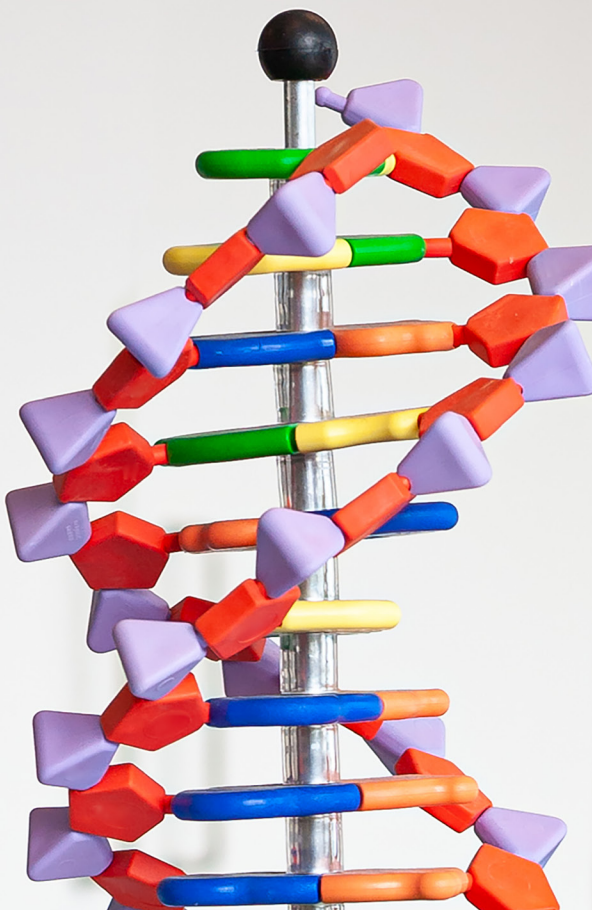
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Digital Healthcare 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers



Switzerland: Law & Practice
and
Switzerland: Trends & Developments

David Vasella
and Anne-Catherine Cardinaux
Walder Wyss Ltd

SWITZERLAND

Law and Practice

Contributed by:
David Vasella and Anne-Catherine Cardinaux
Walder Wyss Ltd

Contents

1. Digital Healthcare Overview p.5
1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics p.5
1.2 Regulatory Definition p.6
1.3 New Technologies p.6
1.4 Emerging Legal Issues p.7
1.5 Impact of COVID-19 p.7

2. Healthcare Regulatory Environment p.7
2.1 Healthcare Regulatory Agencies p.7
2.2 Recent Regulatory Developments p.8
2.3 Regulatory Enforcement p.11

3. Non-healthcare Regulatory Agencies p.11
3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies p.11

4. Preventative Healthcare p.13
4.1 Preventative Versus Diagnostic Healthcare p.13
4.2 Increased Preventative Healthcare p.13
4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information p.14
4.4 Regulatory Developments p.14
4.5 Challenges Created by the Role of Non-healthcare Companies p.14

5. Wearables, Implantable and Digestibles Healthcare Technologies p.14
5.1 Internet of Medical Things and Connected Device Environment p.14
5.2 Legal Implications p.15
5.3 Cybersecurity and Data Protection p.15
5.4 Proposed Regulatory Developments p.15

6. Software as a Medical Device p.16
6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies p.16

7. Telehealth p.18
7.1 Role of Telehealth in Healthcare p.18
7.2 Regulatory Environment p.19
7.3 Payment and Reimbursement p.19

8. Internet of Medical Things p.20
8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things p.20

9. 5G Networks p.20
9.1 The Impact of 5G Networks on Digital Healthcare p.20

10. Data Use and Data Sharing p.20
10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information p.20

11. AI and Machine Learning p.23
11.1 The Utilisation of AI and Machine Learning in Digital Healthcare p.23
11.2 AI and Machine Learning Data Under Privacy Regulations p.23

12. Healthcare Companies p.24
12.1 Legal Issues Facing Healthcare Companies p.24

13. Upgrading IT Infrastructure p.24
13.1 IT Upgrades for Digital Healthcare p.24
13.2 Data Management and Regulatory Impact p.24

14. Intellectual Property p.25
14.1 Scope of Protection p.25
14.2 Advantages and Disadvantages of Protections p.25
14.3 Licensing Structures p.25
14.4 Research in Academic Institutions p.25
14.5 Contracts and Collaborative Developments p.26

15. Liability p.26
15.1 Patient Care p.26
15.2 Commercial p.27

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today the firm has more than 250 legal experts in six offices in Switzerland's economic centres. It is fully integrated, adapts to clients quickly, and does not hide behind formalism. Walder Wyss Ltd is the first large Swiss firm with a strong focus on tech, including data protection. Its team is familiar with recent developments not only on an academic level but also with hands-on experience from a wide range of projects. Its health sector clients represent all relevant stakeholder groups – pharmaceutical, biotech and medtech companies (including start-ups in early-stage development phases), service providers ranging from individually practising physicians to large hospital and pharmacy groups, clinical research organisations, and health insurers. Its data and technology lawyers share the same team with their healthcare and life sciences colleagues, enabling the firm to quickly navigate the cross-sectional topic of digital healthcare.

Authors

David Vasella is a partner and co-head of Walder Wyss Ltd's regulated markets, competition, tech and IP team. He advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. David deals with cross-jurisdictional data protection projects, including GDPR implementation, data retention, e-discovery, cloud projects, digital marketing, online regulation, information technology and e-business matters. He also regularly advises in relation to commercial IP matters, regulated products and market practices. In addition, he frequently speaks and publishes in his areas of expertise. David is an editor of the Swiss journal for data law and information security, is CIPP/E certified, and is a member of the professional bodies IAPP and DGRI.

Anne-Catherine Cardinaux is an associate in Walder Wyss Ltd's regulated markets, competition, tech and IP team. She advises and represents clients in all areas of constitutional and administrative law and specialises in life sciences and health law. Recently, she advised on the health law requirements for cloud projects and assessed the implications of health apps qualifying as medical devices. Prior to joining Walder Wyss Ltd, she worked as a postgraduate in the legal department at the Basel headquarters of one of the world's largest pharmaceutical companies, as a law clerk at a Zurich district court and as a junior associate in the M&A team of a leading Swiss commercial law firm in Zurich.

Walder Wyss Ltd

Seefeldstrasse 123
PO Box
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss attorneys at law

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

Digital Healthcare as an Umbrella Term

The term "digital healthcare" or alternative notions of "electronic health services" and "Health 2.0" generally represent the sum of information technologies designed to increase the health, well-being or fitness of a given population or the efficiency of healthcare services – eg, by facilitating communication between healthcare providers (HCPs), healthcare organisations (HCOs) and patients. "Digital medicine" or "digital therapeutics" describes diagnostic, preventative or therapeutic attributes of information technologies. Digital medicine can thus be read as a subcategory of digital healthcare. The two terms are used in this article in this sense; "digital healthcare" will also cover digital medicine applications.

Differences Between Digital Healthcare and Digital Medicine

From a patient's perspective, digital healthcare technologies often encompass applications that generally inform about human health conditions, enable communication with HCPs, or are intended to increase patients' general well-being – eg, by encouraging an active lifestyle – whereas technologies belonging to the digital medicine realm will make claims of preventing, diagnosing or treating a human disease and improving the patient's medical condition.

From an HCP's perspective, digital healthcare primarily involves applications that increase service efficiency, such as teleconsultation or administrative case-management platforms, patient records or systems supporting the discovery of new therapies; while digital medicine applications form the object of, or influence, their medical decision-making and are subject to a corresponding duty of care.

From a regulatory perspective, digital medicine faces more stringent evidentiary requirements for substantiating medical claims and generally requires some form of clinical evaluation to be marketable in Switzerland.

Promises of Digital Healthcare

Besides improving access to healthcare and reducing inefficiencies, one of the promises of digital healthcare technologies lies in their ability to collect real-time data that can facilitate the generation of evidence required to inform medical decision-making. However, as in other

sectors, decision-making based on "real-time" or "real-world" evidence has pitfalls – using unfiltered data collected from use may perpetuate system bias and pose privacy concerns – risks that are only partly addressed in current Swiss regulation.

1.2 Regulatory Definition

Neither the notion of digital healthcare nor the term digital medicine is currently defined under Swiss regulatory frameworks.

No Comprehensive Regime

There is no comprehensive Swiss legislation on digital healthcare or digital medicine. Rather, aspects of health-related information technologies are generally qualified under each regulatory regime in view of each regulation's objectives.

Swiss legislation has a "technologically neutral" approach. Swiss laws only rarely address a specific technology. Depending on their functions, features and claims, digital healthcare and digital medicine may, for example, be subject to:

- professional practice and licensing requirements;
- provisions on therapeutic and diagnostic products;
- data protection and professional secrecy obligations;
- human (clinical or non-interventional) trial regulations;
- genetic testing legislation;
- laws on patient records;
- advertising restrictions;
- rules on the provision of benefits to HCPs, HCOs or patient organisations;
- (product-)liability regimes;
- telecommunications regulations; and/or
- public procurement provisions.

