



Chambers Global Practice Guides

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

Digital Healthcare 2022

Switzerland: Law & Practice
and
Switzerland: Trends & Developments

David Vasella, Michael Isler and Anne-Catherine Cardinaux
Walder Wyss Ltd

practiceguides.chambers.com

SWITZERLAND

Law and Practice

Contributed by:

David Vasella, Michael Isler and Anne-Catherine Cardinaux
Walder Wyss Ltd see p.23



CONTENTS

1. Digital Healthcare Overview	p.4	6. Software as a Medical Device	p.12
1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics	p.4	6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies	p.12
1.2 Regulatory Definition	p.4	7. Telehealth	p.14
1.3 New Technologies	p.5	7.1 Role of Telehealth in Healthcare	p.14
1.4 Emerging Legal Issues	p.5	7.2 Regulatory Environment	p.15
1.5 Impact of COVID-19	p.6	7.3 Payment and Reimbursement	p.15
2. Healthcare Regulatory Environment	p.6	8. Internet of Medical Things	p.15
2.1 Healthcare Regulatory Agencies	p.6	8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things	p.15
2.2 Recent Regulatory Developments	p.7	9. 5G Networks	p.16
2.3 Regulatory Enforcement	p.8	9.1 The Impact of 5G Networks on Digital Healthcare	p.16
3. Non-healthcare Regulatory Agencies	p.8	10. Data Use and Data Sharing	p.16
3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies	p.8	10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information	p.16
4. Preventative Healthcare	p.10	11. AI and Machine Learning	p.18
4.1 Preventative Versus Diagnostic Healthcare	p.10	11.1 The Utilisation of AI and Machine Learning in Digital Healthcare	p.18
4.2 Increased Preventative Healthcare	p.10	11.2 AI and Machine Learning Data Under Privacy Regulations	p.18
4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information	p.10	12. Healthcare Companies	p.19
4.4 Regulatory Developments	p.11	12.1 Legal Issues Facing Healthcare Companies	p.19
4.5 Challenges Created by the Role of Non-healthcare Companies	p.11	13. Upgrading IT Infrastructure	p.19
5. Wearables, Implantable and Digestibles Healthcare Technologies	p.11	13.1 IT Upgrades for Digital Healthcare	p.19
5.1 Internet of Medical Things and Connected Device Environment	p.11	13.2 Data Management and Regulatory Impact	p.19
5.2 Legal Implications	p.11		
5.3 Cybersecurity and Data Protection	p.12		
5.4 Proposed Regulatory Developments	p.12		

SWITZERLAND CONTENTS

14. Intellectual Property	p.19	15. Liability	p.21
14.1 Scope of Protection	p.19	15.1 Patient Care	p.21
14.2 Advantages and Disadvantages of Protections	p.20	15.2 Commercial	p.22
14.3 Licensing Structures	p.20	16. Hot Topics and Trends on the Horizon	p.22
14.4 Research in Academic Institutions	p.20	16.1 Hot Topics That May Impact Digital Healthcare in the Future	p.22
14.5 Contracts and Collaborative Developments	p.21		

1. DIGITAL HEALTHCARE OVERVIEW

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

From pagers and fax machines to telemedical videoconferencing and electronic patient records, the spectrum of information technologies available to healthcare providers (HCPs), healthcare organisations (HCOs) and patients in Switzerland has proliferated and is expected to reach as-yet unexploited heights.

Digital Healthcare as an Umbrella Term

While “digital healthcare” or alternative notions of “electronic health services” and “Health 2.0” are generally understood to represent the sum of information technologies designed to increase the well-being, fitness or health of a given population or the efficiency of healthcare services – eg, by facilitating communication between HCPs, HCOs and patients – the term “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. When used in this article, the term “digital healthcare” will accordingly be used as an umbrella term covering 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 their general well-being – eg, by encouraging an active lifestyle – whereas technologies belonging to the digital medicine realm will make claims to prevent, diagnose or treat a human disease and improve their medical condition.

