LAUX
LAWYERS AG
ZURICH | BASEL

Cloud for Healthcare

Solutions for commonly expressed reservations – not for healthcare organisations only

Laux Lawyers AG
January 2024

On the initiative and with the kind support of aws

LAUX LAWYERS AG
ZURICH | BASEL

CONTENT

I EXECUTIVE SUMMARY 3

II CLOUD FOR HEALTHCARE 5

Health data in the cloud 5
1. Health data as sensitive personal data 6
2. Regarding the risk potential of health data 6
Concrete application cases of cloud usage in the healthcare sector 8
1. Introduction 8
2. Hospital information system in the cloud 8
3. "Omics" in the cloud 9
4. Artificial intelligence/Machine-Learning in the cloud 10
5. Medical devices in the cloud 11

III COMMON RESERVATIONS AND POSSIBLE SOLUTIONS FROM A LEGAL PERSPECTIVE 12

Introduction 12
Encountered reservations in detail 12
1. Reservation: "Doctor-patient confidentiality precludes cloud use" 12
2. Reservation: "Cloud increases the risk of discrimination" 14
3. Reservation: "Cloud cannot be controlled" 14
4. Reservation: "Cloud increases risks; for there are countless subcontractors" 17
5. Reservation: "An explicit legal basis is needed" 18
6. Reservation: "A cloud with risks of access by authorities from abroad is inadmissible" 20
7. Reservation: "The cloud is at odds with data sovereignty" 24
Conclusion: What remains of the reservations? 24

IV ANNEXES 25

Elements of risk analysis 25
1. A future threat can only be described with statements about risk 25
2. Risk statements as a synthesis of probability and impact 25
3. Illustration using an example (information about the blood type) 25
4. What remains 27
Directory of statutory bases 28
1. Data protection 28
2. Criminal law 28
3. Special Federal health legislation 28
4. Special Cantonal health legislation 28
5. Federal social security legislation 28

Convenience translation of German original; translated with DeepL Pro

I EXECUTIVE SUMMARY

Hospitals, doctors' offices and other players in the healthcare sector process and store large amounts of data around the clock. The extensive data sets largely contain **health data.** The need for control and protection of affected persons regarding health data is recognised and undisputed.

The healthcare system and its service providers are regulated. Health data is considered sensitive data that must be treated confidentially. Data protection law also requires the integrity and availability of such data. These regulatory safeguards are in the public interest.

Digitalisation promises great benefits for the healthcare system. But reservations slow down innovation. What is allowed? What is not? There are many questions and too few clear answers. One thing is certain: Digitalisation is unthinkable without the **trust** of patients, doctors, hospitals, authorities, legislators, and other stakeholders.

Cloud services are at the centre of this conflict.[1] Their potential is enormous: cloud services facilitate many digitalisation initiatives considerably. Costs can be reduced – a concern that is paramount for healthcare organisations. By using cloud services, healthcare organisations can also increase their efficiency, enhance the security and flexibility of their IT systems, and they can free up resources for their core business. In addition, health care organisations can develop modern, highly scalable solutions with the highest security standards and reliability for the provision of healthcare services, the development of new forms of treatment, and – not least – for the personalised care of patients. The IT infrastructures used are state-of-the-art in terms of functionality and cyber security, even without the healthcare organisations having to set up and operate their own major IT and security infrastructure. With the increasing spread of cloud services offered by large international cloud providers (so-called "hyperscalers"), general awareness and understanding of how they handle the data entrusted to them is growing.

Challenges of a different nature can be associated with the advantages. The data is kept by the cloud provider. Reservations pertaining thereto are the subject of intense public debate: The cloud (i.e. cloud services) is described as problematic from a **data protection** perspective and regarding **doctor-patient confidentiality**; furthermore, foreign references would stand in the way of its use.

[1] In this white paper, we understand cloud services to mean the entirety of services that a provider makes available to a healthcare institution for the use of certain IT infrastructures. This offering is standardised, automated, scalable, and provided in non-dedicated form via data networks. "Cloud service" here also stands for the colloquially coined term "public cloud", which is intended to express that the provider's basic components cannot be used individually or exclusively ("dedicated") by any customer; in contrast, the provided usage opportunities within a tenant are individual and separate from other customers ("isolation"), which is made possible, for example, by means of network technology.

One thing is clear: Switzerland has a culture in which a high value is attributed to health data, and that is both good and right. An expression of this culture is the desire to protect health data – precisely because it is important. This leads to the following fundamental findings and important requirements:

- **firstly,** there is a major risk potential associated with health data
- **secondly,** patients must therefore be protected from misuse of their data
- **thirdly,** patients should therefore be allowed to decide whether others can view their data
- **fourthly,** entrusted patient data should remain within the doctor's sphere of influence
- **fifthly,** high security measures are needed to protect the patients' data.

These requirements and the values on which they are based are the foundation on which this white paper is built. The authors uphold them and reaffirm their importance.

However, this does not mean that the authors advise against the cloud or share the problematising positions that are sometimes put forward. On the contrary. Although there is consensus on the basic requirements and values, the public discussion about the cloud in healthcare suffers from misunderstandings.

Healthcare law largely takes place in public hospitals. In this respect, the healthcare system, insofar as it is organised at Cantonal level, is under the **supervision of the Cantonal authorities**. The Cantonal data protection authorities actively shape the discussion and issue guidelines, checklists, and information sheets. **These are expressions of opinion and as such are non-binding for healthcare institutions.**[2] The same applies to recommendations of the relevant industry associations. Nevertheless, uncertainty is increasing.

The following explanations show that certain reservations discussed in the public debate do not stand up to legal scrutiny.

Cloud for healthcare is possible and offers many advantages

The healthcare system must be taken care of. A correspondingly high standard of care must be applied. **Healthcare institutions can master these legal challenges with the high-quality and high-security cloud services available today.**

[2] Cantonal data protection law plays a major role in the healthcare sector. Opinions expressed by Cantonal data protection supervisory authorities are an instrument of proactively communicated legal hearing – the authority explains in advance how it assesses a particular case in legal terms. This serves legal clarity and planning certainty and thus the efficient use of resources of those who could be impaired or slowed down by a decision of such a body – insofar as it has decision-making competence. Public statements are thus primarily binding only for the Cantonal data protection authority itself. The hospital may – as far as data processing in the provision of healthcare services under the Cantonal performance mandate is concerned – trust that the supervisory authority will apply the law as described in the statement. However, these are not legally binding orders for the hospital.

II CLOUD FOR HEALTHCARE

Health data in the cloud

This white paper sheds light from various legal perspectives on the question of whether hospitals, doctors' offices and other healthcare institutions are allowed to store and process healthcare data "in the cloud". What does the term "health data" encompass from a legal perspective? Various laws use the term or a variation of it. There is no universally valid legal definition.

