Use of Cloud in the Healthcare Sector: What You Need to Know and Consider

A practical overview of cloud usage by healthcare institutions

Version 1.1, August 2026

Authors (in alphabetical order): Erik Dinkel, Stefan Hunziker, Stefan Juon, Philipp Stoll, Werner Ulmer

Contents

Introduction

This document provides healthcare institutions with an objective and independent basis for dealing with cloud solutions. It deliberately does not address specific providers or products, nor does it take a position for or against cloud usage.

The aim is to enable healthcare institutions to independently and responsibly address the topic of cloud usage. To this end, the document provides an overview of the key aspects and considerations that must be taken into account. The first part is aimed at a broad audience, while the second part focuses on concrete use cases and technical aspects for specialists.

Management summary

Healthcare institutions have a mandate to provide care to patients. This care must be ensured in an effective, appropriate, economical, and competitive manner. In addition, healthcare institutions are part of Switzerland's critical infrastructure and, as such, must guarantee the security of supply. Resilient ICT systems are therefore an essential prerequisite. The use of cloud services plays a central role in this context and is simply necessary. In an increasingly digital and interconnected society, where many applications and services can only be used online, cloud usage is a reality. Modern medicine and resilient systems are no longer possible without the use of cloud services.

Hyperscalers (large and globally operating companies that provide cloud services) are key and non-substitutable players in this context. Only they provide the required scalability, innovative capacity, skilled workforce, and interoperable products at the necessary scale. The question is therefore not whether hyperscaler services should be used, but rather which services should be used and how. In doing so, legal requirements must be considered across different use cases, and the risks associated with their use must be identified, assessed, and reduced to an acceptable level. Each organization—and thus each healthcare institution—must decide for itself whether specific services should continue to be operated locally or via cloud solutions.

In addition to application- and organization-specific risks, there are two central risks that must be clearly understood: vendor lock-in and system failure. If an organization's ICT infrastructure is fully or largely based on the cloud services of a single provider, and that provider is effectively not substitutable, switching providers—if possible at all—would involve enormous financial, human, and time-related effort. An outage of such a provider, for example due to a cyberattack or another event, would have serious consequences for all organizations relying on its services.

For example, if the services for video conferencing, telephony, and email of all healthcare institutions were based on the infrastructure of a single provider, and that provider were to fail, all healthcare institutions in Switzerland would become unreachable via these channels. The use of cloud services therefore not only increases the resilience of ICT systems but can also endanger it in such scenarios. It is therefore essential to establish redundancies and contingency planning.

However, refraining from cloud services is neither sensible nor feasible—also in the medical field—if healthcare institutions, as part of critical infrastructure, are to continue fulfilling their mandate for the benefit of patients and to ensure the provision of healthcare in Switzerland in the future. This document serves as a guide for healthcare institutions in addressing and using cloud services in a risk-appropriate manner.

General part – Overview and framework conditions

1 Introduction to cloud usage

The use of cloud services has long become a reality in an increasingly digital world. Digitalization is steadily advancing in the healthcare sector, which is already—or will soon be—no longer conceivable without digital solutions. This development creates new potential and opportunities from which society as a whole and individuals will benefit. Cloud solutions are a central component of the digital world, along with the opportunities and risks associated with them.

Between provision mandate and digital transformation

Within the framework of their service mandate and agreements, healthcare institutions ensure the provision of patient care, which must be effective, appropriate, economical, and competitive within the assigned region. Increasing interconnection with upstream and downstream providers—and thus the aim of achieving the highest possible level of integrated care—is a key focus. According to the Federal Council, healthcare institutions are part of Switzerland's critical infrastructure. To fulfil their mandate in crisis situations, resilient ICT systems are required. Cloud services are particularly well suited for this purpose. In addition, market developments among providers must be considered, as many applications and services are no longer offered on an organization's own local infrastructure ("on-premise").

Addressing the topic of cloud usage is therefore unavoidable for healthcare institutions. This document is intended to serve as a guide and to enable a structured and differentiated approach to the subject.

Structure of the document

The first part of this document is aimed at decision-makers in healthcare institutions, as well as at anyone interested in the use of cloud solutions. It covers the following topics:

- Different forms of cloud solutions
- The role of hyperscalers and the "Swiss Cloud" myth
- The development of cloud solutions
- Legal considerations regarding cloud usage
- The special case of the US Cloud Act
- Economic considerations related to cloud usage

The second part of the document is intended for individuals involved in the practical implementation of cloud solutions. It covers the following topics:

- The importance of cloud for backup and recovery
- Cloud-only vs. hybrid usage
- Use cases
- Technical and organizational measures
- Encryption and key management

2 Different forms of cloud solutions

Cloud services or cloud computing refer to the provision of IT resources—such as computing power, storage, application software, and databases—via the internet. Unlike traditional IT models, where organizations must operate their own servers and infrastructure, cloud services allow these tasks to be handled by third-party providers.

Cloud computing offers numerous advantages, including scalability, flexibility, reliability, and cost savings. Organizations can quickly and easily adjust the resources they need without requiring capital or personnel investments. Furthermore, cloud computing enables organizations to access a broader range of applications and deploy them more rapidly. Overall, it provides an innovative solution for organizations seeking to modernize and use their IT infrastructure more effectively.