From an HCP’s perspective, digital healthcare will primarily involve 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 an according duty of care.

From a regulatory perspective, digital medicine faces more stringent evidentiary requirements to substantiate 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.

eHealth and mHealth

The Swiss regulator has, however, defined the terms “eHealth” and “mHealth”. As part of an initiative to increase digitalisation of the healthcare sector, the Swiss federal and cantonal administrations jointly adopted a “Swiss eHealth Strategy 2.0”. According to the strategy, 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 defined "eHealth" as "the integrated use of information and communication technologies (ICT) to design, support and network all processes and participants in the health care system". Inter alia, the eHealth strategy Switzerland led to the release of "mHealth recommendations" (dated March 2017). These mHealth recommendations refer to mHealth as "medical procedures, healthcare and preventive measures supported by wirelessly connected devices" (abbreviated translation).

Though the strategies and recommendations offer useful definitions and guidance for legislators, regulators and economic operators, they do not aim at regulatory qualification, but at serving a basis for reform and allocation of funds. They are thus of limited value when describing the Swiss regulatory landscape.

Lack of a Comprehensive Regime for Digital Healthcare and Digital Medicine

The lack of a regulatory definition is due to the fact that 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.

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;
- telecoms regulations; and/or
- public procurement provisions.

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 (more broadly) 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 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

Due to a widespread acceptance and embracing of digital technologies within the Swiss population and an ageing society weighing on the Swiss social insurance, digitalisation of healthcare has become a priority.

At the same time, increased connectivity has also brought about new legal issues. The current legal aspects in digital health include:

- data privacy and data safety;
- data access;
- cross-border provision of care;
- product liability for machine learning-enabled devices;
- evidentiary requirements for machine-learning technologies and digital apps; and
- reimbursement of new technologies under the mandatory social health insurance scheme.

Amongst the challenges to digital health are obstacles caused by varying national standards and a regulation that is not tailored to digital health technologies.

1.5 Impact of COVID-19

During the COVID-19 pandemic, video consultation, telemedical services and remote monitoring for patients or new digital tools – eg, contact tracing apps – gained ground. The increased use of digital platforms during the pandemic will likely have a lasting and enabling effect on healthcare in Switzerland.

2. HEALTHCARE REGULATORY ENVIRONMENT

2.1 Healthcare Regulatory Agencies

Swiss law is generally characterised by decentralised governance, where default competences lie with the Swiss cantonal authorities.

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

emedical services, and raise 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 benefit 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 inter-operability between HCPs, HCOs and digital healthcare applications, and with the aim of breaking up information silos, the Swiss legislator and regulator laid grounds for an electronic patient dossier (EPD). 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. To enable access to an EPD, the patient must have given their consent with a two-factor authentication. The EPD was rolled out gradually in the course of 2021 and shall be further developed.

Medical devices ordinances

The Swiss regulator also adopted a fundamental reform of the medical-device regimes, including in vitro diagnostic medical devices, with a view to harmonising the Swiss regime with the European Union's Regulations (EU) 2017/745 (MDR) and (EU) 2017/746 (IVDR). The revised Medical Devices Ordinance (MedDO) entered into force on 26 May 2021 and will be supplemented by the Ordinance on In vitro Diagnostic Medical

Devices, a draft of which was published in April 2021. Both ordinances closely mirror and directly reference the respective EU provisions. Neither ordinance is specifically tailored to devices relying on digital technologies, and guidance on artificial intelligence (AI) under the MDR and IVDR is outstanding.

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 the Data Protection Act

To account for the increased role and value of collecting and processing personal data, the Swiss legislator adopted a reformed Federal Data Protection Act (revFDPA), due to apply from 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 HGTA and its imple-

menting ordinance are due to apply from the fourth quarter of 2022.

Reform impact

Amongst the regulatory reform projects under way, 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.

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 telecoms regulations, general product-safety regimes and competition laws.