"eHealth" and "mHealth"

In 2018, the Swiss federal and cantonal administrations jointly adopted a "Swiss eHealth Strategy 2.0", where the terms "eHealth" and "mHealth" were defined. The strategy accompanied the roll-out of the electronic patient record (EPD). The term "eHealth" covers "all electronic health services that serve to network the actors in the health system". The current Strategy 2.0 draws on a previous "eHealth strategy Switzerland", which had led to the "mHealth recommendations" (dated March 2017). These recommendations define "mHealth" as "medical procedures, healthcare and preventative measures supported by wirelessly connected devices". Although the strategies and recommendations offer useful guidance, they have no regulatory qualification.

1.3 New Technologies

Digital healthcare and digital medicine are fuelled by general access to mobile devices equipped with high computing power and storage capacity, enabling real-time collection and processing of health-related data.

With increased connectivity, including wirelessly connected things (internet of things), the idea of healthcare ecosystems tailored to specific indications or conditions (such as diabetes, cardiac issues and depression) – designed to follow the entire treatment cycle from prevention and prediction to diagnosis, treatment, adherence and monitoring – is gaining momentum.

Concurrently, innovation is driven by increasingly sophisticated machine-learning and pattern-recognition technologies. Coupled with advances in genetic sequencing technologies, digital medicine applications promise to provide care tailored to an individual's genetic or physiological make-up and/or to increase diagnostic accuracy. Machine-learning algorithms in digital

healthcare technologies are used to identify new therapy candidates or improve patient triage efficiency.

1.4 Emerging Legal Issues

Important emerging legal issues in digital health include:

- cybersecurity/data protection;
- the limits of medical device and health profession regulation;
- cross-border provision of care;
- product liability for machine learning-enabled devices; and
- the reimbursement of new technologies under the mandatory social health insurance scheme.

In this cross-sectional matter, it is even more important to harmonise different regulations and ensure uniform practice. However, the legal landscape in the Swiss healthcare sector is characterised by high complexity in a field with many different players and responsibilities at all federal levels. The Swiss federal system (see **2.1 Healthcare Regulatory Agencies**) leads to a decentralised approach. This is amplified by health regulations that are not tailored to (or that are falling behind) digital health technologies.

There has been no holistic approach to healthcare data management either. Switzerland lacks a coherent and efficient environment for the lawful and secure further use of health data (see **2.2 Recent Regulatory Developments**).

1.5 Impact of COVID-19

Already in 2018 (two years before the outbreak of COVID-19), Switzerland ranked only 14th in the Digital Health Index, in a study by the Bertelsmann Foundation (a total of 17 EU and OECD countries were compared).

With the outbreak of the COVID-19 pandemic in February 2020, existing deficiencies in Switzerland's digitalisation became visible. Numerous shortcomings have been identified in the management of the COVID-19 pandemic, with the most obvious being that indicators needed to make decisions were incomplete.

In January 2022, the Federal Office of Public Health published a report on improving data management in the health sector. The report highlighted the measures that had been implemented during the pandemic and the areas where deficiencies still exist. Various national projects have followed the January 2022 report on improving data management in the health sector in the areas of health data, secondary use and data spaces (see **2.2 Recent Regulatory Developments**).

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

Switzerland is a federation with 26 states (cantons), one federal government and four official languages. The federal government is responsible for health insurance, medicines, medical devices and public health, among other things. The cantons are responsible for hospital planning or the licensing of service providers, and have a high level of competence for the organisation of their own healthcare system. By default, the cantonal health authorities implement and enforce not only cantonal but also national (health) laws.

Inter alia, Swiss cantonal health authorities have authority over medical professional practice and are competent to enforce professional licensing requirements. Their oversight touches upon digital health technologies that directly impact

on professional practice, such as platforms for telemedical services, and raises questions on the distinction between the provision of medical professional care and platforms acting as intermediaries to that care.

Swiss cantonal authorities are also competent by default to enforce the Swiss Therapeutic Products Act (TPA) governing medicinal products, medical devices and therapies directly linked to medicinal products or medical devices – eg, gene therapies. The cantonal competences under the TPA are superseded where the TPA accords express authority to the Swiss Federal Agency for Therapeutic Products (Swissmedic). Inter alia, Swissmedic is competent for market surveillance of medical devices and has authority over the marketability of medical devices. Digital medicine applications classified as medical devices within the meaning of the TPA may thus fall under both Swissmedic's and cantonal authorities' oversight.

Along with regional ethics committees, Swissmedic is also responsible for authorising certain categories of human (interventional) clinical trials with medical devices under the Swiss Clinical Trials Ordinance (eg, medical devices not yet bearing a conformity marking under medical devices regulations). Non-interventional studies with human subjects, including personal data, require an authorisation by the competent ethics committee under the Swiss Federal Human Research Act (HRA).

Swissmedic's and the cantonal authorities' competences under the TPA are complemented by competences of the Swiss Federal Office of Public Health (FOPH). Inter alia, the FOPH is also competent for granting certain authorisations under the Federal Act on Human Genetic Testing (HGTA) and for assessing the benefits of candidates for reimbursement under the general mandatory Swiss health insurance scheme.

2.2 Recent Regulatory Developments

To keep pace with evolving technologies in digital healthcare, the Swiss regulatory landscape is changing, in terms of substantive legal regimes and in the way in which regulatory authorities conduct market-surveillance activities.

Substantive Reform

In terms of substantive regimes, reforms are ongoing in patient records legislation, medical-device regulations, genetic testing and data protection laws.

Electronic patient dossier

In view of facilitating interoperability between HCPs, HCOs and digital healthcare applications, and with the aim of breaking up information silos, the Swiss legislature and regulators laid grounds for an electronic patient dossier (EPD) in 2017. The EPD is at the heart of the Swiss eHealth Strategy 2.0 and designed to integrate information derived from patient files kept by HCPs and HCOs, information entered by the patient, and mHealth applications connected to the records (see the definition of mHealth under **1.2 Regulatory Definition**). It functions as an overarching link between, and a gateway to, patient information stored locally on decentralised filing systems operated by certified EPD providers. Out of the more than 400 technical and organisational certification requirements, over 100 relate to data protection and data security. The EPD was rolled out gradually in the course of 2021.

Since 1 January 2022 (when health insurance legislation was changed) outpatient service providers must also join the EPD if they wish to provide services that are covered by mandatory health insurance.

For patients, the use of the EPD remains voluntary. They must give their consent with a two-factor authentication.

On 27 April 2022, the Federal Council informed the public that the EPD was to be developed further. It shall become an instrument of mandatory health insurance. All health professionals working in outpatient care shall be obliged to maintain an EPD. The Federal Council also plans access for research purposes with the consent of the persons concerned. It should also be possible to use the technical infrastructure of the EPD for additional services.

Medical devices ordinances

On 26 May 2021, the revised Medical Devices Ordinance (MedDO) entered into force; and on 26 May 2022 the new Ordinance on In Vitro Diagnostic Medical Devices (IvDO) also came into effect. This revision harmonised the Swiss regime with EU Regulations (EU) 2017/745 (MDR) and (EU) 2017/746 (IVDR).

Under the old regulations (the European MDD and old Swiss MedDO), and due to the mutual recognition agreement (MRA), medical devices that were placed on the market in Switzerland could be marketed in Europe with no barriers, and vice versa. However, the MRA has not been updated in line with the new regulations.

Switzerland is now a third country within the meaning of the MDR, and mutual recognition no longer exists. To access the EU market, Swiss manufacturers must designate an authorised representative domiciled in an EU member state (EU-Rep) and arrange for their devices to be placed on the market by an EU importer. According to the industry association "Swiss MedTech", efforts to meet third-country requirements will lead to initial costs representing 2% and yearly costs representing 1.4% of the total export volume.

The status as a third country also has major implications for market surveillance in Switzerland. Since Swissmedic lost access to EUDAMED, manufacturers, authorised representatives and importers must register with Swissmedic and request a "Swiss Single Registration Number", or CHRN, similar to the SRN in Europe. This is to ensure a market surveillance system in Switzerland. In future, devices will also need to be registered via Swissmedic. The deadlines and details for device registration have not yet been established. A system similar to EUDAMED is currently being set up in Switzerland.

For all other aspects, the Swiss medical device regulation remains closely intertwined with the MDR.

mHealth recommendations

mHealth applications (see the definition under **1.2 Regulatory Definition**) not falling under the regime on medical devices (eg, wearable sensors measuring vital parameters for fitness purposes) are subject to generic, non-healthcare-specific regimes on product safety. In view of addressing health-related risks inherent to mHealth applications, the Swiss regulators adopted recommendations and guidance for a self-declaration of mHealth apps based on quality criteria endorsed by the Swiss eHealth initiative. Both recommendations and guidance are designed as non-binding codes of practice increasing transparency and furthering the development of adequate quality standards.