Cloud computing is an approach for dynamically providing and using IT services (e.g., computing power, platforms, applications, or storage) over a network, tailored to demand. The provided resources are pooled and can be accessed and managed quickly with minimal effort or limited interaction with the provider. Billing is based on measured usage.

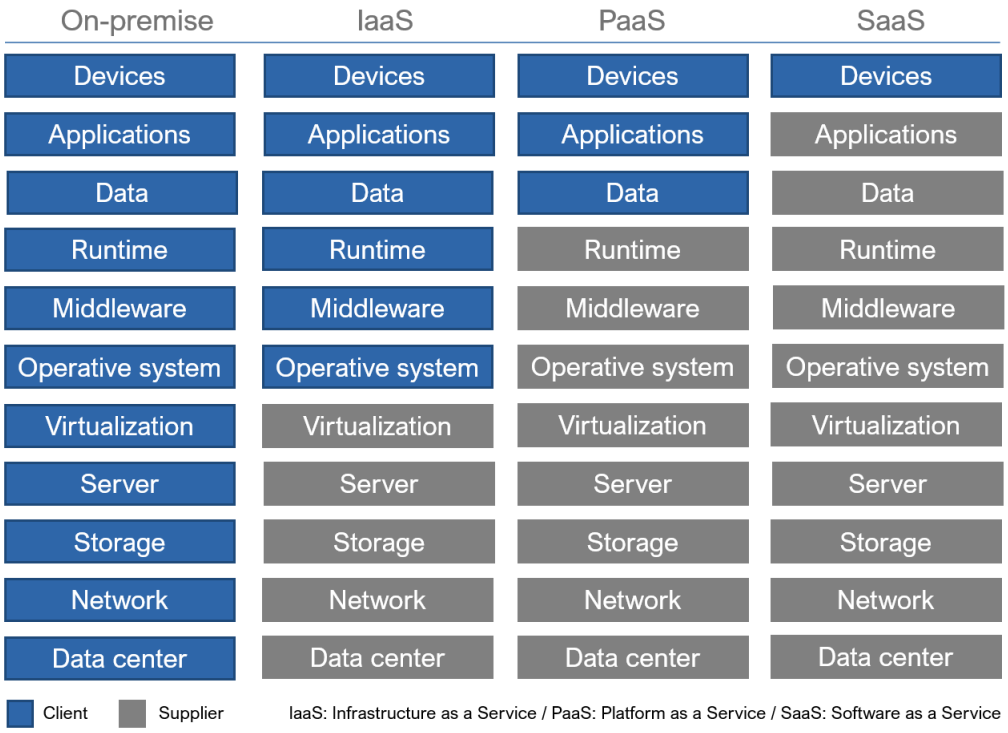
Cloud models: IaaS, PaaS, SaaS

Depending on the services provided and the responsibilities assumed, cloud services can be categorized into three service models:

- Infrastructure as a Service (IaaS): Provides fundamental IT infrastructure components such as computing power, storage, and network resources via the internet. Customers can run their own applications and operating systems on this infrastructure.
- Platform as a Service (PaaS): Offers developers a platform to build, run, and manage applications without having to manage the underlying infrastructure.
- Software as a Service (SaaS): Provides users with access to software applications delivered over the internet. These applications are hosted and maintained by third-party providers, while customers use them online.

These models differ, among other aspects, in how responsibilities are divided between the cloud provider and the cloud customer.

Overview of different types of cloud services compared to local systems (on-premise):



3 The role of hyperscalers and the “Swiss cloud” myth

Hyperscalers are large, globally operating companies that provide cloud computing services at massive scale. Some of the most well-known hyperscalers include Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, and Alibaba Cloud. These companies operate vast data centers around the world to provide IT infrastructure and cloud services.

Hyperscalers as drivers of the cloud computing market

The role of hyperscalers in the cloud computing market has become increasingly important in recent years. Organizations that rely on cloud services often seek solutions that are fast, scalable, and reliable. Hyperscalers are able to meet these requirements by operating large-scale data centers, enabling them to offer a wide range of IT infrastructure and cloud services.

By using hyperscaler cloud services, organizations can also achieve cost savings, as they no longer need to invest heavily in their own IT infrastructure. Hyperscalers offer a broad portfolio of services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which organizations can use depending on their needs.

In addition, hyperscalers possess a high level of expertise and advanced technology to support customers in the development, implementation, and management of cloud computing services. This makes them a key option for organizations seeking to remain competitive in today's business environment.

Overall, hyperscalers have become indispensable in today's cloud computing landscape. Without them, it would be significantly more difficult for organizations to respond quickly and flexibly to the demands of the modern business environment.

"Swissness" in the cloud context

The terms "Swiss Cloud" and "Swissness" refer to cloud services offered by Swiss companies and hosted in Switzerland. There is a widespread perception that these services provide higher standards in terms of data protection, security, and confidentiality compared to services from other providers.

It is important to note, however, that "Swissness" is not an officially recognized certification or label. Nevertheless, there are several reasons why Swiss cloud services are often regarded as particularly secure and trustworthy. Switzerland has strict data protection laws and high standards regarding privacy and data security. It is also politically stable, has a high degree of legal certainty and is neutral, all factors which contribute to an additional level of security and trust.