Telecoms Regulations

Digital healthcare technologies qualified as telecommunication 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 telecoms networks in Switzerland. It defines telecommunication services as the transmission of information for third parties. As per guidance provided by OfCom, a telecommunications services 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 telecoms 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 over the observance of 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 into 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 bodies are subject to oversight by the cantonal data protection 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.

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 (*obligatorische Krankenpflegeversicherung*, or OKP). 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 are increasingly involving preventative measures into 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

The TPA defines medical devices as “products, including instruments, apparatus, equipment, in vitro diagnostics, software [...] and other goods and substances which are intended or claimed to have a medical use [...]”. With regard to standalone software, it is therefore questionable whether it can be a medical device. The TPA explicitly mentions software as a medical device under the condition that the software serves a medical purpose. Thus, general software that does not go beyond imparting knowledge, such as information platforms or electronic patient dossiers, is not considered a medical device. If an app or software only serves to measure fitness or nutrition data or to statistically evaluate clinical or epidemiological data, this does not constitute a medical device. Nevertheless, the term “medical device” is to be understood broadly. For example, an app that measures a woman’s fertility by analysing personal data

was qualified as a medical device by the Federal Administrative Court.

A lack of clarity may particularly arise when an app records or uses the data of a specific person, but mainly to consolidate and summarise data. Such apps 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). To guide app developers and help them with regulatory qualification, Swiss regulators have adopted recommendations and a catalogue of quality criteria for mHealth apps.

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 aiming at prevention, but it is not a key task for mandatory health insurance providers, as noted above. 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 to persons having a professional licence.

5. WEARABLES, IMPLANTABLE AND DIGESTIBLES HEALTHCARE TECHNOLOGIES

5.1 Internet of Medical Things and Connected Device Environment

With their eHealth strategy, the Confederation and the cantons have set specific goals to promote digitalisation in the healthcare sector in a targeted manner. One particular focus is on the electronic patient dossier. Of the numerous innovations in the area of digital health, digital medical devices as well as wearables and biosensors can be highlighted as particularly important.

5.2 Legal Implications

Under Swiss law, there are no specific liability rules regarding digital health.

In general, civil liability rules apply, especially the liability in tort, 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 then 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.

With regard to the use of AI in healthcare, the liability of doctors must be assessed with regard to a possible breach of the doctor's duty of care.

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

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, 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.

In relation to cloud computing, cybersecurity risks are mitigated to an extent but legal risk increases, in view of cross-border data transfers and the required transfer impact assessments.

In order 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 with regard to 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 the area of digitalised medicine are, in particular, Swissmedic, the FOPH and the FDPIC. While 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.

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 European 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 purpose of (each a medical purpose):

- 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

The Swiss regulatory authority, Swissmedic, issued a guidance document on standalone medical-device software, including apps installed on wearable devices, which references the respective EU/EEA guidance MEDDEV 2.1/6 and describes practical examples of non-medical software.

Specifically, an app providing generic non-personalised medical information or an app for "fitness, wellbeing or nutrition (eg, diets)" (translation) is not considered a medical device. In its guidance, Swissmedic also specifies that – 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).

In order to be considered a medical device, software would thus have to perform a certain degree of data processing tailored to individual patients with a view to achieving a medical purpose.

Software not intended to achieve a medical purpose on its own would not in itself be considered a medical device, but may – for example, if it drives or influences a medical device – fall under the scope of the medical-device regime as an accessory to, or component of, a medical device.

To date, Swissmedic has not made reference to, or taken a stance on, the new (non-binding) MDR guidance MDCG 2019-11 issued by the European Medical Device Co-ordination Group (MDCG), an advisory body composed of representatives from the European national regulators. However, since the definition of medical devices adopted by the Swiss regulator corresponds to the MDR, the MedDO will likely be interpreted in accordance with the MDCG 2019-11.

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. Unlike medicinal products, medical devices do not require a marketing authorisation,

but must in principle be marked with a specified conformity marking to be marketable. The marking 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. Nor have harmonised technical standards for the general safety and performance requirements specific to machine-learning algorithms yet been endorsed by the Swiss regulator.

