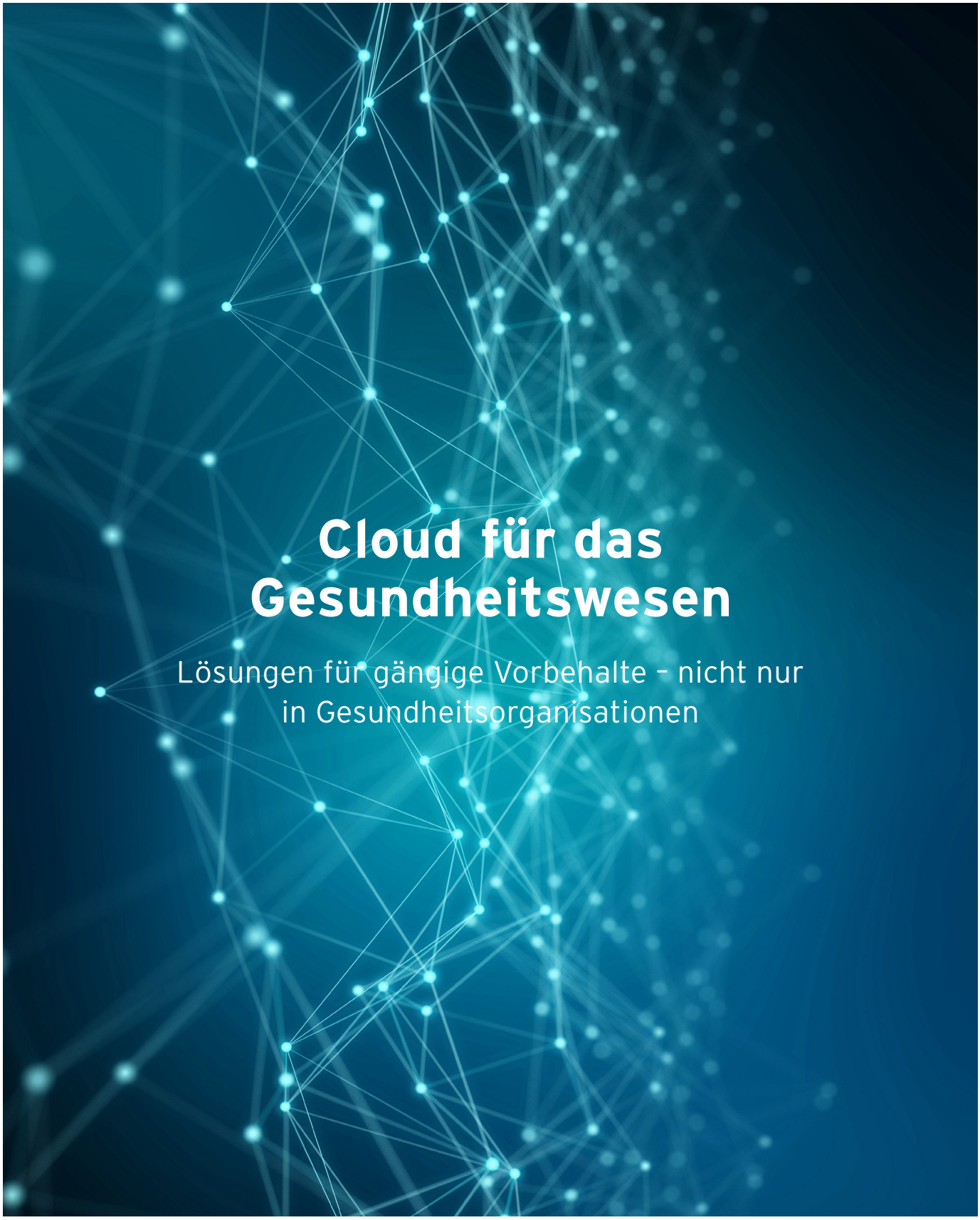
LAUX
LAWYERS AG
ZURICH | BASEL



Cloud für das Gesundheitswesen

Lösungen für gängige Vorbehalte – nicht nur in Gesundheitsorganisationen

Laux Lawyers AG
August 2023

Auf Initiative und mit freundlicher Unterstützung von aws

LAUX LAWYERS AG
ZURICH | BASEL

INHALT

I EXECUTIVE SUMMARY

Spitäler, Arztpraxen und weitere Akteure im Gesundheitswesen bearbeiten und speichern rund um die Uhr grosse Datenmengen. Die umfangreichen Datensätze enthalten zu einem grossen Teil Gesundheitsdaten. Das Kontroll- und Schutzbedürfnis von betroffenen Personen in Bezug auf **Gesundheitsdaten** ist anerkannt und unbestritten.