Reform of data protection legislation

To account for the increased role and value of collecting and processing personal data, the Swiss legislature adopted a reformed Federal

Data Protection Act (FDPA), and a new Ordinance to the Federal Act on Data Protection (FDPO). The new legislation will enter into force on 1 September 2023. The new framework provides for, inter alia, increased transparency requirements while building on previous concepts of the Swiss data protection regime. In contrast to Regulation (EU) 2016/679 (the General Data Protection Regulation, or GDPR), the FDPA is based on the principle of permitted data processing with exceptions requiring justification (ie, consent, overriding interests or legal bases).

Human genetic testing

Further reforms affecting digital healthcare technologies include a revised regime on human genetic testing. The revised Law on Human Genetic Testing (GUMG), the Ordinance on Human Genetic Testing (GUMV) and the Ordinance on DNA Profiling in the Civil and Administrative Field (VDZV) entered into force on 1 December 2022. Depending on the genetic traits examined, genetic tests are regulated to different degrees. The strictest requirements apply to the use of genetic testing for DNA profiling and in the medical field.

No Swiss artificial intelligence law

Over the past three years, the Swiss government has responded to the increasing importance of AI, answered several parliamentary motions on the subject, published guidelines on risks and opportunities and convened expert panels, including the "Artificial Intelligence Competence Network". The position has so far been that there is no need for general regulation of AI, as the general legal framework in Switzerland is basically suitable and sufficient at the present time.

Switzerland is participating in the negotiations for an international convention on artificial intelligence (AI) as a member of the European Committee on AI (CAI), which was set up by the Council of Europe in 2022.

Swiss providers that place AI systems on the market or put them into operation in the EU are also covered by the territorial scope of the EU AI Act. Under the proposed AI Act, medical devices or in vitro diagnostic medical devices that are themselves an AI system or use an AI system as a safety component are covered by the MDR/IVDR and the AI Act. Furthermore, the AI Act applies to Swiss providers and users of AI systems if the result produced by the AI system is used in the EU. The so-called Brussels effect is likely to occur. Many Swiss AI providers will develop their products not just for Switzerland; meaning that the new EU standards of the AI Act should also become established in Switzerland.

Swiss health data space

On 4 May 2022, one day after the EU Commission had announced its plans for the European Health Data Space, the Federal Council informed the public that it wanted to enable better use of health data for research.

The planned health data space for Switzerland is only intended to serve research. This is in contrast to the European Health Data Space, which gives priority to promoting the empowerment of individuals in dealing with health data.

Currently, the Federal Department of Home Affairs is clarifying the requirements for the proposed system and its legal framework on behalf of the Federal Council.

Reform Impact

Among the regulatory reform projects underway, the new regulations on medical devices and the revised FDPA, as the most far-reaching revisions, are likely to have the greatest impact on

digital healthcare. Their impact is, however, not yet fully discernible, as respective enforcement practices have yet to be adopted.

The further development of the EPD and the plans on a Swiss data space do not seem to be co-ordinated or to follow a coherent strategy. Switzerland still lacks a coherent and efficient environment for the lawful and secure further use of (health) data.

Shifting Practices in Regulatory Oversight

Regulatory oversight has shifted procedurally and substantively – ie, in its focus. Changes are most apparent in digital medicine.

- Procedurally, Swissmedic largely communicates with economic operators via its online portal. Through the portal, it receives market surveillance notifications, applications for authorisations and regulatory documentation, and issues regulatory orders. It is also exploring ways of using machine-learning technologies to search for, analyse and validate scientific evidence or detect patterns or trends in reported adverse events. Swissmedic is in the process of evaluating benefits and risks of using AI technologies for assessing projects for, and the results of, clinical trials. As more scientific disciplines become necessary for an effective oversight, Swissmedic also faces increased complexity in its internal knowledge organisation.
- In terms of regulatory focus, Swissmedic and the FOPH are examining ways to address the trend in precision medicine. Swissmedic also aims at improving transparency on risks relating to digital medicine for patients and users – eg, hacking of insulin pumps or patient records.

2.3 Regulatory Enforcement

Key areas of enforcement are centred around applications causing or contributing to the highest health or privacy risks for patients or users. Thus, enforcement focus lies on high-risk digital medicine applications or other such technologies processing high quantities or a broad spectrum of health-related personal data.

Where authorities open investigations against economic operators, they are generally required to grant those operators a right to be heard, unless the suspected risks require immediate or covert action. Any action would have to be proportionate to the operators' legitimate interests. As a rule, prior to issuing any binding order, authorities will generally have to give addressees of any such order the opportunity to submit a defensive statement. Upon the issuing of a binding regulatory order, addressees have the right to take recourse before an instance specified in the applicable legal regime (eg, the Federal Administrative Court).

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

Certain digital healthcare technologies may be subject to generic, non-healthcare-specific legal regimes, such as telecommunications regulations, general product-safety regimes and competition laws.

Telecommunications Regulations

Digital healthcare technologies qualifying as telecommunications services within the meaning of the Swiss Telecommunications Act (TCA) fall under the Swiss oversight of the Federal Office

of Communications (OfCom) and have certain reporting, co-operation and documentation obligations under the Swiss Federal Act on the Surveillance of Post and Telecommunications (SPTA).

The TCA regulates the transmission of information and is aimed, inter alia, at ensuring cost-efficient, stable, competitive and accessible telecommunications networks in Switzerland. It defines telecommunications services as the transmission of information for third parties. As per guidance provided by OfCom, a telecommunications service provider (TSP) is a person who assumes responsibility for the transmission of end-user signals vis-à-vis end users or other TSPs.

In a decision in April 2021 and along the lines of the European Court of Justice's jurisprudence, the Swiss Federal Court held that an internet-based instant messaging app (such as Threema, Signal or WhatsApp) relying on internet access provided and administered by a third party (so-called over-the-top services, or OTT services) does not classify as a TSP. It follows that to be considered a TSP, digital healthcare technologies would have to exercise some form of control over the transmissions network (eg, through a feed-in interconnection agreement allowing users of an internet-based service to access mobile telephone numbers) or provide a contractual guarantee for the correct and uninterrupted transmission of user information.

OTT services enabling one-way or multi-path communication – eg, offering chat or other communication functions between HCPs and patients – may, however, qualify as providers of derived communication services within the meaning of the SPTA. Such providers of derived communication services face certain, albeit reduced, co-operation and reporting obligations in the surveillance of telecommunications networks.

Product Safety Laws

Digital healthcare technologies may also fall under non-healthcare-specific product safety laws. As a rule, products intended for consumer use are governed by the general requirements on product safety provided by the Swiss Federal Act on Product Safety (PrSG). Regulatory oversight lies with authorities specified in the Swiss Ordinance on Product Safety or other sector-specific ordinances.

By way of an example, wearables measuring vital parameters and wirelessly connected to other devices may need to observe essential health and safety requirements set out by the Swiss Ordinance on Telecommunications Installations. Oversight of the adherence to such essential health and safety requirements lies with the Swiss Federal Inspectorate for Heavy Current Installations.

Competition Laws

Oversight over compliance with the Swiss Cartel Act (CartA) lies with the Swiss Competition Commission. Digital healthcare platforms fostering the exchange of data between competitors (eg, HCOs competing for patients) that has the effect of co-ordinating competitive behaviour (such as setting prices) may fall within the realm of co-ordinated behaviour prohibited under the CartA. Furthermore, recent developments in the EU have spurred debates on whether violations of data protection laws may constitute an abuse of market power under the CartA. Depending on their specific functions, digital healthcare platforms may thus need to take competition laws into consideration.

Data Protection

The Federal Data Protection and Information Commissioner (FDPIC) is appointed to supervise federal bodies, advise private operators and enforce federal data protection law.

Cantonal "public bodies" are subject to cantonal data protection laws and an oversight by the cantonal data protection bodies. A vast number of HCOs qualify as "public bodies".

As the healthcare sector becomes increasingly digital and data-driven, the role of the data protection authorities becomes increasingly important, even though their reach, resources and resolve are not on a par with their European counterparts. Interaction or co-operation by the Swiss data protection authorities with other agencies is subject to alignment in each case and the delineation of authority is often blurry. For example, (only) some cantonal regulators have published extensive guidelines on the use of cloud services by "public bodies".

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

The Swiss healthcare system is based on three pillars of medical care: treatment, rehabilitation and care. Prevention and health promotion are less firmly anchored in the Swiss health system.