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 cost. At the same time, the new medical-device regime tightens requirements on

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

7. TELEHEALTH

7.1 Role of Telehealth in Healthcare

Telemedicine is well established in Switzerland. Certain Swiss health insurance companies offer insurance policies with telemedicine gateways akin to the health maintenance organisation model where patients must first seek consultation through a designated telemedical portal.

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 and telemedicine is thus subject to general rules governing conventional forms of healthcare; in particular, medical professional standards of care. 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 requirements for physicians and telemedical platforms providing remote services from EU/European Free Trade Association member states are subject to an ongoing debate.

In principle, physicians based in the EU/EEA benefit from an exemption from cantonal profes-

sional 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. Yet, 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, the 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. Depending on the applicable cantonal provisions, the business model and the relationship between patients and physicians, telemedical platforms may thus have to take into account whether they operate outpatient medical institutions within the meaning of cantonal licensing provisions.

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" (see tariff No 00.0110 et seqq), for telemedical services provided by specialists other than psychiatrists or psychotherapists. During the COVID-19 pandemic, the respective tariff positions were partially and temporarily adapted to account for the need for longer teleconsultations.

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. 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, among other things, that further legal requirements or guidelines should be developed in close international co-ordination, as fragmented regulations across domestic jurisdictions may prove ineffective and lead to unintended market distortions.

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 of the potentials further attributed to 5G is to provide 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, telecoms 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 popula-

tions 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

Personal health information (PHI), directly or indirectly allowing for insights on an identified or identifiable person's physical or mental health, is categorised as particularly sensitive data under the general data protection regime set out in the FDPA and its implementing ordinance.

Using and sharing PHI within the scope of the Swiss jurisdiction may be subject to multiple legal regimes, including:

- professional secrecy rules governing physicians and public officials;
- human research regulations; and
- general data protection law.

The current FDPA is under an ongoing revision; the final text was adopted in 2020. The revised FDPA (revFDPA) is expected to apply from 1 September 2023.

General Data Protection Laws

Under the FDPA, and revFDPA, processing PHI in breach of general principles on transparency, good faith, proportionality, data accuracy or data security, and transferring PHI (including genetic data) 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.

Where consent is required for lack of other bases, 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.

As a rule, a justification is unnecessary where a recipient acts as a processor on behalf of a controller and is subject to respective auditing and instruction rights.

PHI may be transferred abroad under the conditions set out in the FDPA. The USA is not deemed to provide an adequate data protection level within the meaning of the FDPA. The Swiss FDPIC recently published a position paper concluding that the Swiss-US Privacy Shield does not provide an adequate data protection level and 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; eg, through the conclusion of a data transfer agreement, typically using EU standard contractual clauses adapted to Swiss requirements with additional safeguards depending on a case-by-case analysis.

Professional and Official Secrecy

HCPs and HCOs are subject to professional and/or official secrecy obligations. Sharing patient data with third parties is permissible if mandated or permitted on legal grounds or upon informed patient consent. Where such legal bases or consent are lacking, patient data may be entrusted to third parties qualified as auxiliaries (data processors) of the HCP bound by the same professional secrecy as the principal. The majority in doctrine argues that the latter permission also extends to processors located abroad, though

certain scholars also take the view that foreign transfers require patient consent to ensure criminal persecution of processors acting in violation of professional secrecy.

Patient consent legalising transfers under professional secrecy obligations need not be obtained in writing and may be given implicitly or explicitly. Consent must, however, be voluntary and given by a person capable of judgement and in full knowledge of all essential circumstances.

Human Research Laws

Similar consent and information requirements are set by the HRA and its implementing Human Research Ordinance (HRO).

Specifically, if researchers collecting PHI for an authorised research project intend to make further use of PHI (including genetic data) in unencrypted form for another research project, they must obtain informed consent from the data subject or, as applicable, their legal representative or next of kin. Further use of non-genetic PHI in coded form is permitted, provided data subjects are informed of their right to dissent to that further use. The obligation to inform data subjects and provisions on encryption and key management is further specified in the HRO. 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.