Furthermore, Swiss companies often have a strong reputation for quality and reliability, which can further enhance trust in their cloud services.

However, this does not automatically mean that all Swiss cloud services are inherently more secure or trustworthy than those offered by other providers. It is essential to carefully assess the specific characteristics and features of individual cloud services in order to determine the most suitable solution for the specific requirements of an organization.

4 Future development of cloud solutions

There are many forecasts and predictions regarding the future direction of cloud services. Some of the most important trends and developments include:

Multi-cloud strategies: Organizations are increasingly adopting a combination of cloud services from different providers to enhance the flexibility and reliability of their IT infrastructure.

Edge computing: The processing of data and applications is no longer carried out exclusively in centralized data centers, but also at the edge—closer to the end user or the data source. This enables faster response times and improved performance.

Artificial intelligence and machine learning: Cloud services provide an ideal platform for processing large volumes of data and running machine learning algorithms. This allows organizations to gain valuable insights from data and develop innovative applications.

Container technologies: IT containers package and transport software in a standardized way (similar to how shipping containers transport goods) and enable organizations to manage and scale applications more efficiently and flexibly. This will further simplify and broaden access to cloud technologies.

Cloud-only / hybrid cloud: Organizations are increasingly adopting hybrid cloud models that combine public and private cloud services. This allows them to benefit from cloud advantages without fully migrating their entire IT infrastructure to the cloud.

Hybrid cloud / on-premises: Part of the applications and infrastructure is operated in the cloud, while another part continues to run locally. One possible approach is to operate communication and collaboration applications in the cloud, while keeping core business applications—especially those involving structured and sensitive data—on local infrastructure (on-premises). Decisions on whether to run an application in the cloud or locally are made on a case-by-case basis, taking into account opportunities, risks, costs, and legal requirements.

Overall, the future of cloud services will be shaped by innovation and new technologies that enable organizations to use their IT infrastructure more effectively and efficiently. Organizations that leverage cloud

services will be able to respond more quickly and flexibly to the evolving demands of today's business environment, thereby maintaining their competitiveness.

5 Legal considerations for cloud usage

Cloud computing always involves outsourcing and therefore the processing of data by third parties. These third parties are contractually mandated to process data on behalf of the outsourcing healthcare institution. In this context, the data is not made public. This distinction is important, as different requirements apply to commissioned data processing than to data publication. However, responsibility for the data always remains with the outsourcing healthcare institution.

Data types and protection requirements

For legally compliant cloud usage, the first question concerns the data that is to be processed in the cloud: What type of data is involved? How sensitive is it? Depending on the type of data processed in the cloud, different legal and information security requirements apply. It is helpful to distinguish between the following categories:

- Public data
- Internal business data
- Confidential business data
- Personal data (which may be public, internal, or confidential)
- Special categories of personal data, such as patient data

Data state: identifiable, pseudonymized, anonymized

If the data is subject to professional or official confidentiality obligations—as is the case with patient data—not only data protection regulations but also professional secrecy must be observed.

Once it has been determined what type of data is to be processed in the cloud, the next question concerns the state of the data: Is it identifiable, or has it been pseudonymized or anonymized? Depending on this, does it still qualify as personal data?

Personal data is considered pseudonymized—or sufficiently pseudonymized—if it can only be attributed to a specific individual by third parties with disproportionate effort. Re-identification remains possible via an identification key. If this key is held exclusively by the data controller, sufficiently pseudonymized data may be regarded as anonymized from the perspective of the data processor.

In contrast, anonymization is irreversible. It is no longer possible to trace the data back to an individual. Fully anonymized personal data is no longer considered personal data.

Location for storage and processing

Finally, the location where the data is stored and processed must be considered: Is the data stored and processed in Switzerland, or abroad?

If it is processed in Switzerland, Swiss law applies, including professional and official secrecy. According to common practice, the data processor can be contractually bound to an appropriate level of protection, and violations can be enforced. However, a stricter legal interpretation—also supported by some supervisory authorities—argues that professional secrecy fundamentally precludes outsourcing to the cloud. Under such a rigid interpretation, the use of cloud solutions for processing patient data would effectively no longer be possible. In an increasingly digital society, this raises the question of whether hospitals and other healthcare institutions could still fulfil their mandate and ensure adequate medical care as part of Switzerland's critical infrastructure without using cloud services.

If data is stored and processed outside Switzerland, Swiss law does not apply; instead, the law of the respective country applies. Enforcement and legal remedies are only limited in such cases.

Legal requirements for processing sensitive data

If special categories of personal data—such as patient data—are to be processed in the cloud, a contractual basis for commissioned data processing is mandatory from a data protection perspective. The principles of purpose limitation and proportionality must be ensured. This means that data may only be processed by the service provider for the purpose for which it was entrusted by the data controller, and only the data strictly necessary for that purpose may be used.

For any new or significantly changed processing of special categories of personal data, a data protection impact assessment (DPIA) must be conducted. Depending on the applicable legal framework (federal or cantonal data protection law), prior consultation with the supervisory authority may be required.

If data is stored and processed outside Switzerland, this is only permissible if the level of data protection in the recipient country is at least equivalent to that of Switzerland. Although service providers abroad can be contractually bound to an equivalent level of protection, enforcement options are more limited, and the local (data protection) law applies. Due to the increased risk, full transparency regarding the processing of sensitive personal data abroad and explicit, verifiable consent from the data subjects are required. Naturally, all aforementioned legal requirements and duties of care also apply in such cases.