The Federal Act on Data Protection **(FADP)** as well as the Cantonal data protection laws set out requirements for handling **personal data**. In the context of hospitals or doctors, this concerns master data (general personal data such as name, address, and insurance number) on the one hand and health data relating to the respective patient on the other. Health data includes information on the past or current state of health, the course of treatment as well as the use and billing of health services. However, the concept of health data under data protection law includes not only information on current or past illnesses or accidents, but also results from examinations (e.g. examination of blood samples or genetic data) from which risks of illness or other information on the future state of health can be derived.

Special health laws specify this broad understanding. It should also be noted that in the context of a diagnosis, examination or treatment in a hospital or a doctor's office, or in the context of research on human beings, even information on lifestyle (e.g. diet, smoking, exercise), data on the living environment (e.g. air and water quality), on the social environment (e.g. family or profession) as well as fitness tracker data relate to the data subject's health and are thus qualified and categorised as health data in such a context.

Health data (Term)

Health data is data about a person's past, present, or future state of health. In the context of a hospital or doctor's practice, this includes information on the patient's lifestyle and social environment as well as the results of examinations from which information on the state of health can be derived.

1. Health data as sensitive personal data
The FADP and Cantonal data protection laws categorise health data as sensitive personal data. The legislator sees the special need for protection primarily in the fact that the risk of danger is particularly high in the event of uncontrolled disclosure or publication. Essentially, protection against discrimination is addressed here. The patient is to be protected from being stigmatised or discriminated against by the state, insurance companies, the social environment or at work because of a health condition.

In other words, the aim is to prevent the uncontrolled expansion of the circle of those who have plaintext access to sensitive personal data (what we call an "uncontrolled expansion of the sphere of control"). A patient must be able to rely on the doctor's professional handling of her or his data. This must function just as reliably as the confidentiality of the doctor. If the patient confides in a doctor, the information should not leave her sphere of influence. In this sense, the doctor must control her circle (specifically: her medical practice with everything that belongs along with it, including IT resources such as cloud services that she uses).

Sensitivity

In the case of health data, the sensitivity arises from the fact that the affected persons could suffer disadvantages, e.g. because of an illness that has become known in an uncontrolled manner.

Examples of disadvantages
- Stigmatisation in the social environment
- Discrimination in the workplace (economic consequences or psychological impairment)
- Discrimination by insurance (cost risk, restriction of choice of contract partners or available benefits)

2. Regarding the risk potential of health data
In extreme cases, the misuse of health data can have very serious consequences. The potential danger can be shown by concrete examples (see appendix "Elements of risk analysis"). In practice, however, inaccurate conclusions are drawn on this basis. Sometimes the perspectives are lost.

What is the problem of an uncontrolled expansion of the sphere of control?

Uncontrolled expansion of the sphere of control means the process whereby an open number of people receive health data and can do what they want with it. Abuses are in that case possible as well. Especially in the case of health data, it is therefore important to protect against uncontrolled expansion of the sphere of control.

Background:

- When data is sent to an **open group of recipients** who are **not subject to control** regarding the personal data they receive, an uncontrollable situation arises. A typical example is a data breach. *Many potential malicious actors can carry out a wide variety of potential harmful actions* without the ability to reduce this risk. This risk situation cannot be controlled.
- In contrast, if the data is transferred to a **specific recipient** who is subject to **control** regarding the personal data transferred, it is possible to concretely assess the specific risk posed by the specific recipient. This risk situation can be controlled.

In view of the foregoing, it would be wrong to say that the danger arises from the information itself. One and the same piece of information about health can lead to different risks of danger to the personal and fundamental rights of the person affected, depending on who views or processes the data and in what context. The danger cannot be assessed in the abstract but must be viewed in the specific case.

In other words, it is the context of use **(context)** that makes data processing risky. A statement about a person's state of health can take on a different meaning depending on the context of use. For example, fitness measurements have a different meaning in a leisure context than when they are used in a medical diagnosis or as a basis for therapy decisions. The appendix shows in more detail the extent to which risk statements result from the context.

If we apply this insight to this white paper, it becomes clear that the context of use or the purpose of use of a processing does not change by using cloud services.

When using mature cloud services[3] the health data is not made available to an indefinite number of people. The data is stored with a specific recipient, and in a controlled manner (ensuring this is the duty of the health institutions).
An uncontrolled expansion of the sphere of control is also not present if, for example, a foreign law enforcement agency demands the disclosure of certain data from the cloud provider in the context of legal proceedings. In this regard, the (theoretical) risks must be concretely assessed. But there is no uncontrolled expansion of the sphere of control if the process is sufficiently supervised by the court in accordance with the rule of law and the authority does not in turn disclose the data to an indefinite number of other recipients (e.g. through publication or by similar means) or use it for purposes other than law enforcement. However, it must be determined which acts of use it carries out. And the risk assessment must be linked to this (in a concrete way).

The use of cloud services in itself is therefore not a trigger for speaking of an uncontrolled expansion of the sphere of control. In this respect, going to the cloud is a process like any other, even when it comes to health data: one must identify possible hazards and describe their probability of occurrence (probability) as well as their potential for damage (impact). From this, a risk statement can be made in the sense of a synthesis. No more and no less is required.

[3] The term **"mature cloud service"** is an umbrella term. A provider of a mature cloud service should establish a controlled state in terms of service delivery, information security and governance. If it does so, its cloud services can be described as "mature". The provider of a mature cloud service must control its own IT infrastructures, the people used to provide the service and the processes defined for this purpose. In addition, it must be prepared to disclose to the customer which of these measures it is taking, so that the health institutions as customers are able to include the cloud provider and its services in their control.

Concrete application cases of cloud usage in the healthcare sector

1. Introduction

The healthcare sector is highly regulated. A large number of special laws provide framework conditions for the activities of hospitals, other providers of healthcare services, researchers, manufacturers of medical devices or medicines and other actors in the healthcare sector. The special health laws and implementing ordinances[4] also contain rules that supplement the general rules of data protection and secrecy law or concretise them for a specific application (e.g. research on humans or genetic studies on humans). The corresponding rules apply regardless of the infrastructure or technology used. For example, the intended use determines whether software is a medical device.

The decision to use a cloud service thus has a "neutral" effect insofar as the rules apply whether a cloud solution or an "on-premises solution" is used. The following analysis of some typical applications shows this as an example. What changes are the means used, for example, to exercise control – whereby, especially in information security, cloud services increase control options, but health institutions must also ensure organisationally that they consistently use the control options

2. Hospital information system in the cloud

Hospital information systems (HIS) are intended to comprehensively map everyday life in a hospital. As far as data protection aspects are concerned, provisions on the duty to document and the duty to retain records are particularly relevant. Insofar as considerably extended purposes of use result from processing in the HIS, this would also have to be discussed in terms of data protection law.

In the following, the resulting legal requirements (especially those set out in secrecy law and Cantonal data protection law) for the HIS of a hospital are discussed. However, none of these aspects is specifically hostile to the cloud. Or, in other words: with the cloud, these issues are not more problematic, but often better addressed, as follows:

To what extent does the cloud change anything for the use of a HIS in a hospital?

