Criminal Law and Corporate Law).

As in any other business sector, trademarks are also important. In Switzerland, trademark protection requires the registration of the sign with the FIIP. The term of the trademark protection is initially 10 years and can be renewed an unlimited number of times.

Law stated - 18 November 2022

Licensing

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

Under Swiss law, the licensing of IP rights is not subject to any formal requirements. In particular, the validity of licences is not subject to registration (but registration is possible with respect to IP rights that are registered, such as patents and trademarks) or to a written licence agreement. Nevertheless, it is common and recommended to enter into written licence agreements and to register the licence (considering that a licensee can otherwise not enforce its licence rights against a third party acquiring in good faith the concerned IP rights).

Further, if more than one party holds the IP right to be licensed, the consent of all co-owners is, in principle, required.

All IP rights (registered and unregistered) can be licensed in whole or in part. It is, therefore, possible (eg, to grant a licence only for one specific claim of a patent, for only one specific good claimed by a trademark or for only one specific exploitation right of copyrights in software. A licence can be exclusive, sole or non-exclusive, can be limited to a specific territory (competition law requirements have to be taken into consideration) or limited in time.

Law stated - 18 November 2022

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?

Enforcement of IP rights in digital health technologies is subject to the general rules of enforcement of IP rights. Patent infringement and validity cases are heard in the first instance before the Federal Patent Court for the entire country. Non-patent IP proceedings are heard in the first instance by the High Court or Appeals Court of the Canton that has local jurisdiction. The Federal Supreme Court is the only appeal instance in all IP proceedings.

In a recent case, the Federal Supreme Court had to decide a case involving a patent related to a ventilator for use in intensive care. The distinguishing feature of the invention was the presence of a screen showing an animated representation of the ventilated lung. The court had to opine on whether the animated representation of a ventilated lung on a screen contributes to solving a technical problem and thus must be taken into account when analysing the inventive step. The Court sided with the patentee and considered that this feature has a technical character because it provides information about the technical status of the ventilator and credibly assists the user in a human-machine interaction process.

Law stated - 18 November 2022

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?

Digital health products

There are no specific rules governing the advertising and marketing of digital health products. It will therefore depend on whether they qualify as a medical device.

Many digital health products can be qualified as class I medical devices, which are not subject to authorisation or approval by Swissmedic (or any other authority). A declaration to Swissmedic is, however, required if the medical device was not previously placed on the market in an EU country and it is provided in Switzerland by a Swiss company.

Some digital health products, such as fertility tracker apps, will be classified in higher classes and will be subject to stricter regulations (in particular, they may be subject to a mandatory conformity assessment by a notified body).

After placing such a product on the market, material vigilance requirements apply. The entity first putting such product on the market would have to report to Swissmedic material adverse events taking place in Switzerland (within certain specified deadlines depending on the severity of the event).

Advertising for medical devices is subject to the following rules:

- claims with regard to the use, performance and efficacy of medical devices for direct dispensing to the general public or direct use by the general public must be restricted to those contained in the product information only;
- misleading statements concerning the efficacy and performance of a medical device are prohibited; and
- advertising to the general public is prohibited with respect to medical devices that may be dispensed on medical prescription only or that are placed on the market for exclusive use by professionals.

Digital health services

There is a wide spectrum of digital health services and the regulatory rules applicable to them depend on each individual case. As a general rule and subject to individual circumstances, the provision of general information on health issues based on predefined reference materials is not specifically regulated in Switzerland. Conversely, providing medical advice in the individual case constitutes the exercise of a medical profession, which is reserved for persons who are allowed to exercise medical professions (namely, registered with the Swiss Register of Medical Professionals and having sufficient knowledge of the relevant language).

Specific advertising rules apply with respect to digital health services that are provided by health professionals. According to the Federal Act on Medical Professions – which applies to anyone providing services as a doctor, a dentist, a chiropractor, a pharmacist or a veterinary – provides that such professionals must refrain from any advertising that is not objective and that is not in the general interest. Further, such advertising must not be misleading or inconvenient.