Finally, all processed data must be protected in accordance with the current state of information security. This means that appropriate safeguards must be in place, such as encryption during transmission and storage, as well as role-based access controls.

6 Special case: US Cloud Act

The use of cloud computing for commissioned data processing involving special categories of personal data—such as patient data—is generally permissible under prevailing legal practice, provided that an appropriate contractual basis exists and the necessary information security measures are in place. This applies in particular when the cloud infrastructure is located in Switzerland.

However, a special case arises from the extraterritorial application of the US Cloud Act. Under this law, U.S. authorities may, in the context of an ongoing criminal investigation, request access to the data of a person held by companies with ties to the United States. If an organization—or a healthcare institution—processes data in a cloud environment provided by a company with U.S. ties, U.S. authorities may potentially gain access to that data, even if the cloud infrastructure used is located in Switzerland.

For this reason, the processing of patient data by a cloud provider with U.S. ties is problematic from a data protection perspective and must be assessed carefully on a case-by-case basis. In general—and particularly when dealing with providers with U.S. ties—it is essential first to clearly define and specify the relevant applications. Based on these use cases, risks, opportunities, and costs must be weighed, and legal requirements must be assessed.

In addition to confidentiality, the integrity and availability of data must also be considered. The latter is critical to ensuring the operation of a healthcare institution and, therefore, to maintaining the security of supply within critical infrastructure. Based on the findings of such an analysis, appropriate measures must be defined and implemented promptly to eliminate risks or reduce them to an acceptable level.

6.1 Note on Privacy Shield 2.0 and the Swiss-U.S. Data Privacy Framework

On 10 July 2023, the European Commission adopted the adequacy decision for the EU-U.S. Data Privacy Framework, which is also sometimes referred to as “Privacy Shield 2.0”. The decision establishes that the United States ensures an adequate level of protection for personal data transferred from the EU to U.S. companies that are certified under the EU-U.S. Data Privacy Framework and included on the relevant list maintained by the U.S. Department of Commerce. In principle, personal data may be transferred to such companies without additional data protection safeguards.

For data transfers from Switzerland, a corresponding Swiss framework has been in place since 15 September 2024 in the form of the Swiss-U.S. Data Privacy Framework. The Federal Council has included the United States, with respect to personal data transferred to U.S. companies certified under this framework, in the list of countries or specific sectors providing an adequate level of data protection. Such data

transfers may therefore, in principle, be carried out without additional safeguards pursuant to Article 16(1) FADP. Transfers to non-certified U.S. companies, however, continue to require appropriate safeguards pursuant to Article 16(2) FADP.

The legal and institutional stability of these data protection frameworks must, however, be reassessed in light of the U.S. Supreme Court's decision of 29 June 2026 in Trump v. Slaughter. The Supreme Court held that the statutory provision under which members of the Federal Trade Commission could be removed only for certain important reasons – in particular neglect of duty, incapacity, or misconduct in office – was incompatible with the constitutional separation of powers. FTC Commissioners may therefore, in principle, be removed by the President without the need to establish such grounds for removal.

This decision is relevant to the Swiss-U.S. Data Privacy Framework because the FTC is responsible for enforcing the data protection principles with respect to most participating U.S. companies. Switzerland's 2024 adequacy assessment expressly proceeded on the assumption that FTC Commissioners could be removed during their seven-year terms only for good cause and, on that basis, classified the FTC, together with the U.S. Department of Transportation, as an independent supervisory authority. The removal of this protection against dismissal therefore constitutes a material subsequent change to one of the foundations on which the Swiss adequacy assessment was based. It may give rise to doubts regarding the institutional independence of the FTC and the extent to which enforcement of the Swiss-U.S. Data Privacy Framework is protected from political influence.

The Supreme Court's decision does not, however, directly invalidate the Swiss-U.S. Data Privacy Framework. Switzerland's adequacy recognition remains formally applicable unless and until the Federal Council amends the relevant provisions of the Data Protection Ordinance or a competent authority or court reaches a different conclusion. In view of the changed institutional circumstances, however, a renewed review of the Framework is to be expected. Companies relying exclusively on the Swiss-U.S. Data Privacy Framework for data transfers should monitor further developments and, particularly where sensitive personal data or large volumes of personal data are concerned, prepare supplementary or alternative safeguards.

Whether the introduction of the EU-U.S. and Swiss-U.S. Data Privacy Frameworks affects the specific case of the U.S. CLOUD Act remains a matter of debate. The two data protection frameworks do not remove the statutory powers of U.S. authorities to require U.S. providers to disclose data where the conditions of the CLOUD Act are met.

From the current perspective, this document therefore assumes that the specific case of the U.S. CLOUD Act must continue to be considered separately. Rather, the Supreme Court's decision reinforces the need to regularly assess not only the formal certification of a U.S. recipient, but also the actual risks relating to access, oversight, and legal remedies.