The FOPH defines "prevention" as an umbrella term for all measures that are intended to prevent the occurrence, spread or negative effects of health disorders, diseases or accidents. In the field of prevention, a distinction can be made between the following forms of prevention, depending on the timing of the measures:

- primary prevention aims to prevent diseases as far as possible;
- secondary prevention serves to detect diseases at an early stage; and
- tertiary prevention aims to mitigate the consequences of a disease.

A difference between the regulation of preventative and diagnostic medicine arises from the remuneration by the mandatory health insurance. In the case of diagnostic treatment, it is assumed that these medical services comply with the principle of effectiveness, expediency and economic efficiency, which are remuneration conditions. This does not apply to preventative medical services, and all such services are to be paid for by the mandatory health insurance only if specifically included in a list.

4.2 Increased Preventative Healthcare

A quarter of the Swiss population suffers from a non-communicable disease (NCD) such as cancer or diabetes. A healthy lifestyle and knowledge can reduce such diseases or ensure they do not occur. Therefore, care providers such as hospitals and independent health specialists increasingly involve preventative measures in their work for guiding ill people or those at higher risk of disease on how to improve health.

Certain measures of medical prevention are covered by the mandatory health insurance. The costs are paid by the health insurance for prophylactic vaccinations, examinations of the general state of health or the prevention of diseases, among other things.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

Lifestyle/Wellness Apps as Medical Device Software

The Swiss Competence and Co-ordination Centre of the Confederation and the Cantons (eHealth Suisse) published the "Guide for App Developers, Manufacturers and Distributors" together with accompanying "Checklists" in April 2022 to help distinguish between "lifestyle/wellness" (sic) products and medical devices. An app only measuring fitness or nutrition data or statistically evaluating clinical or epidemiological data does not qualify as a medical device (see **6. Software as a Medical Device**).

Data Protection

Personal health information, directly or indirectly allowing for insights into an identified or identifiable person's physical or mental health, is categorised as particularly sensitive data under the general data protection regime (see **10. Data Use and Data Sharing**).

Professional and Official Secrecy

HCPs and HCOs are subject to professional and/or official secrecy obligations. Disclosure of secrets (including personal health information of patients) to third parties is prohibited. It is only permissible if mandated or permitted on legal grounds or upon informed patient consent. In contrast, disclosure to auxiliary persons is permitted. IT service providers involved as auxiliaries (subordination) must maintain professional secrecy (see **10. Data Use and Data Sharing**).

4.4 Regulatory Developments

Prevention today is mostly a task for healthcare professionals and non-governmental organisations, such as organisations for the elderly and for cancer patients. Health insurance providers offer services aimed at prevention, but it is not a key task for mandatory health insurance providers, as noted previously. However, the National Strategy for the Prevention of Non-Communal Diseases (NCD Strategy) 2017–2024 aims to strengthen health promotion and increase disease prevention.

4.5 Challenges Created by the Role of Non-healthcare Companies

As there is no uniform legislation in the field of digital health, companies must comply with different laws and regulations depending on the sector affected by the new technology. While healthcare companies are used to the strict sectoral regulation in the healthcare sector and require their contract partners to comply with those regulations, non-healthcare companies are used to more liberal regulations. Therefore, it is particularly important for such companies to contractually agree on the clear distribution of regulatory responsibilities.

If medical advice is provided in individual cases – for example, in the context of telemedicine – this constitutes the exercise of a medical profession and is only permitted for persons with a professional licence.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

Switzerland's digitalisation is progressing more slowly than in other countries. Governmental digitalisation efforts in the health sector have so far focused on the EPD and the necessary interoperability.

This brings into contrast Switzerland's lively start-up scene in the field of digital health. As of mid-May 2023, the "Swiss Healthcare Startups" association alone had 624 start-up members. A majority of them are active in the medtech sector. Wearables, implantables and digestibles are part of the innovation palette that arises from this.

5.2 Legal Implications

Under Swiss law, there are no specific liability rules regarding digital health. In general, civil liability rules apply, especially tortious liability, contractual liability and product liability. Product safety law, which also covers digital health products, establishes strict liability. The manufacturer of products is therefore liable for death, personal injury and property damage resulting from the defectiveness of a product. A manufacturer within the meaning of the Product Safety Act is also anyone who claims to be a manufacturer or whose name or trade mark is affixed to a product. Those who import a product for the purpose of resale, rental or other commercial purposes also qualify as manufacturers.

Concerning the use of AI in healthcare, the liability of physicians must be assessed with regard to a possible breach of the physician's duty of care.

The attribution of liability between the various parties (especially manufacturers, healthcare institutions and healthcare professionals) must be contractually agreed upon.

5.3 Cybersecurity and Data Protection

Health data is considered sensitive personal data under data protection law.

Moreover, when people record data about themselves via fitness apps or wearables, they accumulate large amounts of data. There is a risk of loss of control, which increases the risks from a data breach. If third parties obtain information about health, the data subjects may suffer serious disadvantage.

Inherent in the use of data processing, including of AI, is the risk of unauthorised disclosure of personal data; in the case of AI, this may occur both during the training and the application phase. Added to this risk is the risk of manipulation of training data. Under the FDPA, any personal data must be protected against unauthorised processing through adequate technical and organisational measures, even though the law does not specifically require certain types of measures.

Cybersecurity risks in cloud computing are mitigated to an extent, though legal risks increase, in view of cross-border data transfers and the required transfer impact assessments.

To address these risks, contracts will usually require adequate security measures, and before data is shared with others, a vendor assessment is necessary or, at least, good practice. In addition, contracts will require breach notification, even though under the current FDPA there is no mandatory obligation to notify breaches to the FDPIC, and an obligation to communicate breaches to the data subjects only arises in exceptional circumstances. The revised FDPA (as of 1 September 2023) will introduce mandatory breach notification, largely in alignment with the GDPR.

5.4 Proposed Regulatory Developments

While the TPA provides the general legal framework regarding the manufacture, distribution and use of all medical devices, the MedDO contains a definition of medical devices. Other relevant laws include the FDPA, the FSA and the PrSG.

In addition, legislation on intellectual property and the Federal Act on Unfair Competition can be relevant.

The regulatory authorities in digitalised medicine are Swissmedic, the FOPH and the FDPIC. Swissmedic is responsible for the authorisation and supervision of clinical trials with medical devices and for market surveillance, and the FOPH regulates the reimbursement of costs in relation to medical devices by the OKP. The FDPIC is the supervisory body for compliance with data protection legislation (see **2.1 Healthcare Regulatory Agencies**).

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Definition of Medical Devices Under the MedDO

Based on the principle of harmonisation with EU medical device law, the current Swiss definition of medical devices mirrors the MDR.

In summary, and in line with the EU regulatory framework, a product, including software, is considered a medical device if it is intended by the manufacturer, inter alia, for the (medical) purpose of:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of a human disease, injury or disability;
- investigation, replacement or modification of the anatomy, or of a physiological or pathological process or state;
- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations; or
- controlling conception or making diagnoses in relation to conception (abbreviated definition).

Whether a product is intended for a medical purpose is determined in accordance with the manufacturer's design and claims, as expressed in the product's labelling, instructions for use, documentation and marketing materials. The qualification of a medical device is determined by a subjective-objective test, meaning that arbitrary disclaimers provided by the manufacturer will be deemed ineffective if they are inconsistent with the product's intended functions and objective presentation.

Medical Device Software

On 26 May 2021, Swissmedic issued a guidance document on standalone medical device software, including apps installed on wearable devices, and described practical examples of non-medical software ("Information Sheet on Medical Device Software"). Swissmedic prominently references the MDR guidance MDCG 2019-11, issued by the EU Medical Device Coordination Group (MDCG).

Software performing a certain degree of data processing tailored to individual patients with a view to achieving a medical purpose qualifies as a medical device. As a rule, the following functions do not qualify as medical in nature:

- storage and archiving;
- communication (flow of information from a source to a recipient);
- simple search; and
- lossless compression (ie, compression permits the exact reconstruction of the original data).

There are numerous software applications in the healthcare sector that are not medical devices. General software that does not go beyond imparting knowledge, such as a (non-personalised) information platform or electronic patient dossier, is not considered a medical device. An app only measuring fitness or nutrition data or statistically evaluating clinical or epidemiological data does not qualify as a medical device.

In contrast, an app that measures a woman's fertility by analysing personal data was qualified as a medical device by the Federal Administrative Court.

Software not intended to achieve a medical purpose on its own is not itself considered a medical device, but may fall within the scope of the medical device regime as an accessory to, or component of, a medical device (for example, if it drives or influences a medical device).

Apps recording or using the data of a specific person, though mainly to consolidate and summarise data, can be classified as non-regulated apps in the health sector. Such digital health products can then, despite not being subject to the TPA and the MedDO, be qualified as utility articles that must comply with the provisions of the Federal Act on Foodstuffs and Consumer Products (FSA).