General rules on advertising

In addition to the above, general rules on advertising in Switzerland apply to digital health products and services. In particular:

- misleading advertising is prohibited under Swiss law; and
- comparative advertising is permitted under Swiss law only to the extent that such advertising is not incorrect, misleading, unnecessarily injurious or imitative; in addition, comparative advertising must not have the effect of exploiting the reputation of a competitor's trademark (free-riding).

Law stated - 18 November 2022

e-Commerce

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

There are no special requirements concerning the formation of contracts online. Swiss law allows for contracts to be entered into by electronic means; this requires a manifestation of the parties' mutual assent to the contract's essential elements. The content of the acceptance must be identical to the offer, which requires that the customer be informed in detail about the offered product and the price. The intention to enter into a contract can be manifested, for example, by clicking on a 'yes' icon (in click-wrap agreements).

The Federal Act against Unfair Competition sets out certain rules a company or person offering goods or services by electronic means has to abide by. Under those rules, the company or person offering must:

- disclose its identity and contact details in full (including an email address), in a clear manner;
- outline the technical steps necessary to conclude the contract; in other words, the offeror must explain to her customer the purchase procedure that has been implemented (eg, step 1: confirmation of shopping basket, step 2: provision of payment details, step 3: a review of the order and payment details, step 4: purchase, step 5: confirmation of order; in practice, this is done in most cases by displaying a flowchart);
- provide the opportunity and technical means to identify and correct input errors before the order is placed (see step 3 above as an example); and
- confirm the order without delay by way of electronic communication (eg, a confirmation email).

Law stated - 18 November 2022

PAYMENT AND REIMBURSEMENT

Coverage

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

Digital health products and services – like all healthcare products and services – are reimbursed by mandatory health insurance if they are effective, useful and economical. The decision on reimbursement lies with the Federal Administration, in particular the Federal Department of Home Affairs and the Federal Office of Public Health.

This general obligation is put in concrete terms in the List of Materials and Objects published by the Federal Department of Home Affairs. The list includes generic descriptions of materials and objects deemed effective, useful and economical, along with the allowed medical indications and maximum reimbursement amounts. The current version of the list mentions several digital health products, such as, for example, transmitters for glucose level monitoring systems, including any necessary software. The list is updated regularly, and further innovative digital health products can be added over time.

Law stated - 18 November 2022

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?

Although Switzerland is not a member of the European Union, its law on medical devices follows EU law and the Mutual Recognition Agreement between the European Union and Switzerland (MRA) ensures that medical devices can freely cross the border between Switzerland and EU countries. As a result, new Regulation (EU) 2017/745 (the Medical Devices Regulation) (MDR) and Regulation (EU) 2017/746 (the In Vitro Diagnostic Medical Devices Regulation), which have been applicable since May 2021, led to a substantial revision of Swiss law to ensure continued equivalence with EU law.

Currently, although the MRA is formally still in force, the European Union is currently (still) blocking an update of the MRA to take into account the new MDR. In addition, there are fundamental differences in the interpretation of the MRA with regard to its application to CE certificates issued in Switzerland prior to the entry into force of the MDR. Unilateral recognition of CE certificates is currently warranted in Switzerland (under certain conditions).

Law stated - 18 November 2022

Jurisdictions

Australia	Gilbert + Tobin
Czech Republic	dubanska & co
France	Intuity
Germany	Ehlers Ehlers & Partner
India	Chadha & Chadha Intellectual Property Law Firm
Indonesia	ABNR
Ireland	Mason Hayes & Curran LLP
Israel	Naschitz Brandes Amir
Japan	Anderson Mōri & Tomotsune
Qatar	Al Marri & El Hage Law Office
South Korea	Bae, Kim & Lee LLC
Spain	Baker McKenzie
Switzerland	Lenz & Staehelin
Thailand	Baker McKenzie
United Kingdom	Latham & Watkins LLP
USA	Seyfarth Shaw LLP