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 control-

ler, 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 with regard to 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.

Liability Risks

Under current legislation, a breach of privacy, including a failure to handle security breaches properly, may lead to civil claims against the controller, including claims for breach of contract. However, financial losses are usually difficult to quantify, which greatly reduces the risk of financial liability. Moreover, the FDPIC may open an investigation into security breaches, which may lead to negative publicity. Besides, infringements are usually not punishable by criminal fines under current law. The revised FDPA will, however, introduce fines of up to CHF250,000 for certain breaches, including failure to comply with minimum security standards.

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, eg, 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 devices software (see **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies**), guidance on evidentiary requirements for general healthcare applications have not yet been set. AI- 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 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 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.

12. HEALTHCARE COMPANIES

12.1 Legal Issues Facing Healthcare Companies

If 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. Depending on the classification of a medical device, there are different approval and authorisation requirements. 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 into 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 these regards.

13. UPGRADING IT INFRASTRUCTURE

13.1 IT Upgrades for Digital Healthcare

In order to support digital healthcare, HCOs need an adequate IT infrastructure suitable to integrate new technologies. Key features of digital healthcare build on connectivity between inter-operable technologies. To ensure inter-operability, 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. Network operators and technology developers alike will thus play a crucial role in harnessing the digital healthcare potential. As with all systems enabling multiparty co-operation, security issues become particularly important, as well as data and information governance.

13.2 Data Management and Regulatory Impact

Although the revised FDPA calls for data security measures that correspond to the state of the art, it does not specify the specific technical standards in more detail. The implementing ordinances to the revised FDPA may contain more detailed regulation about data security, but no final version exists as of yet. However, it is very unlikely that specific requirements for IT upgrades will be introduced. 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 as of the moment of their creation. 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 with regard to the licensing of IP rights under Swiss Law. Nevertheless, it is customary and advisable to enter into written licence agreements and register the licence (as 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 Copy Right 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 in the course of 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) to 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 IP rights, and the allocation of (joint or separate) ownership in foreground IP. Best practice includes fine-tuning the allocation of IP rights to the specific needs of the parties and an awareness that IP 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 torts. 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 inter-dependence 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 general 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 significant-

ly 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 would specifically address AI and potential bias. Generally, the use and outcomes of AI will be 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 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 of 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 a producer liability in torts. Whether and which of these principles apply will depend on the specific facts of the case.

Other ways in which HCOs may safeguard their interests include securing indemnity undertakings from their direct contractual partners.

16. HOT TOPICS AND TRENDS ON THE HORIZON

16.1 Hot Topics That May Impact Digital Healthcare in the Future

As Switzerland is a relatively small market that is keenly aware of developments in the international arena, generally the Swiss regulatory landscape will, with some delay, act on international developments. A key topic in this regard is AI, and the EU regulation laying down harmonised rules on AI proposed by the European Commission in June 2021.

Walder Wyss Ltd is one of the most successful and fastest-growing Swiss commercial law firms, with offices in Zurich, Geneva, Basel, Berne, Lausanne and Lugano. With around 250 legal experts, the firm specialises in corporate and commercial law, banking and finance, technology, data protection and intellectual property, regulation and competition law, dispute resolution and tax law. Clients include national and international companies, publicly held corporations and family businesses, as well as public law institutions and private clients. In relation to

data protection, Walder Wyss professionals advise clients on compliance with data protection restrictions (Swiss and GDPR), represent parties before cantonal and federal data protection authorities and before courts, negotiate agreements, and advise private clients and public entities on all matters of data protection law. They regularly assist clients who are subject to specific restrictions and regulation; for example, in the banking, insurance, telecommunications and health sectors.

AUTHORS



David Vasella advises on all questions of data protection, information, technology law and contract law. He has particular expertise in the monetisation of data, the digitalisation of

business processes and data protection compliance. David is CIPP/E and CIPM certified, and his professional memberships are the Zurich and Swiss Bar, the IAPP and the DGRI. He joined Walder Wyss in 2017 and is a partner and head of the information technology and intellectual property team. David has had secondments with data-driven companies and is co-editor of *digma* and *datenrecht.ch*. He attended the Universities of Fribourg (lic iur 2002) and Zurich (Dr iur 2011), and speaks German and English.