Self-Regulatory Concept of the Medical Device Regime

As in the EU framework, the Swiss ordinances are characterised by a self-regulatory concept based on harmonised technical standards developed by industry organisations and endorsed by Swissmedic. Medical devices do not require a marketing authorisation. To be marketable, they must be marked with a specified conformity marking, which may only be affixed following a specified risk-based conformity assessment. Depending on the medical device's risk profile and corresponding classification, manufacturers must involve third parties in the conformity assessment of their devices – ie, notified bodies accredited by the competent accreditation organisation. Irrespective of their class, all devices must undergo a clinical evaluation procedure based on clinical evidence representative of their risk.

Machine Learning-Enabled Medical Device Software

Medical-device technologies based on adaptive machine-learning algorithms have been described as "black box medicine" due to their evolving "learning" output and opacity. Indeed, machine-learning algorithms are characterised by a certain lack of input-to-output traceability, a fact that poses a hurdle in clinical evaluation. Unlike other regulatory authorities in Europe, Swiss authorities have not yet issued guidance on evidentiary requirements for medical devices based on machine-learning technologies. Respective guidance will likely correspond to guidelines under the MDR and IVDR currently pending with the MDCG. Harmonised technical standards for the general safety and performance requirements specific to machine-learning algorithms have also not yet been endorsed by the Swiss regulators (see **2.2 Recent Regulatory Developments**).

New Market Entries

Software providers that offer software, or parts of a greater system, that qualifies as a medical device are not always mindful at the early stages of planning and development that many applications are caught by the regulatory regime. This tends to delay product development and increases costs. At the same time, the new medical device regime tightens requirements on

documentation, security, connectivity and maintenance, which not all newcomers are prepared to satisfy.

Maintenance (Updates)

According to the TPA, users of the medical device software have a duty to maintain the performance and safety of the medical device. They must follow the manufacturer's instructions for use for the maintenance of the device. The MedDo defines maintenance as "measures such as preventative maintenance, software updates, inspection, repair, preparation for first use and reprocessing for re-use or measures to keep a device in functional condition or restore it to functional condition". The maintenance must be carried out in accordance with the principles of a quality management system (QMS) and must be organised and documented appropriately.

On 12 May 2023, Swissmedic published its report on hospital inspections 2021/2022 and included a strong criticism therein. The maintenance by third parties (most smaller hospitals outsource their maintenance to external service providers) was the aspect most frequently criticised, namely in 84% of the inspections. In 42% of cases, the hospitals did not have an updated equipment inventory or overview of the status of planned maintenance operations by the third-party companies. In 58% of the inspected hospitals, the various maintenance processes and associated interfaces were poorly regulated and documented, and did not satisfy the requirements of an appropriate QMS. The systematic measurement, periodic reporting and continuous improvement of the quality of the internally provided maintenance operations using defined quality indicators were found to be lacking in 42% of the inspections.

It seems reasonable to assume that the maintenance of medical devices by outpatient care providers does not receive great attention.

7. Telehealth

7.1 Role of Telehealth in Healthcare

During the COVID-19 pandemic, the number of long-distance consultations increased sharply in all medical specialties. These were carried out via telephone or simple videoconferencing services. However, the pandemic did not result in the establishment of remote consultations; outside the "gatekeeper" basic insurance model, these have not been widespread. Besides the lack of tariffs, safety and liability concerns are often seen as inhibiting factors.

Apart from a few provisions in cantonal law and an accordingly varying degree of liberality towards telemedicine across the Swiss cantons, there is no telemedicine-specific legislation; telemedicine is thus subject to general rules governing conventional forms of healthcare.

Medical professional standards of care apply. According to the current code of professional practice of the Swiss Medical Professional Association (FMH), telemedical care conforms to professional standards, provided that, as a rule, treatment is not exclusively based on electronic communication or other forms of remote communication.

The current legal issues revolve around the cross-border provision of care and operating licence requirements for telemedical platforms employing or co-operating with physicians.

While the cross-cantonal provision of telemedicine is practically undisputed, licensing require-

ments for physicians and telemedical platforms providing remote services from EU/European Free Trade Association member states are subject to ongoing debate.

In principle, physicians based in the EU/EEA benefit from an exemption from cantonal professional operating licensing requirements. However, there is currently no jurisprudence or consensus in doctrine on whether telemedical services provided from EU/EEA states without cantonal licences would be subject to the limitation of 90 days per year provided for cross-border services based on the sectoral agreements between the EU and Switzerland. Arguably, the limitation only applies to a physical presence in Switzerland and does not extend to remote telemedical services. Nevertheless, the EU's notation of services also encompasses correspondence services, suggesting an according interpretation of the term under the sectoral agreements.

Similarly, jurisprudence has not yet been rendered on the question of whether, and to what extent, a physician's medical practice will be governed by foreign or Swiss professional standards (country of origin versus country of destination principle). Much like in the EU, an established practice and jurisprudence is lacking. Since Switzerland is not bound by the EU's patchwork of directives touching upon cross-border medical professional services, the Swiss regulators are not bound by an interpretation of these directives adopted under EU law.

In recent years, certain cantonal authorities have argued that telemedical platforms acting as intermediaries between physicians and patients would require cantonal operating licences and an establishment in Switzerland. Telemedical platforms thus have to consider whether they are defined as outpatient medical institutions within the meaning of health insurance law licensing provisions. If this is the case, they will only be admitted to providing services under the mandatory health insurance scheme if all their physicians would also (as individual physicians) meet the admission requirements. This can be a real stumbling stone. Physicians are required to have had three years of training at a Swiss continuing education institution (with exceptions) as well as proficiency in the official language of the canton that issued the operating licence for the institution (subject to a purpose-based interpretation, the destination of the remote counselling does not matter).

7.2 Regulatory Environment

During the COVID-19 pandemic, the medical professional association FMH partnered with a videoconferencing service, offering physicians its platform free of charge. Guidance issued by the FMH during the pandemic specifies that the responsibility for the use of messenger or video services lies with the respective physician. To aid decision-making in the choice of a service, the FMH published guidance listing the most common products for video consultations, including a risk assessment available on its website.

7.3 Payment and Reimbursement

The tariff structures for outpatient treatments are negotiated between tariff partners specified in the health insurance statutes – ie, representatives of health insurers and professional associations.

The applicable tariff (TARMED) currently lists only one position, "Telephone consultation by the specialist". However, this tariff item is strictly limited. As a rule, 20 minutes per session can be billed. For psychiatrists, there are separate specific tariff positions, which are also limited. During the COVID-19 pandemic, the respective

tariff positions were partially and temporarily adapted to account for the need for longer teleconsultations.

The outpatient tariff is to be modernised after almost 20 years; related negotiations are ongoing.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

The term "internet of medical things" (IoMT) refers to wirelessly connected sensors transmitting information to other objects in the healthcare ecosystem by way of machine-to-machine communication. Possible applications include inventory or occupancy management in HCOs or real-time monitoring of vital signs in patients.

A systematic roll-out of IoMT applications in healthcare will trigger and amplify general legal issues, including those previously mentioned, such as data privacy and data security, and will expose HCOs, HCPs and patients to new security risks such as hacking, hijacking and manipulation of digital assistants ("vulnerability by design" due to different, often low safety levels). Such risks may raise questions as to whether Swiss regulatory regimes address those risks sufficiently and whether the current criminal provisions are effective in combating related crimes.

The Swiss Federal Council (FC) published a report dated 29 April 2020 on security standards for internet of things devices that found that fragmented regulations across domestic jurisdictions may prove ineffective and lead to unintended market distortions. International coordination will be necessary.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

With transmission speeds approximately 100 times faster than 4G networks, the implementation of 5G may further accelerate the development of digital healthcare.

In telehealth, 5G has the potential to unlock the use of virtual reality technology or sensors to enable treating physicians to monitor a patient's vital parameters. One possibility further attributed to 5G is providing grounds for virtual computerised replication of a surgical procedure remotely controlled by a physician at the patient's site (as part of a vision termed the "tactile internet"). To achieve 5G's potential in remote surgical interventions, telecommunications providers will have to ensure very low latency and transmission priority in their networks, and healthcare providers will need to take care when drafting appropriate contractual provisions to address liability risks.

5G may also underpin treatment in disaster areas by enabling real-time tracing of large populations or facilitating inventory and supply management within HCOs.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

Using and sharing personal health information within the scope of the Swiss jurisdiction may be subject to parallel legal regimes, including:

- general data protection law;
- (medical) and/or (official) secrecy rules; and

• human research regulations.

General Data Protection Laws

Personal health information (PHI), directly or indirectly allowing for insights into an identified or identifiable person's physical or mental health, is categorised as particularly sensitive data under the general data protection regime (revision discussed under **2.2 Recent Regulatory Developments**).

Under the revised FDPA, processing PHI in breach of general principles on transparency, good faith, proportionality, data accuracy or data security, as well as transferring PHI to other controllers, requires a justification. Such justification may lie in:

• a legal basis allowing for such a transfer;
• data subject consent; or
• an overriding private or public interest.

