Cloudnutzung im Spital- und Gesundheitswesen: Was man hierzu wissen und berücksichtigen muss

Eine praxisnahe Auslegeordnung zum Thema Cloudnutzung durch Gesundheitseinrichtungen

Version 1.1, August 2026

Autoren (alphabetisch): Erik Dinkel, Stefan Hunziker, Stefan Juon, Philipp Stoll, Werner Ulmer

Inhalt

Einführung 2
Management Summary 2
Allgemeiner Teil – Auslegeordnung und Rahmenbedingungen 3
1 Einleitung Cloudnutzung 3
2 Verschiedene Formen von Cloudlösungen 3
3 Die Rolle der Hyperscaler und Mythos Swiss Cloud 4
4 Weitere Entwicklung der Cloudlösungen 5
5 Rechtliche Überlegungen zur Cloud 6
6 Sonderfall US-Cloud Act 7
6.1 Hinweis zum Privacy Shield 2.0 und zum Swiss-U.S. Data Privacy Framework 8
7 Wirtschaftliche Überlegungen zur Cloud 9
8 Geopolitische Aspekte 9
Spezifischer Teil - Details für die konkrete Umsetzung 10
9 Die Bedeutung der Cloud für Backup und Recovery 10
10 Cloud only vs. hybride Nutzung 10
11 Anwendungsfälle 11
11.1 Videotelefonie 11
11.2 Kollaboration 12
11.3 Messenger 12
11.4 E-Mail 13
11.5 Klinische und administrative Systeme 13
12 Technische und organisatorische Massnahmen 14
12.1 Bestimmung der Risiken nach Usecase 14
12.2 Verschlüsslung und Schlüsselmanagement 16
Über die Autoren 18

Einführung

Das vorliegende Dokument gibt Gesundheitseinrichtungen eine objektive und unabhängige Basis zum Umgang mit Cloudlösungen. Es wird bewusst nicht auf einzelne Dienstleister oder Produkte eingegangen und auch keine Position zur Cloudnutzung bezogen.

Ziel ist es, Gesundheitseinrichtungen eine Basis zu geben, sich selbständig und eigenverantwortlich mit dem Thema Cloudnutzung auseinandersetzen zu können. Hierzu gibt das Dokument einen Überblick über die wesentlichen Aspekte und Überlegungen, welche dabei berücksichtigt werden müssen. Der erste Teil richtet sich an alle Personen, welche sich mit dem Thema Cloudnutzung auseinandersetzen. Der zweite Teil geht auf konkrete Anwendungsfälle und technische Aspekte ein und richtet sich primär an Fachpersonen.

Management Summary

Gesundheitseinrichtungen haben einen Leistungsauftrag für die Versorgung der Patient:innen. Diese muss wirksam, zweckmässig, wirtschaftlich und konkurrenzfähig sichergestellt werden. Zudem sind Gesundheitseinrichtungen Teil der kritischen Infrastruktur der Schweiz und müssen als solche die Versorgungssicherheit gewährleisten. Hierzu sind resiliente ICT-Systeme zwingende Voraussetzung. Die Nutzung von Clouddiensten spielt hier eine zentrale Rolle und ist schlicht notwendig. In einer zunehmend digitalen und vernetzten Gesellschaft, in der viele Applikationen und Services ausschliesslich online genutzt werden können, ist Cloudnutzung schlicht Realität. Moderne Medizin und resiliente Systeme ohne Cloudnutzung sind nicht mehr möglich.

Hyperscaler (grosse globale Anbieter von Cloudservices) sind hierbei zentrale und nicht substituierbare Player. Nur sie bringen die erforderliche Skalierung, die Innovationskraft, das Fachpersonal und die interoperablen Produkte in der benötigten Anzahl und Grösse. Die Frage ist daher nicht, ob die Services der Hyperscaler genutzt werden sollen oder nicht, sondern welche Services man wie nutzen kann. Dabei gilt es entlang der verschiedenen Anwendungsfälle die rechtlichen Vorgaben zu berücksichtigen und die mit der Nutzung verbundenen Risiken zu identifizieren, zu beurteilen und auf das tragbare Mass zu reduzieren. Jedes Unternehmen bzw. Gesundheitseinrichtungen kann und muss dabei für sich entscheiden, ob einzelne Services weiter lokal oder in Cloudlösungen betrieben werden sollen.

Neben den anwendungs- und unternehmensspezifischen Risiken gibt es zwei zentrale Risiken, welchen man sich sehr klar sein muss: Das Vendor-Lock-in und das Systemversagen. Wenn die ICT-Infrastruktur eines Unternehmens vollständig oder in wesentlichen Teilen auf den Cloudservices eines einzelnen Anbieters basiert und dieser faktisch nicht substituierbar ist, ist ein Anbieterwechsel, wenn überhaupt möglich, mit enormem finanziellem, personellem und zeitlichem Aufwand verbunden. Ein Ausfall eines solchen Anbieters zum Beispiel als Folge eines Cyber-Angriffs oder eines anderen Ereignisses hätte auf alle Unternehmen, welche die Services des Anbieters nutzen, gravierende Folgen.

Wenn zum Beispiel die Services für Videokonferenzen, Telefonie und E-Mail aller Gesundheitseinrichtungen auf der Infrastruktur eines einzigen Anbieters basieren und dieser ausfallen würde, wären sämtliche Gesundheitseinrichtungen der der Schweiz über diese Kanäle nicht mehr erreichbar. Die Nutzung von Clouddiensten erhöht somit nicht nur die Resilienz der ICT-Systeme, sondern kann diese im beschriebenen Fall auch gefährden. Hier sind zwingend Redundanzen und Eventualplanungen zu schaffen.

Auf Clouddienstleistungen zu verzichten ist generell aber auch im medizinischen Bereich weder sinnvoll noch möglich, wenn die Gesundheitseinrichtungen als Teil der kritischen Infrastruktur auch in Zukunft ihren Leistungsauftrag zum Wohl der Patient:innen und zur Gewährleistung der medizinischen Versorgung in der Schweiz erfüllen können sollen. Das vorliegende Dokument ist eine Orientierungshilfe für Gesundheitseinrichtungen in der Auseinandersetzung mit und der risikogerechten Nutzung von Cloudservices.

Allgemeiner Teil – Auslegeordnung und Rahmenbedingungen

1 Einleitung Cloudnutzung

Die Nutzung von Cloud-Services ist unlängst Realität in einer zunehmend digitalen Welt. Die Digitalisierung nimmt mehr und mehr Einzug im Gesundheitswesen, welches ohne digitale Lösungen bereits jetzt oder zumindest in naher Zukunft nicht mehr denkbar ist. Hieraus entsteht neues Potential und neue Möglichkeiten von denen die Gesellschaft als Ganzes und Menschen als Individuen profitieren werden. Ein zentraler Bestandteil der digitalen Welt sind Cloud-Lösungen und die damit verbundenen Chancen und Risiken.

Zwischen Versorgungsauftrag und digitaler Transformation

Eine Gesundheitseinrichtung stellt im Rahmen des jeweiligen Leistungsauftrages und -vereinbarung die Patientenversorgung sicher, die in der zugewiesenen Region wirksam, zweckmässig, wirtschaftlich und konkurrenzfähig sein muss. Dabei steht eine zunehmende Vernetzung mit vor- und nach- gelagerten Versorgen und damit eine möglichst integrierte Versorgung im Vordergrund. Gemäss dem Bundesrat gehören Gesundheitseinrichtungen zu den kritischen Infrastrukturen. Damit der Auftrag in einer Krisensituation erfüllt werden kann, braucht es resiliente ICT-Systeme. Hier sind Clouddienste besonders geeignet. Dazu kommt die allgemeine Marktentwicklung der Anbieter. Viele Applikationen und Services werden gar nicht mehr auf der eingenen lokalen Infrastruktur «on Premise» angeboten.

Die Auseinandersetzung mit dem Thema Cloudnutzung ist daher für Gesundheitseinrichtungen unumgänglich. Das vorliegende Dokument soll Gesundheitseinrichtungen dabei als Orientierungshilfe dienen und eine strukturierte und differenzierte Auseinandersetzung mit dem Thema ermöglichen.

Aufbau des Dokuments

Der erste Teil des vorliegenden Dokuments wendet sich an Entscheidungsträger:innen von Gesundheitseinrichtungen sowie generell an Personen, welche sich für den Umgang mit Cloudlösungen interessieren. Der erste Teil deckt folgende Themen ab:

- Verschiedene Formen von Cloudlösungen
- Die Rolle der Hyperscaler und Mythos Swiss Cloud
- Entwicklung der Cloudlösungen
- Rechtliche Überlegungen zur Cloud
- Sonderfall US-Cloud Act
- Wirtschaftliche Überlegungen zur Cloud

Der zweite Teil des Dokuments richtet sich an Personen, welche sich mit der konkreten Umsetzung von Cloudlösungen befassen. Der zweite Teil deckt folgende Themen ab:

- Die Bedeutung der Cloud für Backup und Recovery
- Cloud only vs. hybride Nutzung
- Anwendungsfälle
- Technische und organisatorische Massnahmen
- Verschlüsslung und Schlüsselmanagement

2 Verschiedene Formen von Cloudlösungen

Cloud-Services oder Cloud-Computing bezieht sich auf die Bereitstellung von IT-Ressourcen, wie Rechenleistung, Speicherplatz, Anwendungssoftware und Datenbanken über das Internet. Im Gegensatz zu traditionellen IT-Modellen, bei denen Unternehmen ihre eigenen Server und Infrastruktur betreiben müssen, können Cloud-Dienste von Drittanbietern genutzt werden, um diese Aufgaben zu übernehmen.