Topic	Requirement[5]	Influence of the cloud
Patient record	Rights to information and access, and the right to obtain a copy of the patient record under Cantonal health and patient laws[6]	neutral (functional requirement[7])
	Rights to information and access, rectification, deletion, and the right to receive a copy of personal data under data protection law	neutral (functional requirement)
Overall system (HIS)	All persons bound to secrecy must be able to comply with their professional secrecy obligations; this even though an overall organisation is connected to the HIS (secrecy obligations).	neutral (authorisation concept required) (functional requirement)
	Protection against unauthorised access (information security, based on data protection and secrecy obligations; also based on the Cantonal service mandate).[8]	neutral (cloud usually better) (functional requirement)
	Protection against unauthorised modification (information security, due to data protection and secrecy obligations; also based on Cantonal service mandate)	neutral (cloud usually better) (functional requirement)
	Ensuring availability (information security, data protection; also based on Cantonal service mandate)	neutral (cloud usually better) (non-functional requirement)
	Processes for exporting patient information, deletion concept and logging of access and data processing (good governance).	neutral (functional requirement)

The illustration shows that the legal and contractual requirements for documentation, storage, information security and the protection of patients' rights do not change if a hospital has its HIS provided and operated on a cloud infrastructure. It is mostly the functional properties that are relevant. The requirements for doctor-patient confidentiality also do not change (see e.g. Reservation 1, below).

What does change: There is an outsourcing of data processing. The hospital must contractually ensure that it is bound by instructions and that appropriate technical and organisational protective measures are in place. This is feasible, as experience shows.

The following remains to be noted: Often the change to an HIS as a cloud service is not the first step of a hospital into the "cloud". Experience shows that applications such as a patient portal (e.g. for booking appointments), information security solutions or training solutions are the first step in a hospital's cloud transformation. It is worthwhile if a hospital develops and tests the methodology in smaller implementation projects, which are also crucial for risk clarifications and implementation measures within the framework of the implementation of a cloud strategy for the HIS.

3. "Omics" in the cloud

Biological and genetic characteristics of people influence whether a drug or therapy is effective for them. The data necessary for individualising treatment and care are obtained by scientists, pharmaceutical companies, and doctors through so-called **omics** studies, among other things. These include the investigation of a person's genetic disposition **(genomics)**, the analysis of the composition of proteins in a person's tissue **(proteomics)** and the analysis of metabolic products **(metabolomics)**. From the results of such **omics** measurements and analyses, indications of existing diseases or disease risks can be derived, as well as indications of how patients are likely to respond to medication or treatment.

4 The annex contains a list of laws and ordinances which, together with general legal provisions (e.g. FADP or Cantonal data protection laws), form the legal framework for cloud use in the healthcare sector.

5 The requirements discussed here arise on one hand from laws (e.g. patient or health laws, data protection law, criminal law), on the other hand from contractual obligations (connection to electronic patient dossier) or from best practice or good governance considerations, some of which are also derived from professional duties of care.

6 E.g. §19 of the Patients Act of the Canton of Zurich; § 39a of the Health Act of the Canton of Berne.

7 E.g. export functions and support for automatic deletion as well as the setting of retention periods.

8 Within the framework of the Cantonal service mandates, hospitals are obliged to ensure that the population receives hospital care of sufficient quality and safety.

Special legal requirements[9] for omics measurements: Cloud relevance?		
Topic	**Requirement**	**Influence of the Cloud**
Data: Health data (processing)	Compliance with data protection law (Federal and Cantonal) and personality rights	neutral
	Information, education and consent requirements	neutral
	Protection of confidentiality	neutral
	Integrity protection	neutral
	Evaluation only with consent	neutral
	Need-to-know principle	neutral
	Logging to ensure the traceability of processing operations	neutral
	secure data transmission	neutral
	Data minimisation	neutral
Actions: Disclosure of genetic data abroad	In case disclosure abroad without adequate data protection is intended, a pseudonymisation obligation applies[10]: Data retention in such a foreign country is inadmissible without the consent of the affected person for genetic data that have not been pseudonymized	neutral
Actions: Clinical trials	Authorisation and reporting procedures	neutral
	Data retention requirements	neutral
Actions: Genetic testing on humans	Principle of non-discrimination	neutral

4. Artificial intelligence/Machine-Learning in the cloud

Artificial intelligence (AI) and machine learning (ML) are gaining importance in medicine. Possible areas of application are the diagnosis of breast cancer or lung cancer or the detection of brain haemorrhages in computer tomography. In the foreground, for example in the field of radiology, is the development of intelligent medical software that "learns" with each diagnosis.

Intelligent software is used today as an aid to diagnosis, with doctors rather than machines making the diagnosis. However, research is also being carried out on forms of application of AI and ML in which the software takes over at least parts of the diagnosis, e.g. by reducing the amount of data to be examined when analysing large amounts of data by weeding out presumably unproblematic findings of a screening. Medicine is hoping for advantages from AI and ML, such as reducing the workload of doctors and increasing efficiency as well as precision.

From a legal perspective, questions arise above all regarding the qualification of intelligent software as medical device software. Swissmedic and the European Commission set criteria that, if met, qualify software as a medical device. These criteria relate primarily to the medical purposes pursued by the software or to the examination purposes. The type of storage and processing – "on-premises or cloud" – has no influence on this.

9 Important is the Human Research Act (HRA), the Human Research Ordinance (HRO), the Federal Act on Human Genetic Texting (HGTA), the Ordinance to the HGTA (HGTO), the Therapeutic Products Act (TPA) as well as the Ordinance on Clinical Trials (ClinO).

10 Pseudonymisation of genetic data is required for data transfers to countries whose legislation does not ensure adequate data protection according to the assessment of the Federal Council (https://www.fedlex.admin.ch/eli/oc/2022/568/de#annex_1).

Accordingly, the decision "on-premises or cloud" does not change whether software is a medical device or not. In addition, questions of the doctors' diligence arise when using AI/ML-supported software, as well as liability issues. However, there are no cloud-specific requirements in this regard either. Whether cloud or not: the general rules of care and liability apply.

From a data protection perspective, provisions on automated individual decision-making may become relevant in AI/ML. However, an automated individual decision only exists if a decision with a legal consequence or significant impairment is made exclusively automatically (i.e. by a software or machine). Thus, if intelligent medical software is only used in an auxiliary manner, but doctors make the diagnosis, the corresponding data protection information obligations and consultation rights of the affected person do not become relevant. Even if they were relevant, these are also not provisions, whose application depends on whether the automated processing takes place "in the cloud" or "on-premises".

5. Medical devices in the cloud

Manufacturers and users of medical devices use cloud services in various forms. For example, platforms for the exchange of analysis data from the use of insulin pens can be stored on an IaaS-based[11] infrastructure. The platform itself may be provided in the SaaS model,[12] or the software used in the medical device may contain SaaS components. In addition, SaaS is used to combine data from different medical devices with further data – e.g. by connecting to an HIS or a laboratory information system.

The use of cloud components has no influence on the qualification as a medical device. According to Swissmedic, only the intended use (purpose)[13] of the software determines whether the software is a medical device.[14] "Cloud" is not a purpose, but a technical implementation issue ("path to the goal"). Thus, the use of cloud services does not determine whether medical device regulation is applicable at all.