As a rule, a justification is not necessary where a recipient acts as a processor on behalf of a controller and is subject to respective auditing and instruction rights.

Where consent is required for lack of other justification, it must be informed, voluntary and explicit. In principle, consent may be provided in any form, including orally or electronically. Where processing activities and purposes are not self-evident and reasonably transparent from the circumstances, consent must be based on adequate information detailing the respective processing purposes.

It is often difficult for healthcare customers to assess whether suppliers of emerging technologies are providing adequate cybersecurity – ie, using state-of-the-art technologies. Unsurprisingly, HCPs and HCOs often cite concerns about not meeting data protection and data security requirements as a reason for their reluctance to use today's digital opportunities.

PHI may be transferred abroad under the conditions set out in the FDPA. The USA, for example, does not provide an adequate data protection level within the meaning of the FDPA. In 2020, the Swiss FDPIC published a position paper concluding that a certification under the Swiss-US Privacy Shield no longer constitutes a sufficient basis for personal data transfers to the USA. An adequate data protection level must therefore be ensured by other means. In practice, this is achieved contractually, by concluding a data transfer agreement, typically using EU standard contractual clauses adapted to Swiss requirements with additional safeguards depending on a case-by-case analysis.

Anonymised and Encrypted (Including Pseudonymised) PHI

In principle, Swiss data privacy laws do not apply to anonymised data or object data unrelated to an identified or identifiable person. Like the GDPR, Swiss law is based on a relative qualification, meaning that data will be qualified as "personal" depending on whether the controller, processor or recipient of the data can relate that data to an identified or identifiable person using reasonable means. Conversely, data is considered anonymised where identification is practically impossible because it requires efforts prohibited by law or reasonably disproportionate to any interest in that identification, such that the person in possession of the data would not be expected to take any such means.

Where merging of multiple data sources leads to, or allows for, an identification of data subjects, the resulting personal data is subject to the data protection regime.

Data encrypted according to the current encryption standard, decipherable only to the person in possession of the relevant key, does not qualify as personal data regarding processing activities carried out on that encrypted data by a third party. To fall outside the scope of the general data protection provisions, the controller must ensure that only authorised persons have access to the decryption key and that data cannot be decrypted without the decryption key.

Professional and Official Secrecy

HCPs and HCOs are subject to professional and/or official secrecy obligations.

- The federal medical secrecy (Swiss Criminal Code, CC) applies to doctors, dentists, chiropractors, pharmacists, midwives, psychologists and the auxiliary of any of these persons. Auxiliary persons include, for example, nurses, medical practice assistants and occupational and physical therapists. In the case of other professional groups that also process health data, cantonal statutory confidentiality obligations may apply.
- Members of an authority and/or public officials and the auxiliary of any of these persons have an official secrecy obligation (CC). This covers both institutional and functional (ie, performance of public duties) public officials. Official secrecy obligations may apply – eg, in the case of health data processed by employees of a public hospital.

Disclosure of secrets (including PHI) to third parties is prohibited. It is only permissible if mandated or permitted on legal grounds (eg, written authorisation of the superior authority) or upon informed patient consent. Consent may be express, silent or by implied conduct. Implied conduct plays an important role in practice.

In contrast, disclosure to auxiliary persons within the meaning of these provisions is permitted.

- Doctrine and practice (most recently the FDPIC in particular) refer to IT service providers as auxiliary persons, if they support the physician in the performance of their work. If they can, in principle, access patient data, they must therefore maintain professional secrecy (and must be informed and obliged accordingly).
- The question of whether IT service providers (including foreign providers) can be auxiliary persons under official secrecy was discussed in an expert opinion from 16 September 2021 (on cloud use by the city of Zurich). It was confirmed that outsourcing was not illegal if done correctly. This requires that the IT service provider must be involved as an auxiliary (subordination).

(Human) Research Laws

The data protection provisions (recently revised, see **2.2 Recent Regulatory Developments**) in the Human Research Act (HRA), the Ordinance on Clinical Trials (ClinO) and the Human Research Ordinance (HRO) are lex specialis to general data protection provisions.

In deviation from the general data protection laws, the HRA does not recognise any research privilege that would make consent redundant. As a rule, the consent of the data subject is required. In certain cases, the absence of an objection is sufficient. In both constellations, an approval from the ethics committee is required.

- Biological material and genetic data may be further used for research purposes as follows:
  (a) in unencrypted form if the data subject gave informed consent (consent cov-

ers further use for one specific research project);
(b) in encrypted (pseudonymised) form if the data subject gave informed consent (consent covers further use for research projects in general); and
(c) in anonymised form (the absence of an objection after sufficient information allows for anonymisation).

- Non-genetic health-related data may be further used for research purposes as follows:
(a) in unencrypted form if the data subject gave informed consent (consent covers further use for research projects in general);
(b) in encrypted (pseudonymised) form in the absence of an objection after sufficient information (absence of objection covers further use for research projects in general); and
(c) in anonymised form (not regulated in the HRA).

Foreign data transfers of genetic research data are only permissible if they are carried out for research purposes and the data subject gave their informed consent. Non-genetic research PHI may be transferred abroad under the conditions provided in the FDPA.

Liability Risks

Violations may result in sanctions for the company as well as fines (up to CHF250,000) for natural persons. The authorities may conduct investigations or issue orders to restrict, modify or stop processing. The disclosure of data within the scope of professional confidentiality may result in additional sanctions. Only some intentional violations are punishable (eg, failure to inform about the processing, or use of a processor without proper appointment). Violations can also lead to civil liability (claims for damages).

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

While the systematic use of technologies based on intelligent (learning) algorithms is still largely experimental in digital therapeutics, machine-learning technologies are gaining ground in, for example, diagnostics, the discovery of new medicinal product candidates or pattern recognition of trends in side effects.

With many applications still at an experimental level, the Swiss regulatory regime has not kept pace with their growing potential. AI-specific Swiss regulations have not yet been adopted. As with medical device software (see **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies**), guidance on evidentiary requirements for general healthcare applications has not yet been set. AI-enabled and machine learning-enabled technologies are thus subject to general principles applicable to the respective product category.

Hence, the use of real-time or real-world data as training data and the according risk of perpetuating system bias is currently not specifically addressed under Swiss law, nor have data access regimes been specifically adapted to the machine-learning context and to the fact that machine-learning algorithms require significant amounts and ranges of training data to reach their full potential. The Swiss EPD is based on patient consent and is not designed to enable insights based on linking patient records.

11.2 AI and Machine Learning Data Under Privacy Regulations

The European Commission's proposed regulation on AI mainly regulates high-risk AI applications, including the use of AI in medicine. Such

applications will need to meet transparency requirements, among other requirements.

In Switzerland, general regulation of AI has so far been rejected, and no specific regulation is foreseeable, except that the FC adopted guidelines for handling AI by the federal administration in 2020. On 13 April 2022, the Federal Council took note of the report "Artificial Intelligence and International Rules" by the Federal Department of Foreign Affairs (FDFA). The report sets out various measures for allowing Switzerland to play an active role in shaping and contributing to an appropriate global set of AI rules.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

Where AI or machine-learning devices or software are designed to serve a medical purpose directed at an individual person, these devices may qualify as medical devices under the MedDO. When qualifying an e-health product as a medical device, the regulations on the conformity of medical devices must be observed. There are different approval and authorisation requirements, depending on the classification of a medical device. Each medical device must be assigned to a class before being placed on the market in Switzerland. Based on the intended purpose and depending on the risk potential of a medical device, classification can be made in Classes I, IIa, IIb and III. The revision of medical device law has led to a higher classification of mobile applications and thus to stricter regulation. Health apps are now regularly assigned to Class IIa. Medical devices that are assigned to Class IIa must, in particular, be assessed by an accredited conformity assessment body. In this regard, a risk assessment shall be carried out, determining the safety of the respective device.

In addition, developers must be mindful of increased expectations for security and data protection of customers and stakeholders and apply high standards in this regard.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

To support digital healthcare, HCOs need an adequate IT infrastructure suitable for integrating new technologies. Key features of digital healthcare build on connectivity between interoperable technologies. To ensure interoperability, the infrastructure must be based on common standards. These standards are still under development. In addition, secure and effective sharing of information relies on stable networks equipped with sufficient capacity. As with all systems enabling multiparty co-operation, security issues become particularly important, as does data and information governance.

13.2 Data Management and Regulatory Impact

Although the FDPA calls for data security measures that correspond to the state of the art, it does not specify the precise technical standards in more detail. The FDPO contains more detailed regulation, but no specific requirements for IT upgrades. Generally, similar requirements as for new software will apply, including privacy-by-design and privacy-by-default requirements.