Die Cloud bietet zahlreiche Vorteile, darunter Skalierbarkeit, Flexibilität, Zuverlässigkeit und Kosteneinsparungen. Unternehmen können die Ressourcen, die sie benötigen, schnell und einfach anpassen, ohne

Kapital- oder Personalinvestitionen tätigen zu müssen. Darüber hinaus ermöglicht es Cloud-Computing den Unternehmen, auf eine breitere Palette von Anwendungen zuzugreifen und diese schneller bereitzustellen. Insgesamt bietet Cloud-Computing eine innovative Lösung für Unternehmen, die ihre IT-Infrastruktur modernisieren und effektiver nutzen möchten.

Cloud-Computing ist ein Ansatz für das dynamische und an den Bedarf angepasste Anbieten und Nutzen von IT-Dienstleistungen über ein Netz. Die angebotenen Ressourcen befinden sich dabei in einem Pool und können schnell und mit minimalem Aufwand bzw. geringer Interaktion mit dem Anbieter, abgerufen und verwaltet werden. Leistungsabrechnung erfolgt auf Basis der gemessenen Nutzung.

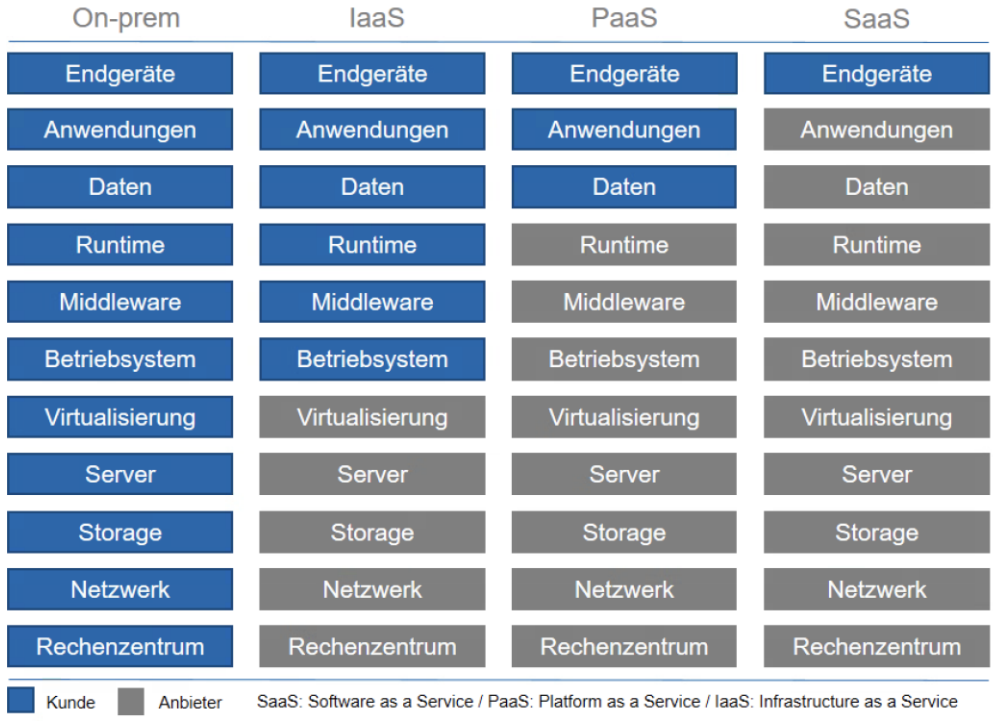
Einordnung der Cloud: IaaS, PaaS und SaaS

Je nach erbrachten Dienstleistungen und wahrgenommen Verantwortungen können Cloud-Dienste in drei Service Modelle unterschieden werden:

- Infrastructure-as-a-Service (IaaS): Bei IaaS werden grundlegende IT-Infrastrukturkomponenten wie Rechenleistung, Speicherplatz und Netzwerkressourcen über das Internet bereitgestellt. Kunden können ihre eigenen Anwendungen und Betriebssysteme auf diesen Infrastrukturkomponenten ausführen.
- Platform-as-a-Service (PaaS): PaaS bietet Entwicklern eine Plattform, um Anwendungen zu erstellen, auszuführen und zu verwalten, ohne sich um die zugrundeliegende Infrastruktur kümmern zu müssen.
- Software-as-a-Service (SaaS): SaaS-Dienste bieten den Nutzern Zugriff auf Softwareanwendungen, die über das Internet bereitgestellt werden. Die Anwendungen werden von Drittanbietern gehostet und gewartet, während die Kunden die Anwendungen über das Internet nutzen.

Diese Varianten zeichnen sich u.a. durch eine unterschiedliche Aufteilung der Verantwortlichkeiten zwischen Cloud-Anbieter und Cloud-Kunden aus.

Übersicht der verschiedenen Typen von Cloudservices im Vergleich mit lokalen Systemen (On-prem):



3 Die Rolle der Hyperscaler und Mythos Swiss Cloud

Hyperscaler sind grosse, global tätige Unternehmen, die Cloud-Computing-Dienste im grossen Massstab anbieten. Einige der bekanntesten Hyperscaler sind Amazon Web Services (AWS), Microsoft Azure,

Google Cloud Platform (GCP), IBM Cloud und Alibaba Cloud. Diese Unternehmen haben riesige Rechenzentren auf der ganzen Welt, um IT-Infrastruktur- und Cloud-Dienstleistungen bereitzustellen.

Hyperscaler als Treiber des Cloud-Computing-Marktes

Die Rolle der Hyperscaler im Cloud-Computing-Markt ist in den letzten Jahren immer wichtiger geworden. Unternehmen, die auf Cloud-Computing-Dienste angewiesen sind, suchen oft nach Lösungen, die schnell, skalierbar und zuverlässig sind. Hyperscaler haben die Fähigkeit, diese Anforderungen zu erfüllen, indem sie riesige Rechenzentren betreiben, die es ihnen ermöglichen, eine enorme Bandbreite an IT-Infrastruktur- und Cloud-Dienstleistungen bereitzustellen.

Durch die Nutzung der Cloud-Dienste von Hyperscalern können Unternehmen auch Kosteneinsparungen erzielen, da sie keine hohen Investitionen in eigene IT-Infrastruktur tätigen müssen. Die Hyperscaler bieten auch eine breite Palette von Dienstleistungen an, darunter Infrastruktur-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS), die Unternehmen je nach Bedarf nutzen können.

Darüber hinaus haben Hyperscaler ein hohes Mass an Expertise und Technologie, um Kunden bei der Entwicklung, Implementierung und Verwaltung von Cloud-Computing-Diensten zu unterstützen. Dies macht sie zu einer wichtigen Option für Unternehmen, die in der heutigen Geschäftswelt wettbewerbsfähig bleiben wollen.

Insgesamt sind die Hyperscaler in der heutigen Welt des Cloud-Computing unverzichtbar geworden. Ohne die Hyperscaler würde es für Unternehmen schwieriger sein, schnell und flexibel auf die Anforderungen des heutigen Geschäftsumfelds zu reagieren.

Einordnung von „Swissness“ im Cloud-Kontext

Die Begriffe "Swiss Cloud" und "Swissness" beziehen sich auf Cloud-Dienste, die von Schweizer Unternehmen angeboten werden und die in der Schweiz gehostet werden. Es herrscht die Meinung, dass diese Cloud-Dienste höhere Standards in Bezug auf Datenschutz, Sicherheit und Vertraulichkeit bieten als Cloud-Dienste von anderen Anbietern.

Es ist wichtig zu beachten, dass "Swissness" kein offiziell anerkanntes Zertifikat oder Label ist. Es gibt jedoch tatsächlich einige Gründe, warum Schweizer Cloud-Dienste als besonders sicher und vertrauenswürdig angesehen werden. Die Schweiz hat strenge Datenschutzgesetze und hohe Standards in Bezug auf Privatsphäre und Datensicherheit. Die Schweiz ist auch politisch stabil, hat ein hohes Mass an Rechtssicherheit und ist neutral, was ein zusätzliches Mass an Sicherheit und Vertrauen schafft.

Darüber hinaus haben Schweizer Unternehmen oft eine hohe Reputation für Qualität und Zuverlässigkeit, was dazu beitragen kann, das Vertrauen in ihre Cloud-Dienste zu stärken.

Allerdings bedeutet dies nicht zwangsläufig, dass alle Schweizer Cloud-Dienste automatisch sicherer oder vertrauenswürdiger sind als Cloud-Dienste von anderen Anbietern. Es ist wichtig, die individuellen Eigenschaften und Merkmale von Cloud-Diensten sorgfältig zu prüfen und abzuwägen, um die bestmögliche Lösung für die spezifischen Anforderungen eines Unternehmens oder einer Organisation zu finden.