7 Economic considerations of cloud usage

With the emergence of cloud offerings and the shift from on-premises solutions to subscription-based licensing models, the financial perspective on software usage in organizations has fundamentally changed. Whereas hardware and software were previously purchased outright, software is now increasingly procured "as a service" on a subscription basis. As a result, investments are no longer capitalized but instead treated as operating expenses (shifting from CapEx to OpEx). This reduces financial risk, as no upfront investments need to be planned and executed, and eliminates the need for capitalization, typically followed by a four-year depreciation period and inflexible capital commitment.

This model (OpEx) provides significantly greater flexibility. Solutions can be adjusted more quickly to actual needs, and the burden of maintenance financing is reduced. Depending on the chosen subscription model, technical updates can usually be implemented immediately or at least much faster than under a traditional purchase model (CapEx). In addition, the adoption of new technologies can be accelerated considerably.

A key economic advantage of cloud computing lies in the flexibility it provides. It enables organizations to rapidly adapt their IT environment to changing requirements and needs. Given the ongoing and accelerating digitalization of society, this capability is becoming increasingly important. This is particularly true for the healthcare sector, which is also undergoing rapid digital transformation.

However, it would be incorrect to assume that a cloud-based solution is always cheaper than a local on-premises solution. The financial impact must be assessed and compared on a case-by-case basis, taking into account specific use cases and the associated efforts required to ensure compliant and secure usage. It is also important to consider that cloud providers may adjust or increase prices over time, while exiting a cloud solution can also entail significant costs.

8 Geopolitical aspects

In light of recent geopolitical developments, it is essential to consider not only the points mentioned above but also the broader geopolitical environment and the unpredictable behavior of certain actors.

Given these developments and the new reality we are facing, it cannot be entirely ruled out that, for example, arbitrary tariff increases or regulatory restrictions could impact operators or users of cloud services; that connections or services could be restricted or interrupted to exert pressure; or that a provider's data center could be physically destroyed as a result of war—as occurred in early March 2026 during a missile attack on a data center of Amazon Web Services in the United Arab Emirates.

These risks are further amplified by the high level of dependence on a small number of global providers. Overall, this results in a complex risk profile that encompasses not only technical but also strategic and security policy dimensions, and that can directly affect the security of supply in the healthcare sector. These factors must be taken into account when making decisions, weighing risks, opportunities, and alternatives, and implementing appropriate measures.

Specific part – Details for practical implementation

9 The importance of cloud for backup and recovery

Business impact analyses, combined with the short recovery time objectives (RTO) and recovery point objectives (RPO) required by healthcare institutions, demonstrate the critical importance of high ICT availability. Failure events show that, in the worst case, a healthcare institution can continue to operate temporarily without substantial IT support, however at the cost of significantly reduced productivity and considerable effort required to maintain and reconstruct essential information flows. Within a multi-layered business continuity management framework, cloud solutions offer robust and scalable approaches to ensuring or restoring operational continuity more effectively.

Another advantage of cloud solutions is that expertise, service, and support are typically provided by the vendor, and system and software updates are managed by the provider. As a result, systems are generally patched promptly and security vulnerabilities are addressed quickly. Service level requirements must be contractually defined, and depending on the type of cloud service, responsibility is shared to varying degrees between provider and customer.

An additional challenge is the integration of data from medical technology systems. Various manufacturers of devices—such as pacemakers or blood glucose monitoring systems—store data in proprietary cloud solutions. For optimal patient care, this data should be aggregated and made available within the systems used by the interprofessional care team.

Note: When using medical technology products, the guidelines of the Swiss Medical Association FMH must be observed.

10 Cloud-only vs. hybrid usage

The transition from the currently predominant on-premises model to the cloud is a long-term process and depends on various factors:

- Availability of cloud-based offerings and the discontinuation of local applications or services
- Reduction of legacy systems that are not cloud-compatible
- Legal requirements and data protection regulations
- Coexistence of private and public cloud services
- Emergence of new services that exist exclusively in conjunction with the cloud (e.g., telemedicine, remote monitoring of patients, use of wearables)

More focus on business needs instead of technology in internal ICT organizations

The core competency (Unique Selling Proposition, USP) of an ICT department within a healthcare institution lies in acting as a transformation layer between technology and the core processes of diagnosis and treatment of patients. Without a solid understanding of both domains, proactive consulting and support aimed at value creation cannot be effectively achieved.

Basic technologies and infrastructures are increasingly becoming commodities. The challenge for internal ICT departments is therefore to orchestrate different components and providers and to manage complexity in an optimal way.

IT challenges: skills shortage and digital transformation

Digital transformation in the healthcare sector lags approximately ten years behind other industries (such as banking, insurance, and telecommunications). This gap is also evident—at a comparable level—when looking at international benchmarks (e.g., Estonia, Singapore, United States).

As a result, there are still many local, mostly client-server-based applications in use, often lacking a clear separation between layers (data, business logic, and presentation). The providers of these systems are typically small and medium-sized enterprises (SMEs), which, over the long term, often face limitations in their ability to provide sustainable operational support and further development.

The shortage of ICT specialists is particularly evident in two areas. On the one hand, ICT education is not very attractive for individuals entering the healthcare sector. On the other hand, healthcare institutions are not competitive in terms of salaries for highly specialized professionals (e.g., Microsoft 365 engineers, enterprise security architects, etc.). In addition, regardless of their use of cloud services, healthcare institutions must manage a large number of network-connected medical devices. This creates a niche area that requires highly specialized IT personnel with specific expertise.