If software is qualified as a medical device, the product safety and quality management requirements of the actors involved must be met. These requirements result from laws, regulations, and industry standards[15]. An analysis of the legal requirements shows that no requirements apply in the "cloud" context that would not also apply outside the cloud context. However, cloud-specific aspects of information security and other aspects of product safety must be considered when complying with the requirements.

Information security

Laws and other requirements rightly demand a high level of information security in the healthcare sector. This also applies to the requirements for software if it is considered a medical device. Whether sufficient information security has been ensured cannot be answered in the abstract. One must look at the concrete solution. Possible technical challenges of the regulation of medical devices cannot be illuminated here. The latter must be examined on a case-by-case basis, especially regarding technical industry standards, from which further requirements may arise.

11 **Infrastructure-as-a-Service**; these types of cloud services can free the health institution from having to operate its own data centres, hardware, and server software.

12 **Software-as-a-Service**; these types of cloud services are used so that the health institution does not have to operate and maintain certain software (operating software or user applications) itself.

13 The definitions of medical devices in art. 3 MedDO andart. 3 IvDO list purposes that qualify hardware or software as a medical device.

14 Swissmedic, Information Sheet Medical Device Software, 26 May 2021.

15 Relevant are the TPA, the HRA, the MedDO, the IvDO and the ClinO-MD. In addition, a number of industry standards must be complied with, namely with regard to information security, risk management, quality management and quality assurance for software for medical devices and for medical device software.

III COMMON RESERVATIONS AND POSSIBLE SOLUTIONS FROM A LEGAL PERSPECTIVE

Introduction

Notwithstanding the fact that there is agreement on the fundamental values that need to be protected, there are misunderstandings in the public discussion about the cloud. Because the need for protection is great, it is a common perception that the use of third-party IT infrastructures is challenging. A cloud service can often initially appear more complex to the health institution than its own familiar IT infrastructure. Health institutions then conclude that they cannot master the cloud. This is probably why there are reservations about the cloud. However, once the health institution has familiarised itself with the functioning of the cloud service and, in many cases, with the associated increase in information security, the new cloud infrastructure is easier to manage, leads to cost savings and higher information security. Similarly, legal reservations often do not stand up to factual scrutiny. Some of the reservations expressed in the public discussion will be addressed in the following.

Encountered reservations in detail

Reservation 1: "Doctor-patient confidentiality precludes cloud use"

"We are bound by doctor-patient confidentiality. We cannot comply with this obligation when using cloud services. Furthermore, contract processing is inadmissible under Swiss data protection law if the obligations to maintain professional secrecy cannot be complied with. Therefore, medical confidentiality stands in the way of cloud use."

Response: The reservation is unfounded. Doctor-patient confidentiality can also be protected and observed when using the cloud.

When cloud services are used, data processing is outsourced. In public discourse, it is often hastily assumed that outsourcing to the cloud is not even possible without the cloud provider gaining access to the data. Or it is argued that only encrypted storage prevents outsiders from gaining knowledge of confidential data.

Doctor-patient confidentiality must be respected by those who keep secrets – and not only because of the threat of punishment. The protection of secrecy enables patients to confide in their doctors even unpleasant or shameful complaints. Only this enables a careful examination and diagnosis with the patient's involvement. Accordingly, it is understandable and important that doctors carefully evaluate cloud services – also and especially regarding possible violations of doctor-patient confidentiality.

The fact that the cloud provider controls the entire system and could theoretically have the technical power to access data may lead the doctor to conclude that she or he would inevitably open the possibility for the cloud provider to actually perceive the data stored on the cloud infrastructure. However, this is not the case. In the case of mature cloud services, it is neither necessary nor reasonable to expect outsiders – e.g. support staff of the cloud provider – to "look" at the information and actually perceive it in the course of everyday normal use of the solution (normal operation). Only machines – not people – access the data in normal operation. The cloud provider must provide technical and organisational measures to secure this. Depending on the provider, encryption techniques already play a major role. The importance of encryption measures, encapsulation of information and controlled routing will continue to increase in the future.

However, medical confidentiality (according to Art. 321 SCC) is only violated if outsiders (people) actually perceive the information stored in the data. This actual perception is referred to as "plaintext access". Criminal liability also requires that the doctor or his or her assistant (e.g. practice assistant) must have actively disclosed the information or culpably and in breach of duty failed to adequately protect the data from plaintext access. As several legal opinions have already pointed out, this is not the case when using mature cloud services.

It is crucial that the cloud customer understands the cloud infrastructure used by the cloud provider and the processes assured by the cloud provider. For effective control can only be exercised by those who understand how the data processing at the cloud provider is supposed to look. This requires the willingness of the cloud provider to deal with the needs of its customers and to provide reliable answers.

Some cloud providers may require access to the customer's environment for support in very specific situations requested by the customer. If the support request cannot be handled with sample data, there may be incidental plaintext access to patient data. If the doctor wishes to act without consulting his or her patients, he or she must take contractual and organisational measures to include such cloud providers in the circle of those who belong to the doctor's office in the broader sense and thus to the doctor's sphere of responsibility. Today, many cloud providers are prepared to provide corresponding contractual assurances.

Reservation 2: "Cloud increases the risk of discrimination"

"Health data is sensitive data and particularly worthy of protection. Unauthorised access to or disclosure of such data poses a high risk to patients' privacy and fundamental rights, in particular the risk of being discriminated against. **The use of cloud services increases the impact and/or likelihood of discrimination**. This is unacceptable given the duty of care of health professionals."

Response: The concern is unfounded. The fact that the use of mature cloud services increases the risk of discrimination cannot be objectively justified.

It is true that health data is sensitive personal data. The latent risk of discrimination in health data must be addressed and mitigated – also, but not only, in cloud implementation projects.

It is not true that the involvement of a cloud provider per se leads to access by unauthorised third parties. At any rate, one should not make such a sweeping statement. It depends on the quality of the cloud provider. A provider with poor security measures can create a risk of an unintentional "expansion of the sphere of control". Then there may be increased risks.

In the opposite case – using a mature cloud service – the likelihood of unauthorised access is reduced. Thus, the risk of discrimination is also reduced.

However, there is no objective justification for increasing the risk of discrimination in a scenario of everyday and normal use of the solution (normal operation) without a data breach at the cloud provider. It should be mentioned in this context that the risk of a data breach at the cloud provider can in turn be reduced by technical measures (and cannot be ruled out in the context of other IT infrastructure).

Reservation 3: "Cloud cannot be controlled"

"Moving data to the infrastructure of a cloud provider leads to the loss of direct control over infrastructure and data. The law requires such direct control, as patients must not be placed in a worse position than if the hospital were to use its own infrastructure."

Response: The reservation is unfounded. Cloud computing does mean a paradigm shift, but with technically skilled implementation it does not mean a loss of control and may even allow for increased control and information security.

Health institutions operate in a very complex environment. They should embrace the opportunities of digitalisation, but not lose sight of important goals. It is a very challenging situation that health institutions find themselves in today. How does the cloud fit in here?