Das Gesundheitswesen und seine Leistungserbringerinnen sind reguliert. Gesundheitsdaten gelten als besonders schützenswert. Sie sind vertraulich zu behandeln. Das Datenschutzrecht verlangt zudem Unverfälschtheit («Integrität») und Verfügbarkeit solcher Daten. Die regulatorische Absicherung liegt im öffentlichen Interesse.

Digitalisierung verspricht dem Gesundheitswesen hohen Nutzen. Aber die Digitalisierung wird durch Vorbehalte gebremst. Was ist erlaubt? Was nicht? Es stehen viele Fragen im Raum. Und es gibt zu wenig klare Antworten. Fest steht: Digitalisierung ohne das **Vertrauen** von Patientinnen, Ärztinnen, Spitälern, Behörden, Gesetzgebern und weiteren Stakeholdern ist undenkbar.

Mitten in diesem Spannungsfeld stehen **Cloud-Services**[1]. Deren Potential ist gross: Cloud-Services erleichtern viele Digitalisierungsinitiativen erheblich. Kosten können gesenkt werden – ein Anliegen, das gerade im Gesundheitswesen zentral ist. Auch können Akteure im Gesundheitswesen bei der Nutzung von Cloud-Services ihre Effizienz steigern, die Sicherheit und Flexibilität ihrer IT-Systeme erhöhen und Ressourcen für das Kerngeschäft frei machen. Zudem können die Akteure zeitgemässe, hochskalierbare Lösungen mit höchsten Sicherheitsstandards und Ausfallsicherheit für die Erbringung von Gesundheitsleistungen, die Entwicklung neuer Behandlungsformen und – nicht zuletzt – für die personalisierte Pflege von Patientinnen und Patienten aufbauen. Die eingesetzten IT-Infrastrukturen sind funktional und betreffend Cybersicherheit auf dem modernsten Stand der Technik, auch ohne, dass die Gesundheitsinstitution hierfür eine eigene grössere IT- und Sicherheitsinfrastruktur selbst aufbauen und betreiben muss. Mit steigender Verbreitung von Cloud-Services der grossen internationalen Cloud-Anbieterinnen (sogenannte «Hyperscaler») nimmt das allgemeine Bewusstsein und das Verständnis im Hinblick auf deren Umgang mit den ihnen anvertrauten Daten zu.

Den Vorteilen können andersgelagerte **Herausforderungen** gegenüberstehen. Die Daten liegen bei der Cloud-Anbieterin. Diesbezügliche Vorbehalte werden in der öffentlichen Debatte intensiv diskutiert: Die Cloud (gemeint sind Cloud-Services) sei **datenschutzrechtlich** wie auch mit Blick auf das **Arztgeheimnis** problematisch; ausserdem würden Auslandsbezüge ihrem Einsatz entgegenstehen.

[1] Unter **Cloud-Services** verstehen wir in diesem White Paper die Gesamtheit der Leistungen, mit denen eine Anbieterin einer Gesundheitsinstitution die Nutzung gewisser IT-Infrastrukturen gewährt. Dieses Angebot erfolgt standardisiert, automatisiert, skalierbar und in nicht dedizierter Form über Datennetze. **«Cloud-Service»** steht hier auch stellvertretend für den umgangssprachlich geprägten Begriff **«Public Cloud»**, was zum Ausdruck bringen soll, dass die Basiskomponenten der Anbieterin für keine Kundin individuell-exklusiv («dediziert») nutzbar sind; demgegenüber ist die bereitgestellte Nutzungsmöglichkeit innerhalb eines Tenants individuell und abgegrenzt gegenüber anderen Kundinnen («Isolation»), was z.B. mittels Netzwerktechnologie ermöglicht wird.