11 Use cases

11.1 Video telephony

Video telephony transmits audio and video data in real time. As a rule, this involves only the transmission of data and not its storage. An exception applies if recordings are made for purposes of traceability or quality assurance.

Key assessment questions:

- Can video telephony be technically limited to the pure transmission of audio and video data?
- Is it known which metadata is stored by the service provider for signaling purposes, and whether this storage and subsequent processing comply with legal requirements? Does the provider adhere to the principle of data minimization, meaning that only data strictly necessary for the intended purpose is collected and processed?
- Does video telephony—and the transmitted audio and video data—constitute personal data? Not only user data but also the visual data of participants may be relevant, as these may require protection of privacy.

- It is recommended to use a virtual background, as commonly available in most applications. However, this functionality is often only available in installed applications and not when participating via a web browser. In such cases, it is advisable for the meeting organizer to inform participants that turning off the video camera is permitted to protect privacy. This information should ideally be communicated in the invitation or at the latest at the beginning of the meeting.
- At a minimum, can user data be encrypted? Is encryption end-to-end, or does it only apply during transmission (data in transit) or storage (data at rest)?

If recordings are made, both audio and video data are stored. This raises additional questions:

- What is the purpose of the recording? How long is the data stored? Can the retention period be adjusted or reduced? Is it ensured that the data will not be used for other purposes and will be deleted within a reasonable timeframe once the purpose has been fulfilled?
- Is there a legal basis, a legitimate interest, or the consent of the participants for this data processing? Does this also apply to the user data transmitted during the video session?

Risks of cloud-based communication

A broad or even organization-wide use of cloud-based communication services creates a high level of dependency on the service in terms of availability. A major disruption at the provider level, or an impairment of access to the service (e.g., connectivity issues), can have a significant impact on the operation of a healthcare institution. This impact is particularly critical for internal and external communications relevant to emergencies. It is therefore recommended to establish fallback options in the form of redundancies and to regularly test them using realistic scenarios.

The increasing integration of algorithms by service providers to detect inappropriate content (e.g., based on artificial intelligence) carries the risk that transmitted medical images may be incorrectly classified as inappropriate or pornographic and consequently blocked. Such functions can have a significant impact on specific use cases, such as telemedicine. These features are often introduced by providers without prior notice or with very short notice, making it difficult for healthcare institutions to respond in time. It is therefore important to clarify early on with the provider how such algorithms can be configured or overridden.

In summary, the use of video telephony in healthcare institutions offers significant advantages and can create substantial added value in many use cases. However, it is essential not to be guided solely by these advantages and to carefully evaluate any broad or widespread deployment in the healthcare sector. Scalable and hybrid operating models have proven effective, particularly where communication critical to emergencies continues to be handled via traditional local services.

11.2 Collaboration

Collaboration is generally understood as interaction via video telephony, complemented by the simultaneous joint editing of centrally stored data by internal and external participants. In essence, the use case described under (a) for video telephony is extended to include the storage and processing of data, typically within the cloud environment of a service provider.

Key assessment questions:

- Can it be ensured that centrally stored data is adequately protected against unauthorized access (protection goal: confidentiality) and unauthorized modification (protection goal: integrity)?
- Can the data be restored in the event of loss within the cloud environment of the service provider? (protection goal: availability)
- Can access to and changes made to the data be traced?
- Is the assignment of access rights exclusively the responsibility of the owner of the shared workspace or explicitly authorized individuals (delegated administration)? Or is it possible for any participant to share data with third parties?

11.3 Messenger

Instant messaging (chat) generally refers to the transmission of short messages to an individual or a group. In addition to plain text, the content may also include images or documents as attachments. Messages are typically stored so that they can be accessed at a later point in time. Transmission usually takes place within a protected address space, meaning that messages can only be sent to participants who are members of that space.

Key assessment questions:

- Is it always clear to the sender of a message who has access to its content?
- Can it be ensured that the transmitted data is not used by the service provider for additional purposes (e.g. WhatsApp)?
- Is it known which metadata is collected and stored in connection with message transmission, for what purposes, and by whom it is processed? Does the service provider adhere to the principle of data minimization?

11.4 Email

Email refers to the transmission of text and data via a dedicated application, often a specialized email client. In practice, this application is not only used for communication but also for storing information, typically within a folder structure inside the email client.

Key assessment questions:

- Is the encryption of data during transmission fully ensured?
- Can digital signatures be used to verify the authenticity of the sender through cryptographic methods?
- Is there a separate option for encrypted email transmission that goes beyond basic transport encryption?

11.5 Clinical and administrative systems

Clinical and administrative systems are used for processing patient data, and therefore particularly sensitive personal data, as well as employee data, which may also include sensitive personal information. This generally includes all information systems and specialized applications, as well as the associated peripheral systems and supporting services used in this context.