4 Weitere Entwicklung der Cloudlösungen

Es gibt viele Prognosen und Vorhersagen darüber, wohin die Reise für Cloud-Dienste gehen wird. Einige der wichtigsten Trends und Entwicklungen sind:

Multi-Cloud-Strategien: Unternehmen setzen zunehmend auf eine Kombination von Cloud-Diensten verschiedener Anbieter, um die Flexibilität und Zuverlässigkeit ihrer IT-Infrastruktur zu erhöhen.

Edge Computing: Die Verarbeitung von Daten und Anwendungen erfolgt nicht mehr ausschliesslich in zentralen Rechenzentren, sondern auch an der Edge, also in der Nähe des Endnutzers bzw. in der Nähe der Datenquelle. Dies soll eine schnellere Reaktionszeit und eine bessere Leistung ermöglichen.

Künstliche Intelligenz und maschinelles Lernen: Cloud-Dienste bieten eine ideale Plattform für die Verarbeitung grosser Datenmengen und die Ausführung von Machine-Learning-Algorithmen. Dies ermöglicht es Unternehmen, wertvolle Erkenntnisse aus Daten zu gewinnen und innovative Anwendungen zu entwickeln.

Container-Technologien: IT Container verpacken und transportieren standardisiert Software und ermöglichen es Unternehmen, Anwendungen effektiver und flexibler zu verwalten und zu skalieren; ähnlich wie Schiffscontainer Waren standardisiert transportieren. Dies wird dazu beitragen, die Cloud noch einfacher und zugänglicher zu machen.

Cloud only hybrid-Cloud: Unternehmen setzen zunehmend auf hybride Cloud-Modelle, bei denen eine Kombination aus öffentlichen und privaten Cloud-Diensten genutzt wird. Dies ermöglicht es Unternehmen, die Vorteile der Cloud zu nutzen, ohne ihre gesamte IT-Infrastruktur vollständig in die Cloud zu verlagern.

Hybrid-Cloud-Onprem: Ein Teil der Anwendungen und Infrastruktur ist in der Cloud. Ein anderer Teil der Anwendungen und Infrastruktur wird weiter lokal betrieben. Eine mögliche Variante ist z.B. die Anwendungen für Kommunikation und Kollaboration in der Cloud zu betreiben und für das Kerngeschäft des Unternehmens relevante Anwendungen mit strukturieren vertraulichen Daten weiter lokal auf der eigenen Infrastruktur (onprem) zu betreiben. Von Fall zu Fall wird im Rahmen einer Abwägung von Chancen, Risiken, Kosten und rechtlichen Vorgaben entschieden, ob eine Anwendung in der Cloud betrieben werden soll oder lokal.

Insgesamt wird die Zukunft von Cloud-Diensten von Innovationen und neuen Technologien geprägt sein, die es Unternehmen ermöglichen, ihre IT-Infrastruktur effektiver und effizienter zu nutzen. Unternehmen, die Cloud-Dienste nutzen, werden in der Lage sein, schneller und flexibler auf die sich ändernden Anforderungen des heutigen Geschäftsumfelds zu reagieren und dadurch wettbewerbsfähiger zu bleiben.

5 Rechtliche Überlegungen zur Cloud

Cloud Computing stellt immer die Auslagerung und damit eine Bearbeitung von Daten durch Dritte dar. Sie wird vertraglich beauftragt, Daten für die auslagernde Einrichtung des Gesundheitswesens zu bearbeiten. Hierbei erfolgt keine Veröffentlichung der Daten. Diese Unterscheidung ist wichtig, da an eine solche Auftragsdatenbearbeitung andere Anforderungen als an die Veröffentlichung gestellt werden. Die Verantwortung für die Daten bleibt allerdings stets bei der auslagernden Einrichtung des Gesundheitswesens.

Einordnung von Datenkategorien und Schutzbedarf

Für eine rechtskonforme Cloudnutzung stellt sich als erstes die Frage nach den Daten, welche in der Cloud bearbeitet werden sollen. Um was für Daten handelt es sich? Wie schutzwürdig sind die Daten? Abhängig davon, welche Daten in der Cloud bearbeitet werden sollen, bestehen andere rechtliche wie informationssicherheitstechnische Anforderungen. Dabei ist es hilfreich, zwischen folgenden Kategorien zu unterscheiden:

- Öffentliche Daten
- Geschäftsinterne Daten
- Vertrauliche Geschäftsdaten
- Personendaten (diese können öffentlich, intern oder vertraulich sein)
- Besondere Personendaten wie z.B. Patientendaten

Sofern es sich dabei um Daten handelt, welche dem Berufs- oder Amtsgeheimnis unterstehen, wie dies z.B. bei Patientendaten der Fall ist, muss neben dem Datenschutz auch das Berufsgeheimnis beachtet werden.

Einordnung von Datenzustand und Datenstandort

Sobald geklärt ist, welche Art von Daten in der Cloud bearbeitet werden sollen, stellt sich die Frage, in welchem Zustand diese Daten sind. Sind diese identifizierbar oder wurden sie pseudonymisiert oder gar anonymisiert und gelten diese abhängig davon weiter als Personendaten oder nicht?

Als pseudonymisiert bzw. ausreichend pseudonymisiert gelten personenbezogene Daten dann, wenn diese nur noch mit unverhältnismässigem Aufwand durch Dritte einer bestimmten Person zugeordnet

werden können. Anhand eines Identifikationsschlüssels ist der Rückschluss auf eine Person weiter möglich. Sofern sich der Identifikationsschlüssel ausschliesslich im Besitz des Auftraggebers befindet, können ausreichend pseudonymisierte Daten aus Sicht des Auftragsempfängers als anonymisiert betrachtet werden.

Im Unterschied zur Pseudonymisierung ist eine Anonymisierung irreversibel. Der Rückschluss auf eine Person ist nicht mehr möglich. Wurden personenbezogene Daten vollständig anonymisiert, gelten sie nicht mehr als Personendaten.

Als letztes stellt sich die Frage nach dem Speicher- bzw. Bearbeitungsort der Daten. Werden diese in der Schweiz gespeichert und bearbeitet oder erfolgt dies ausserhalb der Schweiz?

Sofern Ersteres der Fall ist, greift das Schweizer Recht inklusive Berufs- und Amtsgeheimnis, womit gemäss gängiger Praxis der Auftragsempfänger zumindest vertraglich an ein entsprechendes Schutzniveau gebunden werden und Ahndungen von Verletzungen durchgesetzt werden können. Gemäss einer strengeren Rechtsauffassung, die auch von gewissen Aufsichtsbehörden vertreten wird, steht das Berufsgeheimnis einer Auslagerung in die Cloud grundsätzlich entgegen. Mit einer solchen rigiden rechtlichen Auslegung ist die Nutzung von Cloudlösungen durch Gesundheitseinrichtungen bzw. die Auftragsdatenverarbeitung im Zusammenhang mit Patientendaten faktisch nicht mehr möglich. In einer stetig zunehmend digitalen Gesellschaft, stellt sich die Frage, ob Spitäler und andere Gesundheitseinrichtungen ohne Cloudnutzung überhaupt noch ihren Auftrag wahrnehmen und damit als Teil der kritischen Infrastruktur der Schweiz die medizinische Versorgung der Bevölkerung angemessen sicherstellen können.

Werden die Daten ausserhalb der Schweiz gespeichert und bearbeitet ist nicht Schweizer Recht, sondern das dortige Recht anwendbar. Eine Übertragung und Durchsetzung sind nur bedingt möglich.

Einordnung von rechtlichen und sicherheitstechnischen Anforderungen

Sofern besondere Personendaten bzw. z.B. Patientendaten in der Cloud bearbeitet werden sollen, braucht es aus datenschutzrechtlicher Sicht zwingend eine vertragliche Grundlage für die Bearbeitung im Auftrag. Dabei müssen die Zweckbindung sowie die Verhältnismässigkeit gewährleistet sein. Dies bedeutet, dass die Daten durch den Auftragsempfänger nur zu dem Zweck bearbeitet werden dürfen, zu dem diese dem Auftraggeber anvertraut wurden. Weiter dürfen dabei nur die Daten verwendet werden, welche für den Zweck der Verarbeitung zwingend nötig sind.

Bei jeder neuen oder wesentlich veränderten Bearbeitung von besonderen Personendaten muss eine Datenschutz-Folgeabschätzung durchgeführt werden. Je nach anwendbarer Rechtsgrundlage (Bundesrecht, kantonales Datenschutzrecht) kann eine Vorabkontrolle bzw. Vorabkonsultation bei der Aufsichtsbehörde erforderlich sein.