Eines ist klar: Die Schweiz hat eine Kultur, in der Gesundheitsdaten ein hoher Wert beigemessen wird. Und das ist gut und richtig so. Ausdruck dieser Kultur ist, dass man Gesundheitsdaten schützen will – eben gerade, weil sie wichtig sind. Dies führt zu den folgenden grundlegenden Erkenntnissen bzw. wichtigen Anforderungen:

- **Erstens,** es gibt ein grosses Gefährdungspotential im Zusammenhang mit Gesundheitsdaten
- **Zweitens,** Patientinnen sind deswegen vor Missbrauch ihrer Daten zu schützen
- **Drittens,** Patientinnen sollen deswegen darüber entscheiden dürfen, ob andere ihre Daten einsehen
- **Viertens,** anvertraute Daten der Patientinnen sollen im Einflussbereich der Ärztin verbleiben
- **Fünftens,** es braucht hohe Sicherheitsvorkehren zum Schutz der Daten der Patientinnen.

Diese Anforderungen und die diesen zu Grunde liegenden Werte sind das Fundament, auf dem dieses White Paper aufbaut. Die Autoren halten sie hoch und bekräftigen deren Bedeutung.

Dies bedeutet jedoch nicht, dass die Autoren von der Cloud abraten oder die problematisierenden Positionsbezüge, die mitunter vorgetragen werden, teilen. Im Gegenteil. Obschon man sich über die grundlegenden Anforderungen und Werte einig ist, leidet die öffentliche Diskussion über die Cloud im Gesundheitswesen an Missverständnissen.

Gesundheitsrecht spielt sich zu grossen Teilen in öffentlichen Spitälern ab. Das Gesundheitswesen steht diesbezüglich, soweit es kantonal organisiert wird, unter der **Aufsicht der kantonalen Behörden.** Die kantonalen Datenschutzbehörden gestalten die Diskussion aktiv mit und erlassen Leitfäden, Checklisten und Merkblätter. **Diese sind Meinungsäusserungen und als solche für Institutionen im Gesundheitswesen unverbindlich[2].** Dasselbe gilt für Empfehlungen der einschlägigen Branchenverbände. Die Verunsicherung nimmt dennoch zu.

Die nachfolgenden Ausführungen zeigen, dass gewisse in der öffentlichen Debatte diskutierte Vorbehalte einer rechtlichen Prüfung nicht standhalten.

Cloud für das Gesundheitswesen ist möglich und bietet viele Vorteile

Dem Gesundheitswesen ist Sorge zu tragen. Es ist ein entsprechend hoher Sorgfaltsmassstab anzuwenden. **Gesundheitsinstitutionen können diese rechtlichen Herausforderungen mit den heute verfügbaren, qualitativ und sicherheitstechnisch hochstehenden Cloud-Services meistern.**

2 Im Gesundheitswesen spielt das kantonale Datenschutzrecht eine grosse Rolle. Bei Meinungsäusserungen von kantonalen Datenschutzaufsichtsbehörden handelt es sich um ein Instrument des proaktiv kommunizierten rechtlichen Gehörs – die Stelle erklärt vorab, wie sie einen bestimmten Fall rechtlich beurteilt. Dies dient der Rechtsklarheit und der Planungssicherheit und somit dem effizienten Mitteleinsatz jener, die durch einen Entscheid einer solchen Stelle – soweit sie Entscheidungskompetenz hat – beeinträchtigt oder gebremst werden könnten. Öffentliche Verlautbarungen sind somit vorrangig nur für die kantonale Datenschutzstelle selbst bindend. Das Spital darf – was die Datenbearbeitung bei der Erbringung von Gesundheitsleistungen unter dem kantonalen Leistungsauftrag betrifft – darauf vertrauen, dass die Aufsichtsbehörde das Gesetz wie in der Verlautbarung beschrieben anwenden wird. Es handelt sich aber *für das Spital nicht* um rechtlich verbindliche Anordnungen.

II CLOUD FÜR DAS GESUNDHEITSWESEN

Gesundheitsdaten in der Cloud

Dieses White Paper beleuchtet aus verschiedenen rechtlichen Blickwinkeln die Frage, ob Spitäler, Arztpraxen und weitere Gesundheitsinstitutionen Gesundheitsdaten «in der Cloud» speichern und bearbeiten dürfen. Was umfasst der Begriff «Gesundheitsdaten» aus rechtlicher Sicht? Verschiedene Gesetze nutzen den Begriff oder eine Abwandlung davon. Eine allgemeingültige rechtliche Definition gibt es nicht.