Key assessment questions:

- Can it be clearly determined in which country (legal jurisdiction) and, ideally, in which specific data center location of the service provider the data is stored?
- Can it be ruled out that auxiliary services (e.g., for analytics or similar purposes) are used in connection with the service, which would transfer data to a country that does not provide an adequate level of data protection?
- Can it be fully verified that the data is encrypted at least during transmission (data in transit) and storage (data at rest), and optionally also during processing (data in processing)?
- Is it ensured that key management is performed by the customer (service recipient) or a designated third party, rather than by the service provider?
- Can it ideally be ensured that data is already encrypted by a third-party service before being transmitted to the provider's cloud environment?
- Is the customer aware of potential access points through which the provider could access plaintext data, for example through the creation of memory dumps of running systems for support purposes?
- Does the customer know from which country the provider delivers support services? Can it be verified that no sensitive data needs to be transferred to countries without an adequate level of data protection for operational support purposes?

- Is the service provider willing and able to disclose its subcontracting arrangements? Does the provider have an obligation to inform the customer, and does the customer have a right of veto if a new sub-contractor is introduced during the contract term?
- Can the customer ensure a complete withdrawal from the provider's cloud environment within a reasonable timeframe (typically three to six months) without significant service disruption? Can this also be guaranteed in the event of a change in ownership of the provider?
- Can the customer ensure that, in the event of data loss, all data can be fully restored while complying with all security requirements?
- Can the customer maintain an adequate level of service if it is affected by disruptions in the provider's cloud environment? (service continuity)
- Does the provider grant sufficient audit rights to the customer (e.g., penetration testing and auditing)? Does the provider make external audit reports available to the customer?
- Can the customer rely on sufficiently available connectivity to the provider's cloud environment?
- Has the customer conducted a risk analysis in line with regulatory requirements and does it manage these risks throughout the entire lifecycle of the service?

12 Technical and organizational measures

12.1 Determination of risks by use case

In the previous section of this document, the different use cases were described and key assessment questions were outlined. The answers to these questions help identify existing risks. The use of a risk catalog is also helpful to determine whether a specific risk applies or not. A risk catalog may, for example, include the following risks (based on the ENISA Cloud Computing Risk Assessment).

Organizational risks

R.1 Vendor lock-in

R.2 Loss of governance/control

R.3 Compliance challenges

R.4 Reputational damage

R.5 Failure or degradation of cloud services

R.6 Acquisition of the cloud provider

R.7 Supply chain failure

Technical risks

R.8 Over- or under-provisioning of resources

R.9 Insufficient isolation from other customers in the cloud environment

R.10 Insider risk at the cloud provider

R.11 Compromise of cloud application interfaces

R.12 Interception or eavesdropping during data transmission

R.13 Data theft during upload or download

R.14 Inadequate data deletion

R.15 Distributed Denial of Service (DDoS)

R.16 Economic Denial of Service (EDoS)

R.17 Loss of encryption keys

R.18 Malicious internet scanning activities

R.19 Compromise of cloud service infrastructure

R.20 Conflicts between local backups and cloud backups

Legal risks

R.21 Legally enforced access to data

R.22 Changes in the legal framework

R.23 Data protection risks

R.24 Licensing risks / license violations

Once risks have been identified, the next step is to determine their impact. This involves estimating—based on empirical data where possible—the likelihood of occurrence and the magnitude of potential damage (impact).

Evaluation of potential damages

Alternatively, minimum and maximum impact levels can be estimated for each risk. When assessing impact, it is helpful to consider the dimensions of confidentiality, availability, integrity, and traceability, and to evaluate the consequences for the healthcare institution. For example, what happens if a service outage compromises the availability of dependent systems?

In practical terms, this means assessing the potential damage to a healthcare institution if video telephony, collaboration platforms, messaging services, email, or clinical and administrative applications become unavailable; if data is stolen, manipulated, irreversibly deleted, or destroyed; or if the integrity of information or the traceability of activities is no longer ensured.

A key factor is the type and volume of data processed in the cloud or within specific applications, as well as the processes involved and their criticality for the healthcare institution. Additionally, the loss of sovereignty over data associated with cloud usage, dependency on the cloud provider (vendor lock-in), and the risk of cyberattacks via cloud-exposed systems must be taken into account.

Risk minimization measures

Once risks have been identified and their impact assessed, the next step is to evaluate which measures are already in place to mitigate them and whether the remaining (residual) risk is acceptable to the healthcare institution. If the residual risk is deemed too high, additional measures must be implemented until the risk is reduced to an acceptable level.

Confidentiality, availability, integrity, and traceability must be adequately ensured. For this purpose, it must be defined how these objectives are achieved and what residual risks remain. The goal is to reduce residual risks to an acceptable level while complying with legal and regulatory requirements.

Solutions must be in place and responsibilities clearly defined for the following areas:

- Authentication
- Authorization
- Logging and auditing
- Data backup
- Software updates / patch management
- Perimeter protection (e.g., phishing, email security, attachments)
- Information protection (based on data classification)
- Data Leakage Prevention (DLP)
- Security Information & Event Management (SIEM), threat intelligence
- Security of endpoints connected to the cloud (endpoint protection)

In principle, it must be assessed whether these requirements can be met by solutions provided by the cloud provider, whether those solutions should be used, or whether a multi-vendor strategy with alternative products should be pursued.

A key consideration is which security solutions the healthcare institution already uses, how satisfied it is with them, and whether the cloud provider's solutions offer advantages in terms of effectiveness and/or cost. It must also be considered whether and how existing solutions can be integrated.