Findet die Speicherung und Bearbeitung ausserhalb der Schweiz statt, ist dies überdies nur zulässig, wenn das Datenschutzniveau im Empfängerstaat mindestens jenem der Schweiz entspricht. Obwohl Auftragsempfänger ausserhalb der Schweiz vertraglich an ein gleiches Schutzniveau gebunden werden können, sind die entsprechenden Durchsetzungsmöglichkeiten nicht gleich gut. Zudem findet das dortige (Datenschutz-) Recht Anwendung. Es braucht daher aufgrund des höheren Risikos zwingend Transparenz über die Bearbeitung besonderer Personendaten ausserhalb der Schweiz und eine nachweisbare, explizite Einwilligung der Personen dafür. Selbstverständlich gelten auch dann die genannten rechtlichen Voraussetzungen sowie die Sorgfaltspflicht.

Die bearbeiteten Daten müssen schliesslich stets gemäss dem aktuellen Stand der Informationssicherheit geschützt sein. Dies bedeutet, dass die Daten bei der Übertragung und der Speicherung vor Ort zum Beispiel durch Verschlüsslung und rollenbasierte Zugriffe angemessen geschützt sein müssen.

6 Sonderfall US-Cloud Act

Die Nutzung von Cloudcomputing im Rahmen einer Auftragsdatenverarbeitung mit besonderen Personendaten bzw. Patientendaten ist mit entsprechender vertraglicher Grundlage und mit den nötigen infor-

mationssicherheitstechnischen Vorkehrungen gemäss gängiger Rechtspraxis möglich. Dies gilt insbesondere, wenn sich die Cloudinfrastruktur in der Schweiz befindet. Ein Sonderfall stellt allerdings die exterritoriale Anwendung des US-Cloud Acts dar.

Gemäss diesem dürfen die US-amerikanischen Behörden, bei einem laufenden Strafverfahren gegen eine Person, Zugriff auf die Daten dieser Person bei Unternehmen mit US-Bezug verlangen. Wenn ein Unternehmen bzw. eine Gesundheitseinrichtung Daten in einer Cloud bearbeitet und es sich beim Cloudanbieter um ein Unternehmen mit US-Bezug handelt, können sich die US-Behörden potentiell Zugriff auf die Daten verschaffen, auch wenn die genutzte Cloudinfrastruktur in der Schweiz steht.

Die Bearbeitung von Patientendaten bei einem Cloud-Anbieter mit US-Bezug ist daher aus datenschutzrechtlichen Gründen problematisch und muss im Detail individuell geprüft werden. Generell und insbesondere bei Cloudanbietern mit US-Bezug ist es daher wichtig, zuerst die konkreten Anwendungen zu definieren und zu spezifizieren. Entlang der Anwendungsfälle müssen die Risiken, Chancen und Kosten abgewogen sowie die rechtlichen Anforderungen geprüft werden.

Neben dem Aspekt der Vertraulichkeit sind auch die Integrität und die Verfügbarkeit der Daten zu berücksichtigen. Letzteres ist entscheidend, um den Betrieb einer Gesundheitseinrichtung sicherstellen zu können und somit entscheidend für die Versorgungssicherheit einer kritischen Infrastruktur. Basierend auf den Erkenntnissen dieser Analyse müssen Massnahmen definiert und zeitnah umgesetzt werden, durch welche die Risiken ausgeschlossen oder auf ein tragbares Mass reduziert werden.

6.1 Hinweis zum Privacy Shield 2.0 und zum Swiss-U.S. Data Privacy Framework

Die Europäischen Kommission hat am 10. Juli 2023 den Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework angenommen, das teilweise auch als «Privacy Shield 2.0» bezeichnet wird. Der Beschluss legt fest, dass die USA für Personendaten, die aus der EU an US-Unternehmen übermittelt werden, welche nach dem EU-U.S. Data Privacy Framework zertifiziert und in der entsprechenden Liste des U.S. Department of Commerce aufgeführt sind, ein angemessenes Schutzniveau gewährleisten. An solche Unternehmen können Personendaten grundsätzlich ohne zusätzliche Datenschutzgarantien übermittelt werden.

Für Datenübermittlungen aus der Schweiz besteht seit dem 15. September 2024 mit dem Swiss-U.S. Data Privacy Framework eine entsprechende schweizerische Regelung. Der Bundesrat hat die USA für Personendaten, die an nach diesem Rahmen zertifizierte US-Unternehmen übermittelt werden, in die Liste der Staaten beziehungsweise spezifischen Sektoren mit einem angemessenen Datenschutz aufgenommen. Solche Datenübermittlungen können gestützt auf Artikel 16 Absatz 1 DSG grundsätzlich ohne zusätzliche Garantien erfolgen. Bei Übermittlungen an nicht zertifizierte US-Unternehmen sind dagegen weiterhin geeignete Garantien nach Artikel 16 Absatz 2 DSG erforderlich.

Die rechtliche und institutionelle Stabilität dieser Datenschutzrahmen ist jedoch aufgrund des Entscheids des U.S. Supreme Court vom 29. Juni 2026 in der Sache Trump v. Slaughter neu zu beurteilen. Der Supreme Court erklärte die gesetzliche Regelung, wonach Mitglieder der Federal Trade Commission nur aus bestimmten wichtigen Gründen – namentlich wegen Pflichtvernachlässigung, Unfähigkeit oder Amtsmissbrauch – abberufen werden konnten, als mit der verfassungsrechtlichen Gewaltenteilung unvereinbar. FTC Commissioners können damit grundsätzlich vom Präsidenten ohne Nachweis eines solchen Abberufungsgrundes entlassen werden.

Dieser Entscheid ist für das Swiss-U.S. Data Privacy Framework von Bedeutung, weil die FTC bei den meisten teilnehmenden US-Unternehmen für die Durchsetzung der Datenschutzgrundsätze zuständig ist. Die schweizerische Angemessenheitsprüfung von 2024 ging ausdrücklich davon aus, dass FTC Commissioners während ihrer siebenjährigen Amtszeit nur aus wichtigem Grund abberufen werden können, und qualifizierte die FTC gestützt darauf zusammen mit dem U.S. Department of Transportation als unabhängige Aufsichtsbehörde. Der Wegfall dieses Abberufungsschutzes stellt daher eine wesentliche nachträgliche Veränderung einer Grundlage dar, auf welche sich die schweizerische Angemessenheitsbeurteilung stützte. Er kann Zweifel an der institutionellen Unabhängigkeit und an der politischen Unbeeinflussbarkeit der Durchsetzung des Swiss-U.S. Data Privacy Framework begründen.

Der Supreme-Court-Entscheid hebt das Swiss-U.S. Data Privacy Framework allerdings nicht unmittelbar auf. Die schweizerische Angemessenheitsanerkennung bleibt formell anwendbar, solange der Bundesrat die entsprechende Regelung in der Datenschutzverordnung nicht ändert oder eine zuständige Behörde beziehungsweise ein Gericht zu einem anderen Ergebnis gelangt. Angesichts der veränderten institutionellen Voraussetzungen ist jedoch mit einer erneuten Prüfung des Frameworks zu rechnen. Unternehmen, die sich für Datenübermittlungen ausschliesslich auf das Swiss-U.S. Data Privacy Framework stützen, sollten die weitere Entwicklung beobachten und insbesondere bei besonders schützenswerten oder umfangreichen Personendaten ergänzende beziehungsweise alternative Garantien vorbereiten.

Ob die Einführung des EU-U.S. beziehungsweise des Swiss-U.S. Data Privacy Frameworks den Sonderfall des U.S. CLOUD Act beeinflusst, ist weiterhin umstritten. Die beiden Datenschutzrahmen beseitigen die gesetzlichen Befugnisse von US-Behörden, unter den Voraussetzungen des CLOUD Act die Herausgabe von Daten durch US-Anbieter zu verlangen nicht.

Aus aktueller Sicht wird daher im Rahmen dieses Dokuments davon ausgegangen, dass der Sonderfall des U.S. CLOUD Act weiterhin gesondert berücksichtigt werden muss. Der Supreme-Court-Entscheid verstärkt vielmehr die Notwendigkeit, neben der formellen Zertifizierung eines US-Empfängers auch die tatsächlichen Zugriffs-, Aufsichts- und Rechtsschutzrisiken regelmässig zu beurteilen.

7 Wirtschaftliche Überlegungen zur Cloud

Mit den Cloud-Angeboten und dem Wandel von On-Premises zu Mietlizenzen hat auch eine neue finanztechnische Betrachtung des Softwareeinsatzes in Betrieben stattgefunden. Wo früher Hard- und Software selber beschafft wurden, wird heute die Software «as a Service» eingekauft auf Mietbasis. Somit werden keine Investitionen mehr getätigt, sondern diese Leistungen werden über die laufende Rechnung direkt in den Betriebsaufwand übernommen (von CapEx zu OpEx). Dadurch findet eine Verringerung des Finanzrisikos statt, weil hierfür keine Investitionen geplant und getätigt werden müssen, mit Aktivierung und in der Regel vierjähriger Abschreibung und der unflexiblen Kapitalbindung.

Dadurch kann bei diesem Modell (OpEx) von einer wesentlich grösseren Flexibilität geredet werden. Lösungen lassen sich schneller auf den wirklichen Bedarf anpassen und auch auf der Seite von Unterhaltsfinanzierungen findet eine Entspannung statt. Auch kann, je nach Wahl des Mietmodells, davon ausgegangen werden, dass technische Anpassungen unmittelbar, aber sicher viel schneller umgesetzt werden wie beim Kaufmodell (CapEx). Zudem ist der Einstieg in neue Technologien wesentlich rascher zu vollziehen.