14. Intellectual Property

14.1 Scope of Protection

Under Swiss law, computer programs may be protected by non-registrable copyrights. Unlike in other jurisdictions, commercial intellectual property rights to such computer programs are freely assignable. According to the currently prevailing opinion in doctrine, associated moral rights, such as the right to be named as an author, are non-transferrable, but may be waived. Arguably, their exercise may also be delegated to third parties.

Software as such is not patentable. However, inventions may be patentable provided they have a technical implementation.

The question of how inventions and works of authorship created by AI-based technologies are allocated has not yet been decided. Like the European Patent Office, the majority in doctrine argues that inventorship in patent law – and authorship in copyright law – can only be attributed to natural persons.

14.2 Advantages and Disadvantages of Protections

Patents provide an exclusive right to use the invention commercially, including manufacturing, marketing, importing and exporting. However, private use, research and teaching remain permitted for anyone.

Literary and artistic intellectual creations of an individual character, including computer programs, are subject to copyright protection, regardless of their value or purpose. Such creations are automatically protected. The author has an exclusive right in their own work and the right to recognition of their authorship.

Trade mark and design legislation protects branding but not, generally, the function of products or services.

Switzerland does not have any specific trade secret laws except provisions in criminal and unfair competition law and obligations of secrecy in certain types of contracts. Not being an EEA member state, Switzerland has not implemented the EU Trade Secrets Directive.

14.3 Licensing Structures

There are no formal requirements regarding the licensing of IP rights under Swiss law. Nevertheless, it is customary and advisable to enter into a written licence agreement and to register the licence (otherwise a licensee cannot enforce its licence rights against a third party who acquires the intellectual property rights in question in good faith).

14.4 Research in Academic Institutions

Under Swiss general contract laws, designs and inventions conceived or reduced to practice in the performance of an employment agreement belong to the employer. A similar provision is stipulated for computer programs protected by copyrights under the Copyright Act. According to this provision, the employer shall have exclusive rights of use in a computer program created by its employee in the course of the performance of the employee's contractual obligations.

Where private sector technology companies are involved in developing a device or medical innovation, intellectual property rights are often allocated to the private sector company funding the research. In practice, research institutions often reserve the right to use intellectual property developed during the collaboration for non-commercial purposes. In some cases, such

a reservation may be mandated under competition law considerations.

Competition law considerations also play an important role in licensing agreements. For example, contractual clauses creating an obligation on the licensee to assign or grant an exclusive licence to a licensor (or a third party designated by the licensor) for any improvements made on the licensed technology require careful assessment.

14.5 Contracts and Collaborative Developments

Given the strictures imposed by intellectual property statutes for multiparty inventions and works of authorship, contractual arrangements often regulate cross-licences in background intellectual property rights, and the allocation of (joint or separate) ownership in foreground intellectual property. Best practice includes fine-tuning the allocation of intellectual property rights to the specific needs of the parties and an awareness that intellectual property allocation is not an issue that should be left to lawyers, but requires business buy-in and alignment with the broader strategies of the parties.

15. Liability

15.1 Patient Care

General Principles of Liability

Liability for patient care can be based on:

- the Swiss Product Liability Act (PLA), establishing strict liability for defective products modelled after the EU's Product Liability Directive 85/374/EEC (PLD);
- contractual provisions governed by the Swiss Code of Obligations (CO); or
- the CO's general regime on torts.

In contrast to the PLA, liability under the CO generally requires negligence, with the onus of proof lying on the claimant or the defendant, depending, in principle, on whether damages are sought under contract or tort. While strict liability under the PLA cannot be excluded, liability under the CO can be limited to gross negligence and intentional misconduct.

Liability for AI-Enabled Products

As part of an assessment on the need for regulatory reform tailored to AI technologies, the FC entrusted a working group under the auspices of the Swiss Federal Department of Economics, Education and Research with analysing the Swiss regulatory landscape. In its report, the working group held that the current Swiss liability legislation is broad enough to accommodate liability risks emanating from AI. Following the report, the FC concluded that new regulations addressing liability for AI are currently not a priority.

However, spurred by a project to revise the EU's PLD, multiple scholars in doctrine have recently argued for a revision of the Swiss PLA. Referencing an ongoing international debate, they identify three risks inherent to AI:

- the risk derived from the fact that, by definition, AI systems exercise a certain degree of autonomy;
- risks related to their interaction with humans training the AI; and
- their interdependence with other systems – eg, healthcare ecosystems.

Arguments for a revision project are centred on:

- the definition of a product defect and causality;

- the allocation of responsibility between manufacturers and users (risk governance); and
- the burden of proof.

Under the present regime, robots are not endowed with a legal personality; liability lies with a natural or legal person responsible for the damages caused by such robots. Whether the responsibility is with the manufacturer marketing a product or the user training a product with user data depends on an allocation of risks between the manufacturer and the user and the definition of a product defect. Much like the EU's PLD, the Swiss PLA defines product defects referencing the legitimate safety expectations of the public. These expectations are shaped by industry standards. Much will thus depend on the development of adequate standards by standardisation committees, such as the International Organization for Standardization and the International Electrotechnical Commission. Where users play an integral role in training an AI post-market, the manufacturer's influence on compliance with such standards is significantly reduced. Two of the suggestions for reform brought forward in doctrine therefore include provisions on strict liability of users training the devices and/or mandatory insurance schemes.

There are no concepts under Swiss law that specifically address AI and potential bias. Generally, the use and outcomes of AI are attributed to the party or parties that make use of AI-enabled systems. With respect to end-user data, the revised Swiss data protection regime (likely entering into force by 1 September 2023) requires the controller(s) to inform users about automated decisions, where these could have a substantial adverse effect on end users, and allows them to challenge the decision and have it reviewed by a natural person.

15.2 Commercial

Damages for harm incurred by an HCO due to disruptions in the commercial supply chain caused by third-party vendors' products or services will often depend on contractual arrangements between the HCO and the seller or service provider, and on the latter's arrangement with third-party vendors. Should damages from the direct contractual partner of HCOs be unattainable for legal or other reasons, Swiss jurisprudence has established principles regarding:

- third-party liquidation;
- the concept of a contract with a protective effect in favour of third parties;
- enabling liquidation of damages suffered by a non-contracting party; or
- a reversal of the onus of proof under the principle of producer liability in tort.

Whether and which of these principles applies will depend on the specific facts of the case.

Another way in which HCOs may safeguard their interests includes by securing indemnity undertakings from their direct contractual partners.

Trends and Developments

Contributed by:
David Vasella and Anne-Catherine Cardinaux
Walder Wyss Ltd

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today the firm has more than 250 legal experts in six offices in Switzerland's economic centres. It is fully integrated, adapts to clients quickly, and does not hide behind formalism. Walder Wyss Ltd is the first large Swiss firm with a strong focus on tech, including data protection. Its team is familiar with recent developments not only on an academic level but also with hands-on experience from a wide range of projects. Its health sector clients represent all relevant stakeholder groups – pharmaceutical, biotech and medtech companies (including start-ups in early-stage development phases), service providers ranging from individually practising physicians to large hospital and pharmacy groups, clinical research organisations, and health insurers. Its data and technology lawyers share the same team with their healthcare and life sciences colleagues, enabling the firm to quickly navigate the cross-sectional topic of digital healthcare.

Authors

David Vasella is a partner and co-head of Walder Wyss Ltd's regulated markets, competition, tech and IP team. He advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. David deals with cross-jurisdictional data protection projects, including GDPR implementation, data retention, e-discovery, cloud projects, digital marketing, online regulation, information technology and e-business matters. He also regularly advises in relation to commercial IP matters, regulated products and market practices. In addition, he frequently speaks and publishes in his areas of expertise. David is an editor of the Swiss journal for data law and information security, is CIPP/E certified, and is a member of the professional bodies IAPP and DGRI.

Anne-Catherine Cardinaux is an associate in Walder Wyss Ltd's regulated markets, competition, tech and IP team. She advises and represents clients in all areas of constitutional and administrative law and specialises in life sciences and health law. Recently, she advised on the health law requirements for cloud projects and assessed the implications of health apps qualifying as medical devices. Prior to joining Walder Wyss Ltd, she worked as a postgraduate in the legal department at the Basel headquarters of one of the world's largest pharmaceutical companies, as a law clerk at a Zurich district court and as a junior associate in the M&A team of a leading Swiss commercial law firm in Zurich.

Walder Wyss Ltd

Seefeldstrasse 123
PO Box
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss attorneys at law

Introduction

The COVID-19 pandemic highlighted the potential of digital technologies for tackling global health challenges. It also propelled a health technology boom in some countries.

However, digitalisation of healthcare in Switzerland is progressing more slowly than in other countries.