12.2 Encryption and key management

To adequately protect data, encryption is a key measure. A distinction must be made between: 1) encryption during transmission (in transit), 2) encryption of data at rest (in storage), and 3) encryption during processing (in use / in process). Encryption during data transmission to the cloud is mandatory and undisputed: it must always be ensured.

Points to consider for encryption at rest

With regard to encryption of data at rest in the cloud, different key management solutions exist depending on the cloud provider, and these must be carefully evaluated. This is a prerequisite for processing data in the cloud. In other words, if key management is not properly ensured, the cloud, including the use cases described above, cannot be used.

A key differentiating factor is whether key management is handled by the cloud provider within the cloud (with each customer receiving their own key), or locally by the healthcare institution itself. If key management is handled locally, the healthcare institution bears full responsibility.

If key management is handled by the cloud provider, the provider guarantees and is responsible for its functionality. However, this introduces the risk that the provider or individual employees with sufficient privileges could gain unauthorized access to the keys and thus to the data. This risk does not exist in the same way with local key management. Therefore, it is essential to consider how access to keys is controlled.

Additional security can be achieved through solutions that require any access by the cloud provider's staff to be explicitly authorized. Such authorization can be performed either by designated personnel within the provider organization with oversight responsibilities or by authorized personnel from the healthcare institution itself.

It should be noted that individuals responsible for granting such authorizations must be available in accordance with the required service levels. If service level agreements require provider administrators to perform support activities outside regular business hours, those responsible for approving access must also be available outside those hours. Otherwise, administrators may be unable to act despite being ready to provide support.

Points to consider for encryption during processing

A particular challenge is the encryption of data during processing (in use / in process), especially when the execution of SaaS solutions takes place directly in the cloud rather than locally or in the browser. Available solutions vary between providers and generally involve a certain level of complexity, potential error susceptibility, and limitations in functionality.

Encryption during processing requires that users (internal and external) working with data in the cloud use encryption keys that are not held by the cloud provider. Accordingly, cryptographic management must be handled by the healthcare institution. For example, in collaborative scenarios where a healthcare institution processes data with external partners via a cloud application, external partners must first access the institution's infrastructure to obtain a certificate (key), which they then use to decrypt and process data within the cloud application.

This setup alone is complex and introduces risks to availability. In addition, the chosen encryption solution must be sustainably compatible with the respective cloud application. If compatibility is not ensured, the application cannot be used with the encryption solution.

Whether a viable solution for encryption during processing exists for a given cloud application—and what functional limitations it entails—must be assessed on a case-by-case basis. Currently, no solution is known that provides fully reliable encryption of data in use while maintaining full functionality. If encryption during processing is not implemented, full functionality is retained; however, during processing, the data may potentially be accessible to provider staff with appropriate access rights.

Note: This document is available in multiple language versions. In case of doubt, the German version shall prevail.

About the authors

Erik Dinkel

Erik Dinkel has been CISO since 2018 and, since 2024 also Chief Security Officer at the Universitätsspital Zürich (USZ). Prior to joining USZ, he worked in Business Risk Management and as Head of Access Governance at Credit Suisse Switzerland. He holds a Master's degree (M.A. UZH) in Political Science from the University of Zurich and has completed advanced training in corporate management, risk management, and information security (CAS UZH, CAS FHNW, BSI). Since 2021, he has been a lecturer in cyber and information security at the Hochschule Luzern, and since the end of August 2025, he has served as President of the newly established Healthcare Cyber Security Center.

Stefan Hunziker

Stefan Hunziker, a medical doctor with a degree in business informatics, led medical informatics from 2002 and the IT division of the LUKS Gruppe from 2012 to 2025. In addition, he represented the IT division as CIO on the executive board of the LUKS Gruppe from 2021 to 2025. During this time, he was primarily responsible for the IT integration of Nidwalden Hospital into the LUKS Gruppe. Since 2026 he has been supporting the Universitätsspital Zürich as a project manager in digital transformation.

Stefan Juon

Stefan Juon worked at the Kantonsspital Graubünden from 2009 to 2022 in various roles, most recently (2016–2022) as CISO and Co-Head of ICT. He holds tertiary-level qualifications in engineering and business administration, as well as advanced certifications in information security, risk management, and IT architecture. He is also certified in ITIL, TOGAF, and as a CISA.

Philipp Stoll

Philipp Stoll is a trained mechanical engineer. For the last 20 years until his retirement, he was a member of the hospital management of the Universitäts-Kinderspital beider Basel (UKBB). Since then, he has been working as a consultant for companies in the healthcare sector. His areas of expertise include construction, logistics, procurement, maintenance, medical technology, and security, with a particular focus on the interface between users and planners. Since 2011, he has also been a delegate of H+ to the Federal Office for Civil Protection (FOCP) and the Federal Office for National Economic Supply (FONES).

Werner Ulmer

Werner Ulmer has been CISO of the Department of Economic Affairs of the Canton of Zurich since 2024. Previously, he served as CISO of the Kantonsspital St. Gallen (now HOCH Health Ostschweiz) and its hospital network, where he was responsible for the strategic and operational development of information security, culminating in successful ISO 27001 certification. With solid academic and professional training, including studies in information security and IT management at the Hochschule Luzern,and many years of experience, he has extensive expertise in cybersecurity, information security, risk management, and security governance.