Als grosser wirtschaftlicher Nutzen ist in der durch Cloud Computing gewonnenen Flexibilität zu sehen. Cloudcomputing ermöglicht es Unternehmen die IT-Umgebung rasch den sich verändernden Anforderungen und Bedürfnissen anzupassen. Angesichts der zunehmenden und immer schnelleren Digitalisierung der Gesellschaft wird diese Fähigkeit je länger je wichtiger. Dies gilt insbesondere für das Gesundheitswesen, welches sich ebenfalls zunehmend und immer schneller digitalisiert.

Grundsätzlich zu sagen, eine cloudbasierte Lösung wäre immer günstiger als eine lokale On-prem Lösung wäre falsch. Die finanziellen Auswirkungen müssen abhängig von den konkreten Anwendungsfällen und den damit verbundenen Aufwänden für die Gewährleistung der rechtskonformen und sicheren Nutzung jeweils erhoben und verglichen werde. Dabei ist auch daran zu denke, dass ein Cloudanbieter die Preise über die Zeit anpassen bzw. diese steigen können und gelichzeitig ein Ausstieg ebenfalls mit hohen Kosten verbunden ist.

8 Geopolitische Aspekte

In Anbetracht der geopolitischen Veränderungen der jüngsten Vergangenheit muss neben den oben genannten Punkten die geopolitische Lage und das erratische Verhalten einzelner Akteure berücksichtigt werden.

Aufgrund dieser Entwicklungen bzw. der neuen Realität, der wir uns gegenübersehen, kann nicht gänzlich ausgeschlossen werden, dass beispielsweise willkürliche Zollerhöhungen oder regulatorische Einschränkungen Auswirkungen auf die Betreiber oder Nutzer von Cloud-Dienstleistungen haben, Verbindungen oder Services eingeschränkt oder unterbrochen werden, um Druck auszuüben, oder ein Rechenzentrum eines Anbieters durch Krieg physisch zerstört wird; wie Anfang März 2026 im Rahmen eines Raketenangriffs auf ein Rechenzentrum von AWS in den Vereinigten Arabischen Emiraten geschehen.

Verstärkt werden diese Risiken, durch die hohe Abhängigkeit von wenigen globalen Anbietern. Insgesamt entsteht so ein komplexes Risikoprofil, das nicht nur technische, sondern auch strategische und sicherheitspolitische Dimensionen umfasst und die Versorgungssicherheit im Gesundheitswesen direkt beeinflussen kann. Dies gilt es bei den Überlegungen und Entscheidungen in Abwägung der Risiken, Chancen und Alternativen zu berücksichtigen und angemessene Massnahmen zu treffen.

Spezifischer Teil - Details für die konkrete Umsetzung

9 Die Bedeutung der Cloud für Backup und Recovery

Business Impact Analysen mit seitens Kliniken geforderten kurzen RTO (Recovery Time Objective, Wiederanlaufzeit) und RPO (Recovery Point Objective, zeitlich maximal tolerierbarer Datenverlust) zeigen die Wichtigkeit einer hohen Verfügbarkeit der ICT in Gesundheitseinrichtungen. Ausfallereignisse zeigen, dass eine Gesundheitseinrichtung im schlimmsten Fall vorübergehend ohne wesentliche IT-Unterstützung funktionieren kann; allerdings mit dem Preis einer stark reduzieren Produktivität und eines grossen Aufwands zur Aufrechterhaltung und Nachtragen der relevanten Informationsflüsse. In einem mehrstufigen Business Continuity Management bieten Cloudlösungen gute und skalierbare Ansätze, um die Kontinuität besser zu Gewährleisten oder wiederherzustellen.

Ein weiterer Vorteil von Cloudlösungen ist, dass Expertenwissen, Service und Support in der Regel durch den Anbieter zur Verfügung gestellt werden und auch die Aktualisierung der Systeme und Software durch den Betreiber sichergestellt wird. In der Regel werden daher Systeme zeitnah gepatcht und Sicherheitslücken geschlossen. Die Serviceansprüche müssen vertraglich geregelt werden und abhängig vom Cloud-Service Typ ist auch der Kunde mehr oder weniger in der Verantwortung.

Eine zusätzliche Herausforderung stellt die Integration von Daten von Medizintechnischen Systemen dar. Die verschiedensten Anbieter von (Mess-)Geräten wie z.B. Herzschrittmacher oder Blutzuckern-Messgeräte sammeln diese Daten in proprietären Cloudlösungen. Zur optimalen Behandlung sollten diese Daten in den Systemen des interprofessionellen Behandlungsteams aggregiert zur Verfügung gestellt werden können.

Hinweis: Bei der Nutzung von medizintechnischen Produkten müssen die Vorgaben der FMH berücksichtigt werden.

10 Cloud only vs. hybride Nutzung

Die Reise von der aktuell vorherrschenden «on Premise» in die Cloud ist von grösserer Dauer und abhängig von verschiedenen Faktoren:

- Verfügbare Angebote resp. Abkündigung von lokalen Applikationen resp. Services
- Reduktion von nicht-Cloud fähigen Legacy Systemen
- Rechtliche Bestimmungen und Datenschutzvorgaben
- Koexistenz von private und public Clouddiensten
- Neue Services, welche ausschliesslich in Verbindung mit der Cloud existieren; z.B: Telemedizin, remote Monitoring von Patient:innen, Einsatz von Wearables.

Einordnung der Rolle der ICT: Fokus auf Business-Mehrwert statt Technologie

Die Kernkompetenz (Unique Selling Proposition, USP) einer ICT-Abteilung einer Gesundheitseinrichtung liegt in der Transformationsschicht zwischen der Technologie und dem Hauptprozess der Diagnose und

Behandlung der Patient:innen. Ohne das Verständnis beider Domänen ist eine proaktive Beratung und Bereuung im Sinne der Wertgenerierung nicht zielführend. Basistechnologien und Infrastrukturen sind Commodity, die Herausforderung der internen ICT-Abteilung besteht in der Orchestrierung der Element und Provider sowie in der optimalen Gestaltung der Komplexität.

Herausforderungen der ICT: Fachkräftemangel und digitale Transformation

Die digitale Transformation ist im Gesundheitswesen ca. 10 Jahre im Rückstand gegenüber anderen Brachen (Banken, Versicherungen, Telekommunikation). Dies gilt auch innerhalb der Gesundheitsbranche in ähnlichem Ausmass, wenn man ins nahe und ferne Ausland blickt (Estland, Singapur, USA).

Dementsprechend gibt es noch sehr viele, lokale meist Client/Server Applikationen bei denen zudem keine saubere Trennung der verschiedenen Schichten (Daten, Businesslogik und Präsentation) besteht. Bei den Anbietern handelt es sich meist um kleine KMUs bei denen in der Langzeitbetrachtung häufig die «Ability to execute» fehlt hinsichtlich operationeller Unterstützung und Weiterentwicklung.

Der Fachkräftemangel im ICT ist in zwei Bereichen besonders evident. Einerseits ist eine ICT-Ausbildung für Berufseinsteige im Gesundheitswesen nicht attraktiv, andererseits sind Gesundheitseinrichtungen bei den Spezialisten (z.B. M365 Engineers, Enterprise Security Architekten etc.) lohnmässig absolut nicht konkurrenzfähig. Zudem haben Gesundheitseinrichtungen unabhängig von deren Cloudnutzung durch die Nutzung einer grossen Anzahl von medizintechnischen Geräten, welche mit dem Netzwerkverbunden sind, eine Nische, welche mit spezifisch ausgebildetem IT-Fachpersonal abgedeckt werden muss.

11 Anwendungsfälle

11.1 Videotelefonie

Die Videotelefonie übermittelt Ton- und Bilddaten in Echtzeit. In aller Regel erfolgt dabei lediglich eine Übermittlung, jedoch keine Speicherung von Daten. Eine Ausnahme liegt diesbezüglich vor, wenn zum Zwecke der Nachvollziehbarkeit oder Qualitätssicherung eine Aufzeichnung erfolgt.