The response reads like a burden at first: health institutions need to have their organisation under control. Of course, this also applies to the use of cloud services by health institutions. The governing bodies must control the situation as a whole. They cannot simply ignore third-party providers, such as cloud providers.

For health institutions that have so far steered clear of cloud services, it may seem challenging at first glance to integrate a cloud service into their own organisation. The analysis in this regard is multi-layered and based on the examination of a multitude of factors. It is still true that whoever wants to control must understand.

Example "Storage location"

Concern: One cannot trace where the data is stored in the cloud.

Classification: Nowadays, the cloud customer can choose the storage location itself from existing options in most cloud services. One should choose cloud providers who contractually guarantee to only change the storage location on the instruction of the cloud customer.

Example "Processing abroad"

Concern: It is no longer possible to trace where the data is being processed in the cloud.

Classification: Many cloud providers can use process descriptions to make clear statements about which services lead to a foreign connection and in what way.

Example "Subcontractor"

Concern: It is no longer possible to trace who is accessing data.

Classification: The health institution does not have to acquire detailed knowledge of the cloud provider and/or the subcontractor down to the individual persons involved. It can rely on conceptual answers. This includes the identity of the subcontractors used and information on what support services they provide or how they handle the data in the cloud.

To achieve the control objective, the right knowledge must be brought on board. A transversal view of the situation is needed. To obtain such a view, the management can ask for help. But those who rely entirely on external resources make themselves dependent on the advisory approach. It should be the goal of the health organisation to not only serve short-term compliance, but rather to fully and thus transformatively adapt to the cloud situation. Those who recognise a cloud transformation as an opportunity for their own organisational development and the expansion of information security acquire real control (instead of compliance documentation) and take a big fitness step towards the future. Such an approach is a good idea anyway. It is beneficial to get right into it (but one misses this chance with a pure compliance approach).

One can only control what one understands. The reverse is also true. Sufficient understanding of processes that fulfil the control objectives leads to control. Understanding must address key aspects of cloud infrastructures, locations, security architecture and controls, contractual assurances, and applicable legal and regulatory requirements.

Health institutions can develop these responses. They can therefore also exercise comprehensive control in the new world of cloud computing. The means of exercising control are adapted to the new circumstances and are often different from what was known in the old days, when the institution's own staff still operated physical devices.

Just because something is different does not mean that control has been lost. In the meantime, better control can be achieved with modern instruments such as cloud services. At the same time, however, it is true that blanket statements are not possible. The IT infrastructure that is actually used must undergo an audit as part of the audit methodology and pass the corresponding tests.

Loss of control: crystallisation point, benchmark and starting point of the testing methodology

The following **requirements** should be checked with test **questions**:

- Confidentiality: Is the confidentiality of the information to be protected given?
- Availability: Is the availability given?
- Integrity: Can the health institution protect the information from unintentional modification?
- Integrity: Can the health institution demand that third parties delete certain information that flows out of the IT infrastructure?
- Accountability: Changes to or access to data must be clearly traceable at all times ("audit trail").
- Business continuity: Can the health institution maintain its business operations in the long term even after using a cloud provider?
- Traceability: Can the health institution ensure that it can decide at any time which IT provider it wants to work with?

The following **checkpoints** are important in deciding whether the health institution retains control over the IT infrastructures it wants to use:

- Admission: Can only authorised persons gain controlled admission to the IT infrastructures?
- Access: Can only authorised persons gain controlled access to the IT infrastructures?
- Plain text access: Does the cloud provider have access to the content of customer data as part of the general provision of cloud services?
- Support: Are there clear and assured access processes to data in support cases (where support becomes necessary at all)?

For all the points specified above, the significance of any events of the type described (e.g. a person may gain admission to the data centre) must be determined and how such events affect the legally relevant test questions (see above).

The control points are addressed by means of measures and it is then checked whether these measures are suitable to assume an appropriate risk in relation to the control point being tested. Measures are divided into those of a technical, organisational or contractual nature.

Reservation 4: "Cloud increases risks; for there are countless subcontractors"

"For us as a hospital, it is important to also keep control over IaaS providers who are subcontracted by e-health software providers. However, subcontracting is problematic because we will not directly control the IaaS providers."

Response: The reservation is unfounded. Control can also be observed when other subcontractors are involved. In particular, this requires contractual and organisational protective measures.

Data protection law permits the use of subcontracted processors by cloud providers. Conditions must be met for this, but in practice this is regularly successful.

The cloud provider may involve other providers (subcontracted processors) to perform its services. Insofar as these receive access to personal data (access to encrypted data is sufficient, i.e. without plain text access), the following must be implemented: The authorisation of the health institution is required but can be granted in general and in advance. The use of further providers by the cloud provider is therefore not an expansion of the sphere of control if the health institution controls and has the risks under control.

Flat-rate approval with concern of revocation

Regarding cloud services, the option of general authorisation with the right to object is customary in the industry and appropriate. With this model, the cloud provider is obliged to inform clients about the addition of new subcontractors or the replacement of existing subcontractors and to enable them to object to the addition, which can also be achieved by granting a right of termination.

The health institution should ensure that specific requirements resulting from legal requirements (e.g. assurances regarding the involvement of auxiliary persons under confidentiality law, etc.) are mapped by the primary system provider (SaaS provider) and that relevant subcontractors have also made corresponding provisions in their standard contracts. At the very least, there should be a documented explanation of the essential interrelationships.

Reservation: 5: "An explicit legal basis is needed"

"Hospitals with a service mandate from a canton must comply with **Cantonal data protection laws** when processing health data. The Cantonal laws require that all data processing be **based on a legal basis**. This legal basis must also cover cloud use."

Response: The reservation is unfounded. Even hospitals with a Cantonal service mandate can use cloud services without an explicit basis in the law. A legal basis is required for data processing and certain purposes of use – but not for the technology used (e.g. cloud computing).

The Federal Constitution and Cantonal constitutions require that state action be based on a legal basis. If authorities (have to) process personal data in their field of activity, they generally need an explicit special authorisation. Data processing by authorities should not take place without a legal basis. The requirement of the legal provision is of great importance in terms of the rule of law. As a control rule, the provision pursues the following cardinal objectives (in the sense of a so-called prohibition of expansion): (a) control over important topics (includes data protection), (b) protection against the state getting out of hand without legitimisation in the rule of law. The mere fact that an authority is entrusted with a task should not be abused for limitless data processing.

If the law ensures that (a) the scope of the use of the data is essentially known or can be inferred from the context (transparency requirement) and (b) the purposes of the use of the data do not get out of hand (certainty requirement), the requirement is satisfied. For the purposes of use not to get out of hand, they must be described in the relevant legal provision. The technology used to implement the steps in the life cycle of data is not a separate purpose of use. The fact that technologies such as cloud computing ("path to destination") are used for the purposes of data analysis does not change the purpose of use.