- Although Switzerland has required the introduction of an electronic patient record (EPD) by law since 2017, until recently this only applied to inpatient service providers. For patients, the use of the EPD remains voluntary.
- Remote monitoring of chronically ill patients is mostly limited to pilot programmes, partnerships and research studies by healthcare providers, technology companies and insurers.
- Remote consultations outside the "gatekeeper" basic insurance model have not been widespread.
- There are some partnerships regarding digital therapies. Selected disease-specific apps have been introduced. In addition, a consortium of insurers and providers launched the first digital health platform called "Well" in 2021. Switzerland has yet to include digital therapies in standard care and to support their reimbursement.

eHealth Suisse, which is supported by the federal government and the cantons, refers to a recently published report by the Swiss Health Observatory (OBSAN) on the study entitled "Physicians in Primary Care – Situation in Switzerland and in International Comparison". The report concludes that Switzerland is still lagging far behind in the digital transformation of the healthcare system by international standards. This is particularly noticeable in the eHealth offering for patients and in interprofessional co-ordination.

The slow digitalisation of healthcare stands in contrast to the innovation taking place at a fast pace in the country. Switzerland has a lively start-up scene in the field of digital health. In particular, the École Polytechnique Fédérale de Lausanne (EPFL) and the Swiss Federal Institute of Technology (ETH) in Zurich are innovation drivers. Start-up incubators and government-funded programmes also foster innovation. There is a very active investor scene, consisting of both traditional venture capital and private equity, as well as of large industrial companies.

Causes for slow digitalisation in Switzerland

Some causes are systemic, and solutions cannot be expected overnight. In the context of digital health, there has been no actual political leadership in the past. The Swiss health system has many different actors and responsibilities at all federal levels. This results in a fragmented stakeholder landscape. The legal landscape is characterised by a high degree of complexity, and regulations are implemented through a decentralised approach. This is increasingly evident in health regulations that are not tailored to digital health technologies.

There is also no holistic approach to health data management. Switzerland lacks a coherent and efficient environment for the legitimate and secure re-use of health data.

Recent Regulatory Developments in Terms of Health Data

The COVID-19 pandemic made the health data regulatory deficiency visible in Switzerland. Research, industry and politicians are increasingly commenting on the problem, with "isolated solutions" and "data silos" often being mentioned as keywords.

Since the pandemic, a lot has been happening in terms of health data, secondary use and data spaces. Various reports have been written and projects launched at the federal level. In April 2022, the Federal Council gave information on its plan to develop the EPD further – ie, that it shall become an instrument of mandatory health insurance, and all health professionals working in outpatient care shall be obliged to maintain an EPD. The Federal Council also plans access for research purposes with the consent of the persons concerned.

It should also be possible to use the technical infrastructure of the EPD for additional services. On 4 May 2022, one day after the EU Commission had announced its plans for the European Health Data Space, the Federal Council informed the public that it wanted to enable better use of health data for research.

It seems, however, that the various projects are not especially co-ordinated with each other. A coherent strategy or a comprehensible data and digitalisation policy is not in place.

Among the ongoing reform projects likely to impact the most on innovators in healthcare are the two new medical device ordinances, mirroring the EU MDR and IVDR, and the reformed data privacy regime set out in the Federal Data Protection Act (FDPA) and its implementing ordinance. These two reform projects are dealt with in more detail below.

Reform of the Medical Devices Regime

On 26 May 2021, the revised Medical Devices Ordinance (MedDO) and on 26 May 2022 the new Ordinance on In Vitro Diagnostic Medical Devices (IvDO) entered into force. This revision harmonised the Swiss regime with EU Regulations (EU) 2017/745 (MDR) and (EU) 2017/746 (IVDR).

For the past two decades, Swiss and EU manufacturers of medical devices have benefited from mutual market access thanks to a mutual recognition agreement (MRA) between Switzerland and the EU. Due to the failed negotiations between the EU and Switzerland on the institutional framework agreement, the MRA has been suspended for classical medical devices since 26 May 2021 and for in vitro diagnostic medical devices since 26 March 2022.

As a result, Swiss manufacturers of in vitro diagnostic medical devices are now treated as established in a third country, and must appoint an authorised representative based in the EU and label products accordingly. In addition, the European Commission clarified on 24 May 2022 that Swiss certificates of conformity will not be recognised in the EU, even if the certificate of conformity was issued before 26 May 2022.

This contrasts with the legal regulation of imports into Switzerland, which stipulates that EU certificates of conformity continue to be recognised. In particular, the provisions on the unilateral recognition of EU certificates of conformity are intended to reduce disruptions in the supply of in vitro diagnostic medical devices in Switzerland. Supplementary requirements such as the registration of economic operators and the reporting of serious incidents to the Swiss Federal Agency for Therapeutic Products (Swissmedic), as well as the establishment of a so-called Swiss authorised representative for foreign manufacturers, help to ensure that Swissmedic can maintain market surveillance despite being excluded from the network of EU authorities.

As there is no access to the European database EUDAMED, Swiss economic operators (manufacturers, importers and authorised representatives) must register with Swissmedic. This requirement may lead to EU manufacturers not being prepared to disclose the entire technical documentation to the Swiss authorised representative (especially where importers wish to assume the role of authorised representative for several manufacturers) (business secrets) and therefore preferring not to place the product on the Swiss market. To counteract a possible supply gap in Switzerland in such a case, as an alternative to keeping a copy of the technical documentation available at the authorised representative's premises, the foreign manufacturer is also permitted to send the data directly to Swissmedic.

In terms of digital healthcare, the medical device reform will affect software with an intended medical purpose defined in the MedDO, as well as software driving or influencing a medical device. By contrast, digital healthcare technologies providing, for example, generic non-tailored health or nutrition information, or mobile applications processing sensor data solely for fitness or wellness purposes, would fall outside the MedDO's scope. To guide app developers and help them navigate regulatory qualification, the Swiss regulators have endorsed recommendations and a catalogue of quality criteria for mHealth applications.

Revised Data Protection Act

In view of adapting the Swiss data protection regime to the digital age and to account for the pivotal role of personal data, the Swiss legislature has enacted a revised FDPA, which will come into force on 1 September 2023. The FDPA is largely aligned with Regulation (EU) 2016/679 (the General Data Protection Regulation, or GDPR), but with some significant deviations. The FDPA will be accompanied by a revised ordinance to the FDPA (FDPO). Inter alia, the revised regime increases transparency requirements and liability risks for controllers.

As under the GDPR, personal health information (PHI) belongs to a special category of personal data requiring an elevated level of protection and security. While the definition of PHI under the revised FDPA will not change fundamentally, the definition will be supplemented with additional categories of genetic data and biometrical data "uniquely" identifying a natural person.

Inter alia, current debates are centered around foreign transfers of PHI. Following the decision of the European Court of Justice in re Schrems II, the Swiss Federal Data Protection and Information Commissioner (FDPIC) considers that a certification under the Swiss–US Privacy Shield no longer justifies transfers of personal data to the USA under the FDPA. Thus, transfers must be based on other means – eg, data transfer agreements. Most importantly, the revised standard contractual clauses (SCCs) passed by the European Commission on 4 June 2021 have been recognised by the FDPIC. However, according to the FDPIC, the new EU SCCs only allow the transfer of personal data to states without adequate protection "if the necessary adaptations and additions are made for use under Swiss data protection law". From a Swiss perspective, exporters would therefore have to slightly amend the respective SCCs (with Swiss additions). In addition, data transfer agreements must be accompanied by a transfer impact assessment and potentially by supplementary technical or organisational measures.

Switzerland is regarded as a "third country" from the EU's perspective. However, the European Commission decided on 26 July 2000 that Swiss law provides adequate protection of personal data, and therefore that data transfers from member states to Switzerland are, in principle, permitted. Switzerland's level of data protection is now subject to review for the first time in two decades, and for the first time under the GDPR. A new adequacy decision was originally expected by 2020. However, the decision was postponed, and the EU decision on the continued recognition of the adequacy of Swiss data protection legislation is still pending.

Regulatory Aspects on the Horizon

Regulatory aspects on the horizon include questions on:

- the cross-border provision of medical care;
- product liability and evidentiary requirements for machine learning-enabled devices;
- data access rights unlocking research and innovation;
- interoperability standards; and
- reimbursement of new technologies under the mandatory statutory health insurance scheme.

The soon-expected introduction of the tariff for outpatient services will be of great importance. It has been modernised after 20 years and should better reflect technical developments.

As a market intertwined with the EU, Switzerland follows developments in the EU's regulatory landscape closely, while generally keeping a pragmatic and liberal approach to regulation. In Switzerland, the position has so far been that there is no need for general regulation of AI, as the current general legal framework in Switzerland is basically suitable and sufficient. In particular, the view is expressed that no general AI law should be created, but that sector-specific and technology-neutral regulation should be examined in Switzerland. Moreover, with data protection, Switzerland already has a regulation that covers AI. In particular, the revised FDPA stipulates that data subjects have a right not to be judged by an AI when making important value decisions.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com