Michael Isler is a partner at Walder Wyss practising in IT, intellectual property and life sciences law, with a particular focus on health technology. He regularly advises in complex

outsourcing, technology transfer and platform projects from the conceptual and negotiation phase to dispute settlement. Michael takes an active role in several professional organisations and is co-editor of *Life Science Recht*, the Swiss law journal for pharma, biotech and medtech. Before joining a major law firm in Basel and Zurich in 2010, Michael worked as in-house counsel at a technology group and a global telecoms infrastructure and service provider, having attended the Universities of Zürich (lic iur 2000) and Lucerne (Dr iur 2011), and speaks German and English.



Anne-Catherine Cardinaux

specialises in life sciences, health and data protection law and advises and represents clients in all areas of constitutional and administrative

law. She joined Walder Wyss in 2022 and is an attorney in the Regulated Markets, Competition, Technology and IP team. Anne-Catherine attended the University of Basel (MLaw, 2013) and then worked as a postgraduate in the legal department of one of the world's largest pharmaceutical companies based in Basel, as a junior associate at a major Swiss commercial law firm in Basel, as a law clerk at the Meilen District Court and as a junior associate at a leading Swiss commercial law firm in Zurich.

Walder Wyss Ltd

Seefeldstrasse 123
P.O. 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

Trends and Developments

Contributed by:

*David Vasella, Michael Isler and Anne-Catherine Cardinaux
Walder Wyss Ltd see p.28*

Introduction

The COVID-19 pandemic has highlighted the potential of digital technologies in tackling global health challenges, including novel viruses, climate change and ageing societies. It has also propelled a health-technology boom that is likely to outlive strictures imposed during the pandemic.

The impetus for digital health and a mobile technology-friendly Swiss population makes Switzerland a fertile ground for innovation. At the same time, developers in the health-technology realm are closely following ongoing substantial legal reforms that – if left unaddressed by market operators – may hamper innovation and slow down the impulses catalysed by COVID-19.

Amongst the ongoing reform projects likely to impact innovators in healthcare the most are the two new medical device ordinances, mirroring the European Union's Regulations (EU) 2017/745 (MDR) and (EU) 2017/746 (IVDR), and the reformed data privacy regime set out in the Federal Data Protection Act (FDPA) and its implementing ordinance.

Reform of the Medical Devices Regime

In synchrony with the EU's MDR, the Swiss regulator enacted the Swiss Medical Devices Ordinance (MedDO), which entered into force on 26 May 2021. While the Swiss medical device regime largely corresponds to, and references, the MDR, the Swiss reform also provides for Swiss specifics. The MedDO will be supplemented with a revised regime on in vitro diagnostic medical devices. On 4 May 2022, the Federal Council adopted the new Ordinance on In Vitro

Diagnostic Medical Devices and the amendment to the Ordinance on Clinical Trials with Medical Devices. The aim of the new regulations is to improve patient safety by means of stricter requirements for conformity assessment and post-market surveillance. The new legal requirements entered into force on 26 May 2022.

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 is in contrast to 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 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 the Swiss Federal Agency for Therapeutic Products (Swissmedic). This requirement may lead to EU manufacturers not being prepared to disclose the entire technical documentation to the Swiss authorised representative (especially if importers wish to assume the role of authorised representative for several manufacturers) (business secrets) and therefore to prefer 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, eg, 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 legislator has enacted a revised FDPA. The revised FDPA was adopted by the Swiss parliament on 25 September 2020 and it will most likely 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, which the federal administration is still working on and which is expected to be published by August 2022. 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 in practice centred around foreign transfers of PHI. Following the decision rendered by 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 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, inter-operability standards, and reimbursement of new technologies under the mandatory statutory health insurance scheme.