Zentrale Prüffragen sind:

- Kann die Videotelefonie technisch auf die reine Übermittlung von Ton- und Bilddaten limitiert werden?
- Ist bekannt, welche Randdaten zum Zwecke der Signalisierung vom Diensteanbieter gespeichert werden, und dass diese Speicherung und nachfolgende Bearbeitung im Einklang mit den rechtlichen Vorgaben erfolgt? Setzt der Diensteanbieter das Grundprinzip der Datensparsamkeit um, welches besagt, dass nur jene Daten erhoben und bearbeitet werden, welche zum Zwecke zwingend erforderlich sind?
- Hat die Videotelefonie resp. die in diesem Kontext übermittelten Ton- und Bilddaten einen Personenbezug? Hierbei sind nicht rein die Nutzerdaten von Relevanz, welche übermittelt werden, sondern auch die Bilddaten der Teilnehmenden, welche allenfalls einen Schutzbedarf hinsichtlich der Privatsphäre haben könnten.
- Als Empfehlung gilt hierbei die Einblendung eines künstlich generierten Hintergrundbildes, wie es bei den gängigen Anwendungen in der Regel möglich ist. Allerdings steht diese Funktionalität oftmals nur bei einer installierten Anwendung zur Verfügung, nicht jedoch bei der Teilnahme über einen Internetbrowser. In diesem Falle empfiehlt sich die Information des Gesprächsleiters, dass das Ausschalten der Videokamera zum Schutze der Privatsphäre erlaubt sei. Diese Information sollte vorteilsweise schon mit der Einladung oder spätestens dann einleitend im Videogespräch übermittelt werden.
- Können im Minimum die Nutzerdaten verschlüsselt werden? Erfolgt diese Verschlüsselung end-to-end, oder nur während der Übermittlung (data-in-transit) resp. während der Speicherung (data-in-rest)?

Im Falle einer Aufzeichnung werden sowohl Ton- als auch Bilddaten aufgezeichnet und damit gespeichert. Es stellen sich damit zusätzlich folgende Fragen:

- Zu welchem Zweck erfolgt die Aufzeichnung? Wie lange werden die Daten gespeichert? Kann die Dauer der Speicherung angepasst bzw. verkürzt werden? Ist sichergestellt, dass sie keinem anderen Zweck zugeführt werden und nach Zweckerfüllung innert nützlicher Frist gelöscht werden?

- Liegt eine rechtliche Grundlage, ein berechtigtes Interesse oder die Einwilligung der Teilnehmenden zu dieser Datenbearbeitung vor? Gilt dies ebenso für die Nutzerdaten, welche während des Videogesprächs übermittelt werden?

Risiken und Abhängigkeiten cloudbasierter Kommunikation

Ein breiter oder gar flächendeckender Einsatz von cloudbasierten Kommunikationsdiensten in der Gesundheitseinrichtung schafft im Sinne der Verfügbarkeit eine hohe Abhängigkeit zum Dienst. Eine grössere Störung beim Anbieter oder aber auch eine Beeinträchtigung des Dienstzugangs (Stichwort Konnektivität) hat einen sehr hohen Einfluss auf den Betrieb der Gesundheitseinrichtung. Dieser ist namentlich bei internen und externen notfallrelevanten Kommunikationen besonders hoch. Es empfiehlt sich deshalb, für diese und anderweitig für den ordentlichen Unternehmensbetrieb unabdingbaren Kommunikationen Rückfallebenen im Sinne von Redundanzen zu schaffen und diese regelmässig mit realitätsnahen Szenarien zu prüfen.

Die zunehmende Integration von Algorithmen zur Erkennung von unzulässigen Inhalten durch den Diensteanbieter (vgl. künstliche Intelligenz) birgt das Risiko, dass übermittelte medizinische Bilddaten als pornographisch eingestuft und blockiert werden. Solche Funktionen können einen hohen Einfluss auf spezifische Anwendungsfälle wie zum Beispiel die Telemedizin haben. Entsprechende Funktionen werden vom Diensteanbieter oftmals nicht oder nur kurzfristig angekündigt, was es der Gesundheitseinrichtung erschwert, darauf reagieren zu können. Die Möglichkeit der Steuerung und Übersteuerung solcher Algorithmen ist deshalb frühzeitig mit dem Anbieter zu klären.

Summarisch bietet der Einsatz von Videotelefonie in der Gesundheitseinrichtung überwiegende Vorteile, welche bei zahlreichen Anwendungsfällen wesentliche Mehrwerte schaffen können. Es ist jedoch zwingend, sich nicht von diesen nicht einvernehmen zu lassen und einen breiten oder gar flächendeckenden Einsatz im Gesundheitswesen seriös zu erwägen. Bewährt haben sich skalierte und hybride Betriebsmodelle, bei welchen die notfallrelevanten Kommunikationen über traditionelle lokale Dienste geführt werden.

11.2 Kollaboration

Die Kollaboration umfasst im allgemeinen Verständnis die Interaktion mittels Videotelefonie sowie ergänzend die gemeinsame gleichzeitige Bearbeitung von zentral gespeicherten Daten von internen und externen Teilnehmenden. Im Wesentlichen erweitert sich der u. beschriebene Anwendungsfall der Videotelefonie um die Speicherung und Bearbeitung von Daten, typischerweise auf der Cloud-Umgebung eines Diensteanbieters.

Zentrale Prüffragen sind:

- Kann gewährleistet werden, dass die zentral gespeicherten Daten ausreichend gegenüber missbräuchlichem Zugriff (Schutzziel Vertraulichkeit) und der missbräuchlichen Veränderung (Schutzziel Integrität) geschützt sind?
- Können die Daten im Falle eines Verlustes auf der Cloud-Umgebung des Diensteanbieters wiederhergestellt werden? (Schutzziel Verfügbarkeit)
- Können Zugriffe und Änderungen an den Daten nachvollzogen werden?
- Obliegt die Vergabe von Zugriffsrechten alleinig dem Eigentümer des gemeinsamen Arbeitsbereiches resp. explizit durch ihn autorisierte Personen (delegated administration)? Oder ist es jedem Teilnehmenden möglich, einen Datensatz mit Dritten zu teilen?

11.3 Messenger

Unter Instant Messaging (Chat) wird allgemeinhin die Übermittlung einer Kurznachricht an eine Einzelperson oder eine Gruppe verstanden. Der übermittelte Inhalt kann dabei nebst reinem Text auch Bilddaten enthalten kann oder auch ein Dokument im Anhang. Dabei erfolgt eine Speicherung, damit der Inhalt auch zu einem späteren Zeitpunkt noch einsehbar ist. Die Übermittlung erfolgt in der Regel innerhalb eines geschützten Adressraums, womit entsprechende Kurznachrichten nur an Teilnehmende gerichtet werden können, welche Mitglied des Adressraums sind.

Zentrale Prüffragen sind:

- Ist für den Absender einer Kurznachricht in jedem Fall erkennbar, wer Zugriff auf die Inhalte hat?
- Kann sichergestellt werden, dass die übermittelten Daten vom Diensteanbieter nicht für weitere Zwecke verwendet werden? (vgl. Whatsapp)
- Ist bekannt, welcher Randdaten in Zusammenhang mit der Übermittlung erhoben und gespeichert werden, sowie zu welchem Zwecke sie von wem verarbeitet werden? Setzt der Diensteanbieter das Prinzip der Datensparsamkeit um?

11.4 E-Mail

Unter E-Mail versteht man die Übermittlung von Text und Daten über eine separate Anwendung, oftmals einen speziellen E-Mail Client. Dabei wird diese Anwendung oftmals nicht zum reinen Zwecke der Informationsübermittlung verwendet, sondern teilweise auch von den Nutzern zur Speicherung dieser Informationen in einer Ordnerstruktur innerhalb des E-Mail Clients.

Zentrale Prüffragen sind:

- Ist die Verschlüsselung der Daten während der Übermittlung lückenlos sichergestellt?
- Kann eine Signierung eingesetzt werden, um die Authentizität des Absenders mittels kryptographischer Verfahren prüfen zu können?
- Besteht eine separate Möglichkeit zur verschlüsselten Übermittlung von E-Mails, welche sich nicht nur auf die reine Transportverschlüsselung beschränkt?

11.5 Klinische und administrative Systeme

Im Kontext von klinischen und administrativen Systemen sind solche zu verstehen, welche dem Zwecke der Bearbeitung von Patientendaten und damit besonders schützenswerte Personendaten dienen oder von Daten von Mitarbeitenden, unter welchen sich ebenfalls besondere Personendaten bzw. besonders schützenswerte Daten befinden können. Dazu zählen daher grundsätzlich sämtliche Informations- und Fachsysteme sowie zugehörige Umsysteme und Hilfsdienste, welche dabei genutzt werden.

Zentrale Prüffragen sind:

- Kann lückenlos nachvollzogen werden, in welchem Land (Rechtsraum) und vorteilsweise sogar in welchem Rechenzentrum-Standort des Diensteanbieters die Daten gespeichert werden?
- Kann ausgeschlossen werden, dass in Zusammenhang mit der Nutzung ein Randdienst beispielsweise zur Analysezwecken oder ähnlich zum Einsatz kommt, welcher die Daten in ein Land ohne angemessenes Schutzniveau in Bezug auf den Datenschutz übermittelt würde?
- Kann lückenlos nachvollzogen werden, dass die Daten im Minimum während der Übermittlung (data-in-transit) und Speicherung (data-in-rest), und optional auch während der Prozessierung (data-in-processing) verschlüsselt sind?
- Ist gewährleistet, dass das Schlüsselmanagement durch den Dienstbezüger oder einen Beauftragter nicht aber durch den Diensteanbieter erfolgt?
- Kann idealerweise gewährleistet werden, dass die Daten bereits vor der Übermittlung auf die Cloud-Umgebung des Diensteanbieters durch einen Drittdienst verschlüsselt werden?
- Ist dem Dienstbezüger bekannt, welche potentiellen Zugriffspunkte der Diensteanbieter für den Zugriff auf Klartextdaten hat, beispielsweise durch die Generierung eines Speicherabbilds (Memory-Dump) eines laufenden Systems zu Supportzwecken?
- Ist dem Dienstbezüger bekannt, aus welchem Land der Diensteanbieter Supportleistungen erbringt? Kann er nachvollziehen, dass zum Zwecke der Betriebsunterstützung keine schützenswerten Daten in ein Land ohne angemessenes Schutzniveau in Bezug auf den Datenschutz übermittelt werden müssen?
- Ist der Diensteanbieter willens und in der Lage, seine Unterauftragsverhältnisse offen zu legen und hat der Diensteanbieter eine Informationspflicht sowie der Dienstbezüger ein Vetorecht, im Falle, dass

während der Laufzeit ein neues Unterauftragsverhältnis zustande kommt und der Dienstbezüger sich mit diesem nicht einverstanden erklären kann?