It is not part of the requirement of the legal provision that **the means of performing the task** are also limited in detail. For this reason, no independent legal basis is required for the so-called "administrative support activity". **Administrative support activity** means the procurement of those necessary material goods or services that the administration needs to perform its public task. Examples of this are the procurement of office supplies, the conclusion of contracts for work for the construction of a public building or the use of an ICT service provider. If the requirement of a legal basis is met for the actual activity of the state that requires legitimisation, **the associated administrative support activity is also covered by the legal basis and does not have to be explicitly mentioned.** For these, the legal basis is derived directly from the legal basis for the respective public task. A special legal basis is not required for activities within the scope of demand management.

As part of an implementation project, compliance with data protection law must be ensured, namely compliance with all data security requirements, and compliance with the data processing principles. Cantonal data protection supervisory authorities supervise the implementation project of the hospital with a Cantonal service mandate. There is therefore already sufficient protection under data protection law. **In contrast, the opinion that new technologies must always be regulated in a law in the formal sense cannot be upheld.**

In the public discussion, it is argued that citizens should not be placed in a worse position when cloud services are used than if the public institution were to perform the same task without using cloud services. This point of view implies that the use of cloud services may not be proportionate.

In such sweeping form, this concern does not stand up to legal scrutiny. When deciding on one of numerous suitable means, the authority has a large margin of discretion within the framework of the administration of needs. When choosing the means, the authority must keep in mind the public interest in an efficient, economic, and secure execution of public tasks as well as the legitimate data protection interests of affected persons.

Thus, a case-by-case assessment is required regarding specific cloud services, types of processing and the context as well as the types of data processed. Cloud services can certainly be used in such a way that no relevant encroachments on fundamental rights occur in the performance of the same administrative task.

Reservation 6: "A cloud with risks of access by authorities from abroad is inadmissible"

"The risk of access by foreign law enforcement agencies or intelligence services prohibits the use of cloud services."

Response: The reservation is unfounded. The discussion on this topic takes up too much space today; the issue can be solved with technical, organisational, and contractual measures.

Authority practices in all countries of the world should be divided and distinguished into two categories. The distinction is important because there are fundamentally different considerations to be made:

1 Surveillance: The state intends to carry out data analyses concerning a large number of people. An indeterminate number of people are affected by this. It is about the surveillance of society and possibly about multiple or undefined protection goals. However, we do not want to live in a surveillance state.

2 Criminal prosecution: The state intends to conduct criminal proceedings against an accused person. It is about individuals and not about an indeterminate number of persons. It is also not a matter of indeterminate protection objectives, but of enabling evidence to be gathered against an individual involved in the proceedings or yet to be involved.

In the first case **(surveillance)**, it is a question of whether and for what purposes acts of surveillance are acceptable in terms of the rule of law and society. A distinction can be made between mass surveillance (e.g. permanently recording video cameras, whereby all recordings are stored in a new data set and, if necessary, further investigated) and systematic data collection (also known as "bulk data collection", e.g. searching a set of data concerning a large number of persons on the basis of search criteria "telephone number" or "e-mail identification", whereby only positive hits are stored in a new data set and, if necessary, further investigated). Under data protection law, these issues are addressed and resolved in the cross-border context in the rules on disclosure abroad.[16] In practice, the risk of this type of foreign interference can be reduced or, over long distances, eliminated by the choice of storage locations (e.g. in Switzerland) or technical measures (e.g. encryption).

In the second case **(criminal prosecution)**, it must be assessed to what extent the procedural rights of the affected person are safeguarded in the criminal proceedings affecting them. In addition, it must be decided who should ensure that this is the case (their own state, a foreign state or, if necessary, a cloud provider). This consideration is prompted, for example, by the US CLOUD Act, which allows US law enforcement authorities to demand that the cloud provider active in their own state secure the cloud customer's data (legal hold) so that they can subsequently be brought into criminal proceedings.[17] This should also be possible if the data is stored abroad[18] (as long as the cloud provider has the possibility to actually disclose the data[19]).

16 Both the adequacy decisions under Art. 16 para. 1 FADP (incl. future rules on the Swiss-US Data Privacy Framework) and the mechanisms around transfers under the EU standard contractual clauses (Art. 16 para. 2 lit. d FADP) address and resolve this issue for the healthcare facility.

17 For more information on the US CLOUD Act, see our white paper "Public Cloud for Public Services – Solutions to Common Reservations" Public Cloud for Public Services – Solutions for commonly expressed reservations – not for public authorities only (lauxlawyers.ch)

18 It should thus be possible to do what is provided for (for certain data: subscriber information, but not content data) in Art. 18 of the Cyber Crime Convention (CCC). This reference is interesting because Switzerland has joined this international agreement.

19 In US law, this is referred to as "possession", "custody" and "control". Contrary to the processes, legal resistance assumes immediate plaintext access as soon as a US prosecutor applies for a legal hold from the cloud provider. However, this is not the case. The analysis of purely legal terms such as possession, custody and control fall short.

US CLOUD Act outcome: What changes will there actually be?

Ultimately, what exactly changes with the US CLOUD Act? Under the current concept of international mutual legal assistance, the USA, for example, receives content data from Switzerland (or "computer data" according to the terminology of the Cyber Crime Convention), if necessary, under certain conditions. When talking about risk considerations, the status quo should also be taken into account. Even today, Switzerland supplies content data (computer data) to the USA.

The discussion about the US CLOUD Act concerns the **law enforcement** aspect. But it is usually conducted too abstractly. Lawyers discuss access possibilities with purely legal approaches. But this examination does not answer the question that is actually of interest, namely: (1) whether there is de facto plaintext access by foreign authorities and (2) whether the fundamental values of our legal system are in that case still being adhered to. What we as a society actually want and what the patient wants: The patient must be protected from misuse of data ("uncontrolled expansion of the sphere of control"). However, in the context of the US CLOUD Act, one cannot seriously speak of an "uncontrolled expansion of the sphere of control" or a legally relevant loss of control. In the discussion, the focus on the essentials is getting lost.

US CLOUD Act: Not losing focus on the essentials

The hospital must protect patient data against misuse. However, the US CLOUD Act can in no way be seen as a risk of abuse. The US CLOUD Act does not contradict the fundamental values mentioned at the beginning. It is important to note that issues surrounding the protection of confidentiality only arise when it is already possible to give the affected person a legal right to be heard or at least give the health institution participation rights. This is discussed in detail in the publicly available legal opinion prepared for the City of Zurich.[20]

This having been said, the only remaining question is whether the remaining risk of foreign access in the cloud context can be dealt with appropriately. Within the framework of the implementation projects, all technical, organisational, and contractual measures should be examined and inventoried, insofar as they serve the purpose of protecting the client's data from being handed over to foreign authorities. Both the cloud provider and the client (as part of the implementation project) may be obliged to implement such measures.