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 general legal framework in Switzerland is basically suitable and sufficient at the present time. 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 FDPAs stipulates that data subjects have a right not to be judged by an AI when making important value decisions.

In addition, the Federal Council has decided that the Federal Act on the Electronic Patient File (*Bundesgesetz über das elektronische Patientendossier*) should be revised. This is particularly because a clear division of tasks and responsibilities as well as sustainable financing are lacking for the successful introduction and dissemination of the electronic patient dossier.

Besides, due to various legal amendments in recent years to the Federal Health Insurance Act, the Federal Therapeutic Products Act and the Federal Ordinance on Integrity and Transparency in relation to Therapeutic Products, the Association of Medical Laboratories in Switzerland (FAMH) and several leading players in laboratory medicine have developed a Laboratory Code of Conduct, which entered into force on 1 April 2022. The FAMH Laboratory Code of Conduct is intended to make it easier for laboratory medicine and other health actors to orient themselves in a complex regulatory environment. It will thus provide the basis for fair and equitable competition among the health actors involved and promote the confidence of patients, customers, politicians and financiers. The FAMH Laboratory Code of Conduct enables all signatories to formally commit to business practices that meet the highest ethical and commercial requirements.

Walder Wyss Ltd is one of the most successful and fastest-growing Swiss commercial law firms, with offices in Zurich, Geneva, Basel, Berne, Lausanne and Lugano. With around 250 legal experts, the firm specialises in corporate and commercial law, banking and finance, technology, data protection and intellectual property, regulation and competition law, dispute resolution and tax law. Clients include national and international companies, publicly held corporations and family businesses, as well as public law institutions and private clients. In relation to

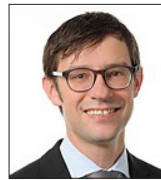
data protection, Walder Wyss professionals advise clients on compliance with data protection restrictions (Swiss and GDPR), represent parties before cantonal and federal data protection authorities and before courts, negotiate agreements, and advise private clients and public entities on all matters of data protection law. They regularly assist clients who are subject to specific restrictions and regulation; for example, in the banking, insurance, telecommunications and health sectors.

AUTHORS



David Vasella advises on all questions of data protection, information, technology law and contract law. He has particular expertise in the monetisation of data, the digitalisation of

business processes and data protection compliance. David is CIPP/E and CIPM certified, and his professional memberships are the Zurich and Swiss Bar, the IAPP and the DGRI. He joined Walder Wyss in 2017 and is a partner and head of the information technology and intellectual property team. David has had secondments with data-driven companies and is co-editor of *digma* and *datenrecht.ch*. He attended the Universities of Fribourg (lic iur 2002) and Zurich (Dr iur 2011), and speaks German and English.



Michael Isler is a partner at Walder Wyss practising in IT, intellectual property and life sciences law, with a particular focus on health technology. He regularly advises in complex

outsourcing, technology transfer and platform projects from the conceptual and negotiation phase to dispute settlement. Michael takes an active role in several professional organisations and is co-editor of *Life Science Recht*, the Swiss law journal for pharma, biotech and medtech. Before joining a major law firm in Basel and Zurich in 2010, Michael worked as in-house counsel at a technology group and a global telecoms infrastructure and service provider, having attended the Universities of Zürich (lic iur 2000) and Lucerne (Dr iur 2011), and speaks German and English.

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



Anne-Catherine Cardinaux

specialises in life sciences, health and data protection law and advises and represents clients in all areas of constitutional and administrative

law. She joined Walder Wyss in 2022 and is an attorney in the Regulated Markets, Competition, Technology and IP team. Anne-Catherine attended the University of Basel (MLaw, 2013) and then worked as a postgraduate in the legal department of one of the world's largest pharmaceutical companies based in Basel, as a junior associate at a major Swiss commercial law firm in Basel, as a law clerk at the Meilen District Court and as a junior associate at a leading Swiss commercial law firm in Zurich.

Walder Wyss Ltd

Seefeldstrasse 123
P.O. 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



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

practiceguides.chambers.com