- Kann der Dienstbezüger gewährleisten, dass ein Rückzug aus der Cloud-Umgebung des Diensteanbieters vollumfänglich und innert nützlicher Frist (in der Regel innerhalb von drei bis sechs Monaten) möglich ist, ohne einen wesentlichen Serviceeinbruch in Kauf nehmen zu müssen? Kann diese Vorgabe auch im Falle eines Besitzwechsels seitens des Diensteanbieters gewährleistet werden?
- Kann der Dienstbezüger gewährleisten, dass er im Falle eines Datenverlustes diese vollumfänglich und unter Wahrung sämtlicher Sicherheitsvorgaben wiederherstellen kann?
- Kann der Dienstbezüger den Service in ausreichender Qualität aufrechterhalten, wenn dieser durch eine Beeinträchtigung der Cloud-Umgebung des Diensteanbieters beeinflusst wird? (Service Kontinuität)
- Räumt der Diensteanbieter dem Dienstbezüger ein ausreichendes Prüfungsrecht ein? (Penetrationstesting und Auditing) Legt der Diensteanbieter externe Prüfungsberichte gegenüber dem Dienstbezüger offen?
- Kann der Dienstbezüger auf eine ausreichend verfügbare Konnektivität zur Cloud-Umgebung des Diensteanbieters zählen?
- Hat der Dienstbezüger eine Risikoanalyse unter Berücksichtigung der regulatorischen Empfehlungen durchgeführt und verwaltet er die Risiken während der kompletten Laufzeit des Dienstes?

12 Technische und organisatorische Massnahmen

12.1 Bestimmung der Risiken nach Usecase

Im vorherigen Abschnitt dieses Dokuments wurden die verschiedenen Anwendungsfälle beschrieben und die zentralen Prüffragen aufgeführt. Die Antworten auf die einzelnen Fragen helfen die vorhandenen Risiken zu identifizieren. Hilfreich bei der Identifikation der Risiken ist zudem die Verwendung eines Risikokatalogs.

Anhand der Antworten auf die Fragestellungen kann der Risikokatalog bearbeitet und jeweils entschieden werden, ob ein Risiko zutrifft oder nicht. Ein Risikokatalog kann zum Beispiel folgende Risiken enthalten (basierend auf Enisa Cloud Computing Risk Assessment):

Organisatorische Risiken

R.1 Lock-in

R.2 Verlust der Vorgabenkontrolle

R.3 Compliance Herausforderungen

R.4 Reputationsverlust

R.5 Ausfall oder Beeinträchtigung des Cloudservice

R.6 Übernahme des Cloudanbieters

R.7 Versagen der Lieferkette

Technische Risiken

R.8 Zu hohe oder zu geringe Bereitstellung von Ressourcen

R.9 Ungenügende Trennung zu Cloudumgebung von anderen Kunden

R.10 Insider-Risiko bei Cloudanbieter

R.11 Kompromittieren der Anwendungsschnittstelle zur Cloud

R.12 Ausspähen oder abhören von Informationen bei der Übertragung

R.13 Datendiebstahl beim Up- oder Donwload

R.14 Unzureichende Datenlöschung

R.15 Distributed denial of Service (DDoS)

R.16 Economic denial of Service (EDOS)

R.17 Verlust der Verschlüsselungs-Schlüssel

R.18 Durchführung von missbräuchlichen Internetscanns

R.19 Kompromittieren von der Cloud-Serviceinfrastruktur

R.20 Konflikte zwischen der lokalen Sicherung und der Sicherung in der Cloudumgebung

Rechtliche Risiken

R.21 Rechtlich erzwungener Zugriff auf Daten

R.22 Veränderung der rechtlichen Rahmenbedingungen

R.23 Datenschutzrisiken

R.24 Lizenzrisiken / Lizenzverletzungen

Sind die Risiken identifiziert, geht es darum deren Auswirkungen zu bestimmen. Dabei muss zum Beispiel unter Verwendung empirischer Daten bestimmt bzw. abgeschätzt werden, wie wahrscheinlich es ist, dass das jeweilige Risiko eintritt (=Eintrittswahrscheinlichkeit) und wie gross der Schaden wäre (=Schadenmass oder Auswirkung).

Schadensanalyse und Risikodimensionen in der Cloud

Alternativ kann pro Risiko das minimale und das maximale Schadenmass bestimmt bzw. abgeschätzt werden. Bei der Bestimmung des Schadenmasses ist es hilfreich, den Schaden auf die Dimensionen Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit zurückzuführen und sich jeweils zu überlegen, welches die Auswirkungen auf die Gesundheitseinrichtung sind. Beispielsweise wenn aufgrund eines Serviceausfalls die Verfügbarkeit der vom Service abhängigen Systeme nicht mehr gegeben ist.

Konkret geht es darum, einen potentiellen Schaden für die Gesundheitseinrichtung zu erheben, wenn die Videotelefonie, die Kollaborationsplattform, der Messenger Service, E-Mail oder allfällige klinische oder administrative Anwendungen nicht mehr zur Verfügung stehen, über die genannten Anwendungen Daten gestohlen, manipuliert oder unwiderrufliche gelöscht oder zerstört werden oder die Integrität der Informationen oder die Nachvollziehbarkeit der Aktivitäten nicht mehr gegeben sind. Zentral ist dabei welche Art von Informationen und Daten, in welcher Menge, in der Cloud bzw. der jeweiligen Anwendung bearbeitet werden sollen und um welche Prozesse es sich dabei handelt und wie kritisch diese für die Gesundheitseinrichtung sind.

Weiter zu berücksichtigen ist der Hoheitsverlust über die Daten, welche mit der Cloudnutzung einhergeht, die Abhängigkeit vom Cloudanbieter (Vendor Lock-in) und das Risiko, dass über die in der Cloud exponierten Systeme ein Cyber-Angriff auf die eigene Gesundheitseinrichtung erfolgen kann.

Massnahmen zur Risikominimierung

Sind die Risiken identifiziert und deren Auswirkungen auf die Gesundheitseinrichtung bestimmt, stellt sich die Frage, welche Massnahmen bereits bestehen, um die Risiken zu reduzieren und ob das Restrisiko durch die Gesundheitseinrichtung getragen wird. Sofern das Restrisiko als zu hoch erachtet wird, müssen zusätzliche Massnahmen getroffen werden, bis sich das Risiko auf dem durch die Gesundheitseinrichtungen tragbaren Niveau reduziert.

Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit müssen angemessen gewährleistet werden. Hierzu muss für die folgenden Punkte definiert werden, wie diese sichergestellt sind und welche Restrisiken bestehen. Ziel ist es, die Restrisiken auf das akzeptierte Niveau zu reduzieren und gleichzeitig rechtliche und regulatorische Vorgaben zu erfüllen.

Für folgende Punkte müssen Lösungen vorhanden und Verantwortlichkeiten definiert sein:

- Authentisierung
- Autorisierung
- Logging und Auditing
- Datensicherung (Back-up)

- Software Updates / Patching
- Perimeterschutz (Phishing, Exchange Sicherheit, Anhänge)
- Informationsschutz (Schutz nach Datenklasse)
- Data Leakage Prevention (DLP)
- Security Information und Event Management, Threat Intelligence
- Sicherheit der mit der Cloud verbundenen Endgeräte (Endpoint Protection)

Grundsätzlich stellt sich die Frage, ob die genannten Anforderungen durch Lösungen, welche der Cloudanbieter zur Verfügung stellt, abgedeckt werden können und ob diese gegebenenfalls genutzt oder entlang einer Multivendor-Strategie auf alternative Produkte gesetzt werden soll. Zentral ist hier die Frage, welche Sicherheitsprodukte die Gesundheitseinrichtung bereits einsetzt und wie zufrieden dieses damit ist bzw. ob die Lösungen des Cloudanbieters gegenüber den bestehenden Lösungen einen Vorteil hinsichtlich Wirksamkeit und/oder Kosten darstellen. Dabei muss berücksichtigt werden, ob und gegebenenfalls wie bestehende Lösungen integriert werden können.