20 www.lauxlawyers.ch/oiz-cloud-gutachten

Measures against access by authorities		
Measures	**Use against Surveillance**	**Use against Law enforcement**
"Defend Your Data" clauses	Yes	Yes
No access to contents of the customer data by the provider[21]	No	Yes
Recognition of official and professional secrecy[22]	seldom[23]	Yes
Confidentiality commitments	No	Yes
Location of the data centre: Switzerland	Yes	Yes
Organisational issues (e.g. access restrictions by approval processes involving the client)	seldom[24]	Yes[25]
Encryption	Yes	Yes
Further technical measures	Yes	Yes

"Defend Your Data" means clauses designed to protect against the release of data to law enforcement agencies, with the cloud provider implementing a comprehensive **cascade of defence:**

Cascade of defence	
Direct **referral** of the inquiring foreign authorities to the customer	
if this is not successful:	prompt **notification** of the customer (and efforts to remove any prohibition of notification)
if this is not successful:	Judicial **contestation** of: (a) Legal deficiencies under US law[26] (b) Conflicts with Swiss law[27]

21 No clear text access by the cloud provider as part of the general provision of cloud services; clear and assured access processes to data in support cases (where at all necessary).

22 E.g. Art. 320 SCC, Art. 321 SCC; Art. 62 FADP.

23 The benefit is not predictable and cannot be presented as a resilient measure in the area of mass surveillance.

24 The benefit is not predictable and cannot be presented as a resilient measure in the area of mass surveillance.

25 Can be treated as a measure in the area of access protection against measures of foreign law enforcement in the USA, "Control" to be negated with the US provider.

26 If you describe it in the abstract: "according to the law of the requesting authority".

27 So-called "blocking statutes" should also be mentioned in this context. These are in any case the prohibitions on a Swiss company to assist a foreign authority on Swiss soil without involving its own competent authority and coordinating the procedure with it (Art. 271 SCC, similar: Art. 273 SCC). The duties of secrecy under Art. 320 SCC and Art. 321 SCC can also be included.

Depending on the situation and the need for protection, it should also be examined whether increased or even almost absolute security should be provided (e.g. encryption technologies) if the primarily legal defence cascade should not be effective. However, this will only be appropriate or meaningful in rare cases. The hospital does not owe absolute protection against access in the context of criminal proceedings (e.g. under the US CLOUD Act). The "Bring Your Own Key" (BYOK) approach is often overestimated. "Hold Your Own Key" (HYOK) does bring more security to the discussion about access by authorities, but often at the price of unjustifiable additional risks. In many cases, even with HYOK, a (further) provider is integrated, which immediately relativises the protective effect gained.

Encryption: a good measure, surrounded by myths

Comprehensive encryption of all at-rest customer data is hardly ever mandatory. However, where such encryption is possible without significantly affecting the service design or the usability of the cloud services, it may be worth considering key management by the hospital itself.

Experience has shown that the measures outlined above (defence cascade and further measures) in their entirety lead to a de facto very extensive protection against access by foreign authorities.

US CLOUD Act: The hospital does not have to solve the Swiss Confederation's task

The digital world presents us with new challenges. If Switzerland wants to enforce its law enforcement claim, this may conflict with the design claim of other states (the same applies vice versa). The domestic interests of one state may require access to data stored within the territorial sovereignty of another state. The Swiss Confederation should address this issue; however, a hospital does not have to resolve this international conflict. The hospital, on the other hand, only (but still) must organise its own operations in accordance with the applicable law. This includes protecting Doctor-patient confidentiality. However, the US CLOUD Act is not an obstacle here.

Reservation 7: "The cloud is at odds with data sovereignty"

"Health data must be stored in Switzerland and may not be transferred internationally."

Response: The reservation is unfounded. Data sovereignty is a call to action for the Swiss Confederation, but not a barrier for the health institutions. The latter must necessarily, but also sufficiently, comply with the applicable law of Switzerland.

In the wake of digitalisation, efforts to regain sovereignty – the control that many nation states have increasingly lost in the past – are increasingly focused on the networked economy. Data sovereignty as an important aspect of digital sovereignty formulates what needs to be done in connection with data for the state to become sovereign. Regarding the sovereignty discussion, data sovereignty means narrowing the view to all questions about data.

Data sovereignty is a task that the Swiss Confederation must take on. To this end, it must take measures in the intergovernmental sphere. This can lead to special forms of international treaties, whereby the central demands from the Swiss perspective – the state's duty to take necessary action to protect data sovereignty (duty to protect) and starting points on how to improve interstate trade in digital, cross-border traffic – should be placed in the foreground. A central aspect of the duty to protect is to ensure access to the law.

Companies as well as health institutions must abide by the applicable law. Insofar as applicable law implements core elements of the duty to protect, the health institution will thus also integrate aspects of data sovereignty into its project goals.

However, a hospital does not have to comply with more than the applicable law. Data sovereignty or rather digital sovereignty does not result in any obligations for the health institutions to act or refrain from action beyond the applicable law.

This delimitation of competences also applies to public hospitals or other public health institutions to the same extent as it does to private health institutions, as a recent legal opinion prepared for the City of Zurich has shown.[28]

Practical experience shows that institutions in the healthcare sector (as well as those in the financial and public sectors) very often want to achieve more than what the law requires for good reasons. They want to secure their operations in the long term. The IT departments of such institutions rightly devote a lot of attention to continuity planning. However, the motivation for this is not the law, nor the sovereignty debate, but quite simply what good and prudent corporate governance dictates.

Conclusion: What remains of the reservations? After having discussed the most important reservations against the cloud as such in the healthcare sector, it becomes clear that the scepticism towards the cloud cannot be objectively justified. The focus should be shifted, and the internal energies should be spent on how to optimally protect oneself and, above all, the patients *with* the cloud.

28 www.lauxlawyers.ch/oiz-cloud-gutachten

IV ANNEXES

Elements of risk analysis

1. A future threat can only be described with statements about risk
If we knew what the future would bring, health data would also be easier to manage on electronic systems. But this is not the case. Thus, the health institution has to make a prognosis about the future and check how risky the management of a certain system is in the specific context.
It is obvious that the decision "cloud" or "not cloud" does not per se entail more or less risks. Every system decision requires a separate risk assessment. Not making a change to a system with greater security entails risks just as much as deciding to make a change and (also) encountering risks in the new system.

Risk statements should be made as follows:
- the target state should be described
- possible threats should be identified for the target state
- each of the identified threats should be assessed in terms of the likelihood of its occurrence (often referred to as **probability**)
- each of the identified threats should be further assessed in terms of damage potential (often referred to as **impact**)

2. Risk statements as a synthesis of probability and impact
The combination of probability and impact then permits a risk statement.

A concern that is not very likely to occur and, if it does, causes little damage, is a **small risk.**

Conversely, a danger that is very certain to occur and which, if it does occur, will also cause great damage, is a **great risk** (crossing an avalanche slope with a gradient of more than 30° after precipitation poses a great danger to life and limb, and it is very possible that an avalanche will break loose if one crosses the slope).

An event with potentially large damage potential, but which hardly ever occurs (meteorite impact), is assessed differently **(small risk)** than an event with medium damage potential, the occurrence of which is very likely **(medium risk)**.

3. Illustration using an example (information about the blood type)
Whether there is a potential for harm and how it materialises depends on the **context**. What is important here is that the type of information is not necessarily decisive. There is no automatism about risk statements in this respect. This is true although sensitive personal data is involved in the healthcare sector. In other words, there are no shortcuts to arrive at an adequate risk assessment. You must do the work and assess a risk concretely. The explanations in this appendix are intended to illustrate this.