12.2 Verschlüsslung und Schlüsselmanagement

Um Daten angemessen zu Schützen bietet sich die Verschlüsslung der Daten an. Dabei muss unterschieden werden zwischen 1) der Verschlüsslung während der Übertragung (in transfer), 2) der Verschlüsslung im Datenspeicher (at rest) und 3) der Verschlüsslung in der Bearbeitung (in process). Zwingend und unbestritten ist die Datenverschlüsslung während der Datenübertragung in die Cloud. Dies muss immer sichergestellt sein.

Schlüsselmanagement bei Verschlüsselung im Datenspeicher

Hinsichtlich der Verschlüsslung der Daten im Datenspeicher in der Cloud (at rest) bestehen je nach Cloudanbieter verschiedene Lösungen für das Schlüsselmanagement, welche es zu evaluieren gilt. Ein zentrales Unterscheidungsmerkmal ist, ob das Schlüsselmanagement durch den Cloudanbieter in der Cloud erfolgt (wobei jeder Kunde seinen eigenen Schlüssel erhält) oder ob das Schlüsselmanagement lokal durch die jeweilige Gesundheitseinrichtung erfolgt. Ist letzteres der Fall, trägt die Gesundheitseinrichtung die volle Verantwortung für das Schlüsselmanagement. Dieses wiederum ist Voraussetzung, dass die Daten in der Cloud bearbeitet werden können. Oder anders gesagt, wenn das Schlüsselmanagement nicht sichergestellt ist, kann die Cloud inkl. der aufgeführten Anwendungsfälle nicht genutzt werden.

Findet das Schlüsselmanagement durch den Cloudanbieter statt, garantiert und verantwortet dieser die Funktionalität. Allerdings besteht dadurch das Risiko, dass sich der Cloudanbieter bzw. einzelne Mitarbeitende mit entsprechenden Rechten, missbräuchlich Zugriff auf den Schlüssel und somit auf die Daten verschaffen, was bei einem lokalen Schlüsselmanagement nicht möglich ist. Daher stellt sich auch die Frage, wie auf die Schlüssel zugegriffen werden kann.

Eine zusätzliche Sicherheit bieten hier Lösungen, welche sicherstellen, dass Zugriffe durch Mitarbeitende des Cloudanbieters zusätzlich autorisiert werden müssen. Dies kann wiederum durch dedizierte Personen des Cloudanbieters mit entsprechenden Kontrollaufgaben stattfinden oder aber über durch die jeweilige Gesundheitseinrichtung bestimmte eigene Mitarbeitende.

Dabei ist zu beachten, dass die Mitarbeitenden, welche die Zugriffe autorisieren müssen, gemäss den benötigten Servicelevels zur Verfügung stehen müssen. Wenn es aufgrund der Servicelevels erforderlich ist, dass Administratoren des Cloudanbieters ausserhalb der Bürozeiten Unterstützung leisten können müssen, müssen die Personen, welche die Zugriffe der Administratoren autorisieren, ebenfalls ausserhalb der Bürozeiten zur Verfügung stehen. Andernfalls stehen die Administratoren bildlich mit dem Werkzeugkasten vor der geschlossenen Türe und können nicht unterstützen obwohl sie vor Ort sind.

Schlüsselmanagement bei Verschlüsselung in der Bearbeitung

Eine besondere Herausforderung ist die Datenverschlüsslung der Daten in Bearbeitung (in process); insbesondere, wenn die Verarbeitung bei SaaS Lösungen direkt in der Cloud und nicht lokal oder im Browser geschieht Die Lösungen hierfür unterscheiden sich von Cloudanbieter zu Cloudanbieter. Vereinfacht kann zusammenfassend gesagt werden, dass die Lösungen immer eine gewisse Komplexität und eine

damit verbundene Fehleranfälligkeit mit sich bringen und Einschränkungen auf die Funktionalitäten haben.

Die Datenverschlüsslung der Daten in Bearbeitung setzt voraus, dass die Personen (In- und Externe), welche die Daten in der Cloud bearbeiten, während der Bearbeitung einen Schlüssel verwenden, welcher sich nicht beim Cloudanbieter befindet. Entsprechend muss die Kryptographie von der Gesundheitseinrichtung verwaltet werden. Dies bedeutet zum Beispiel, dass bei einer gemeinsamen Datenverarbeitung einer Gesundheitseinrichtung mit externen Partner in einer Cloudanwendung, der externe Partner zuerst auf die Infrastruktur der Gesundheitseinrichtung zugreifen können muss, um sich ein Zertifikat (Schlüssel) ausstellen zu lassen, mit welchem er anschiessend die Daten in der Cloud in der Anwendung entschlüsseln und bearbeiten kann.

Allein diese Konstellation ist komplex und bringt daher Risiken für die Verfügbarkeit mit sich. Hinzu kommt, dass die genutzte Verschlüsslungslösung nachhaltig kompatibel mit der jeweiligen Cloudanwendung sein muss. Ist dies nicht gegeben, kann die jeweilige Anwendung nicht mit der Verschlüsslungslösung verwendet werden.

Ob potentiell eine Lösung für die Verschlüsslung der Daten in Bearbeitung in der jeweiligen Cloudanwendung besteht und welche Einschränkungen deren Nutzung auf die Funktionalität hat, muss jeweils konkret geklärt werden. Aktuell ist keine Lösung bekannt, welche eine zuverlässige Verschlüsslung für Daten in process bei voller Funktionalität erlaubt. Wird auf die Verschlüsslung der Daten in Bearbeitung verzichtet, ist zwar die volle Funktionsfähigkeit gegeben, die Daten während der Zeit der Bearbeitung aber potentiell durch Mitarbeitende des Anbieters mit entsprechenden Zugriffsrechten einsehbar.

Dieses Dokument liegt in verschiedenen Sprachfassungen vor. Im Zweifelsfall geht die deutsche Version vor.

Über die Autoren

Erik Dinkel

Erik Dinkel ist seit 2018 CISO und seit 2024 zusätzlich Chief Security Officer des Universitätsspitals Zürich (USZ). Vor der Zeit am USZ war Erik Dinkel im Business Risk Management und als Head Access Governance bei der Credit Suisse Schweiz. Er verfügt über einen Masterabschluss der Universität Zürich (M.A. UZH) in Politikwissenschaft sowie über einschlägige Weiterbildungen in den Bereichen Unternehmensführung, Risikomanagement und Informationssicherheit (CAS UZH, CAS FHNW, BSI). Er ist seit 2021 Lehrbeauftragter für Cyber- und Informationssicherheit an der Hochschule Luzern (HSLU) und seit Ende August 2025 Präsident des Healthcare Cyber Security Center (H-CSC).

Stefan Hunziker

Der promovierte Mediziner und Wirtschaftsinformatiker leitete ab 2002 die Medizininformatik und von 2012 bis 2025 die Informatik der LUKS Gruppe. Daneben vertrat er als CIO den Gruppenbereich der Informatik von 2021 bis 2025 in der Geschäftsleitung der LUKS Gruppe. In dieser Zeit war er massgeblich verantwortlich für die IT-Integration des Spitals Nidwalden in die LUKS Gruppe. Ab 2026 unterstützt er das Universitätsspital Zürich als Projektleiter in der digitalen Transformation.

Stefan Juon

Stefan Juon war von 2009 bis 2022 in verschiedenen Funktionen am Kantonsspital Graubünden tätig, zuletzt von 2016 bis 2022 als Informationssicherheitsbeauftragter (CISO) und als Co-Leiter ICT. Er verfügt über Ausbildungen im Ingenieurwesen und in der Betriebswirtschaft auf Tertiärstufe sowie über weiterführende Qualifikationen in den Bereichen Informationssicherheit, Risikomanagement und IT-Architektur. Darüber hinaus ist er in ITIL, TOGAF und als CISA zertifiziert.

Philipp Stoll

Philipp Stoll ist ausgebildeter Maschinenbauer. Während der letzten 20 Jahre bis zu seiner Pensionierung war er Mitglied der Spitalleitung des Universitäts-Kinderspital beider Basel (UKBB). Seither ist er als Berater für Unternehmen im Gesundheitswesen tätig. Seine Schwerpunkte liegen in den Bereichen Bau, Logistik, Einkauf, Unterhalt, Medizintechnik sowie Sicherheit, mit besonderer Spezialisierung auf die Schnittstelle zwischen Nutzern und Planern. Seit 2011 ist er zudem Delegierter von H+ beim Bundesamt für Bevölkerungsschutz (BABS) und beim Bundesamt für wirtschaftliche Landesversorgung (BWL).

Werner Ulmer

Werner Ulmer ist seit 2024 CISO der Volkswirtschaftsdirektion des Kantons Zürich. Zuvor war er CISO des Kantonsspitals St. Gallen (heute HOCH Health Ostschweiz) und der Spitalverbunde, und verantwortete dort den strategischen und operativen Aufbau der Informationssicherheit bis zur erfolgreichen ISO-27001-Zertifizierung. Mit fundierten Aus- und Weiterbildungen, unter anderem an der Hochschule Luzern in Informationssicherheit und IT-Management, sowie langjähriger Erfahrung verfügt er über ausgewiesene Expertise in Cybersicherheit, Informationssicherheit, Risikomanagement und Security Governance.