The abstract information that an undetermined number of people have "Blood Type 0" is anonymous information (data protection law does not apply; **Scenario 01**). If a doctor reports that she or he has treated 8,000 patients with Blood Type 0 in her or his career of 35 years (**Scenario 02**), she or he is expressing aggregate information – the statement is of a statistical nature and is based on real personal data, but references to real persons are no longer discernible. A threat is objectively excluded in the first case (anonymous information that could be found in a textbook). In the second case, a certain (minimal) danger would arise at most if an investigation were to be conducted against the doctor based on the information, in the context of which the proof that she or he had cared for such a high number of such patients would be examined. Regardless of this: The risk is very low in both cases.

However, if the information "Blood Type 0" is linked to a person and thus individualised, one has to distinguish further scenarios to describe the risk, which the following should show:

• **Scenario 03:** Someone at a party casually reports that she also has Blood Type 0. The information is individualised. There are no special measures to protect the information. However, the information is soon forgotten by the conversation partner; he is not interested in it. One can hardly recognise a risk. Even if instead of the blood type, information about an existing, incurable disease had been exchanged: one could assume little risk.

• **Scenario 04:** Someone saves his blood type information in the electronic patient record. Thus, it is a question of the statement "I have Blood Type 0". There are protective measures prescribed in regulations. The affected person may have a very high expectation of technical security and protection of their data.

• **Scenario 05:** The employer happened to be at the next table at the party (Scenario 03) and overheard the information. Perhaps it deduces something from it. Whether blood group values have a potential for harm in the specific context? Perhaps not. If instead it were an indication of an incurable disease, which normally results in incapacity to work for several months to years in the near future, one can see: Unlike in Scenario 03, the risk assessment for Scenario 05 changes when the type of information changes. In Scenario 03 there was no significantly different risk assessment despite the changed situation, now there is; because the employer could have an interest in terminating the employment relationship. You can see: The context changes the risk assessment. In contrast, the information per se did not change the risk situation.

Consequential statement: Just because sensitive personal data is processed, this does not result in a maximum "swing" on the test scale (impact or probability). It would not be tenable to say that there is always a maximum risk with health data. It is not the data set (the information) that leads to the risk assessment, but the **context.**

Having identified the meaning of context, another "form of intensification" will be discussed. In the following examples, "real blood" is part of the processes, not "just" information about it:

• **Scenario 06:** A child is playing football. During the game, a ball hits the child on the head. A nosebleed occurs. The child throws the bloody handkerchief into the trash can. The waste collector empties the bin the next day. It is obvious: this is an everyday situation. Although a blood sample was in the bin and although information about the blood type could have been derived from it, there is a very small risk that the blood type information will actually be collected (or even subsequently misused) in this way. And if it is, it is very vague what danger would be derived from it. The references to the child are hardly visible. Someone with very high criminal energy would already have to be after the child. At least from today's perspective in Switzerland, we can say: It is not in our realm of experience that so much criminal energy is lurking around every corner. There is a low potential for harm with a low probability of occurrence.

• **Scenario 07:** A potential offender is accused of a serious crime (e.g. violent crime). The investigating authorities lack evidence to convict the perpetrator. The information about the blood type could be used to convict the perpetrator. A child of the accused has deposited a DNA sample with the online service 23andMe. The investigating authorities come across this information and can deduce the blood type of the accused from the information about the child[29]. This makes it possible to subsequently convict the perpetrator of the crime. From the point of view of the affected person (perpetrator), there is a considerable potential for harm. Initially (as his child had registered with 23andMe) one had to speak of low probability of occurrence. Looking at the energy of the law enforcement authorities in the current case, the risk of the probability of occurrence has changed. The law enforcement authorities had taken the seriousness of the case as an opportunity to make considerable inquiries (which they normally wouldn't do). The willingness to devote so much energy to the case changed the risk analysis considerably. The example shows that it is once again the context and not the information per se that concretely influences the risk analysis.

4. What remains

What does this mean in concrete terms for health institutions? In any case, one thing is clear: the fact that the maximum disadvantage is potentially conceivable in each case must not lead to the conclusion that there is necessarily an uncontrollable or high risk. This also applies when it comes to the management of health data. If one were to assume an uncontrollable risk and thus regard the path to the cloud as inadmissible, one would be **ignoring the context**. However, the context is crucial for assessing the risk. The prohibitive attitude is inadmissible. The risk-based approach applies, for which all circumstances (including those that speak in favour of a cloud deployment, such as massively higher processing capacities, greater system resilience or more comprehensive cyber security that is always up to date, etc.) must be assessed in the given context.

29 www.nytimes.com/2021/12/27/magazine/dna-test-crime-identification-genome.html

Directory of statutory bases

1. Data protection
- Federal data protection law: FADP, FODP (SR 235.1; SR 235.11)
- Cantonal data protection laws: e.g. IDG-ZG, IDG-BS and ordinances to the IDG
- European and international data protection laws, depending on the context: e.g. EU-GDPR

2. Criminal law
- Official Secrecy: Art. 320 SCC (SR 311.0)
- Doctor-patient confidentiality: Art. 321 SCC (SR 311.0)
- Art. 62 FADP (SR 235.1)

3. Special Federal health legislation
- Human Research Act (HRA), Human Research Ordinance (HRO), (SR 810.30; SR 810.301)
- Federal Act on Human Genetic Testing (HGTA), Ordinance on Human Genetic Testing (HGTO) (SR 810.12; SR 810.122.1)
- Therapeutic Products Act (TPA) (SR 812.21)
- Ordinance on Clinical Trials with the exception of Clinical Trials of Medical Devices (ClinO) (SR 810.305)
- Medical Devices Ordinance (MedDO) (SR 812.213)
- Ordinance on Clinical Trials with Medical Devices (ClinO-MD) (SR 810.306)
- Ordinance on In Vitro Diagnostic Medical Devices (IvDO) (SR 812.219)
- Federal Act on the Electronic Patient Record (EPRA) (SR 816.1)
- Implementing ordinances to the EPRA (SR 816.11; SR 816.111)

4. Special Cantonal health legislation
- Cantonal hospital acts, e.g. Hospital Act-BL, Hospital Act-AG
- Cantonal health acts, e.g. Health Act-ZH, Health Act-GE
- Cantonal patient acts, e.g. Patient Act-ZH
- Cantonal service mandates assigned to hospitals

5. Federal social security legislation
- Federal Act on the General Part of Social Security Law (SR 830.1)
- Federal Act on Health Insurance (SR 832.10)
- Federal Act on Accident Insurance (SR 832.20)

LAUX
LAWYERS AG
ZURICH | BASEL

ZURICH OFFICE
A Seegartenstrasse 2
P. O. Box 360 · CH 8024 Zurich
T +41 44 880 2424
W www.lauxlawyers.ch

BASEL OFFICE
A Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

Each registered with the
competent attorneys' register