Das Bundesgesetz über den Datenschutz (die revidierte Fassung vom 25. September 2020 hiernach: **DSG**) sowie die kantonalen Datenschutzgesetze regeln Anforderungen an den Umgang mit **Personendaten**. Im Kontext Spital oder Arzt betrifft dies einerseits Stammdaten (allgemeine Personendaten wie Name, Adresse und Versichertennummer) und andererseits Gesundheitsdaten, die sich auf die jeweilige Patientin beziehen. Zu den Gesundheitsdaten gehören Angaben zum vergangenen oder aktuellen Gesundheitszustand, zum Behandlungsverlauf sowie zur Inanspruchnahme und Abrechnung von Gesundheitsleistungen. Zum datenschutzrechtlichen Begriff der Gesundheitsdaten gehören aber nicht nur Angaben zu aktuellen oder vergangenen Krankheiten oder Unfällen, sondern auch Ergebnisse aus Untersuchungen (z.B. Untersuchung von Blutproben oder genetischen Daten), aus denen sich Krankheitsrisiken oder andere Angaben zum künftigen Gesundheitszustand ableiten lassen.

Gesundheitsrechtliche Spezialgesetze präzisieren dieses weite Verständnis. Auch ist zu beachten, dass im Kontext einer Diagnose, Untersuchung oder Behandlung in einem Spital oder in einer Arztpraxis, oder aber im Rahmen der Forschung am Menschen, sogar Informationen zum Lebensstil (z.B. Ernährung, Rauchen, Bewegung), Daten zum Lebensumfeld (z.B. Luft- und Wasserqualität), zum sozialen Umfeld (z.B. Familie oder Beruf) wie auch Fitness-Messdaten einen Gesundheitsbezug haben und somit in solchem Kontext als Gesundheitsdaten qualifiziert und kategorisiert werden.

Gesundheitsdaten (Begriff)

Gesundheitsdaten sind Daten über den vergangenen, aktuellen oder künftigen Gesundheitszustand eines Menschen. Dazu gehören im Kontext Spital oder Arztpraxis selbst Informationen zum Lebensstil und zum sozialen Umfeld der Patientin sowie Resultate von Untersuchungen, aus denen sich Angaben zum Gesundheitszustand ableiten lassen.

1. Gesundheitsdaten als besonders schützenswerte Personendaten
Das DSG und kantonale Datenschutzgesetze kategorisieren Gesundheitsdaten als besonders schützenswerte Personendaten (oder ähnlich: besondere Personendaten). Der Gesetzgeber sieht den besonderen Schutzbedarf in erster Linie darin, dass das Gefährdungsrisiko bei unkontrollierter Bekanntgabe oder Offenlegung besonders hoch ist. Im Wesentlichen ist hier der Diskriminierungsschutz angesprochen. Die Patientin soll davor geschützt werden, vom Staat, von Versicherungen, vom sozialen Umfeld oder im Beruf aufgrund eines Gesundheitszustands stigmatisiert oder diskriminiert zu werden.

Mit anderen Worten: Es soll verhindert werden, dass in unkontrollierter Weise die Kreise jener erweitert werden, die Klartextzugriff auf besonders schützenswerte Personendaten erhalten (sog. unkontrollierte Kreiserweiterung). Eine Patientin muss sich darauf verlassen können, dass die Ärztin ihre Datenbearbeitungen professionell betreibt. Dies muss ebenso zuverlässig funktionieren wie die Verschwiegenheit der Ärztin. Wenn die Patientin sich einer Ärztin anvertraut, sollen die Information deren Einflussbereich nicht verlassen. Die Ärztin muss in diesem Sinne ihren Kreis (konkret: ihre Arztpraxis mit allem, was dazugehört, auch IT-Mittel wie z.B. Cloud-Services, die sie einsetzt) kontrollieren.

Besondere Schutzbedürftigkeit

Die besondere Schutzbedürftigkeit ergibt sich bei Gesundheitsdaten daraus, dass die betroffene Person z.B. wegen einer unkontrolliert bekannt gewordenen Erkrankung Nachteile erleiden könnte.

Beispiele für Nachteile:
- Stigmatisierung im sozialen Umfeld
- Diskriminierung am Arbeitsplatz (wirtschaftliche Folgen oder psychische Beeinträchtigung)
- Diskriminierung durch Versicherung (Kostenrisiko, Einschränkung der Wahl der Vertragspartner oder der verfügbaren Leistungen)

2. Zum Gefährdungsrisiko von Gesundheitsdaten
Der Missbrauch von Gesundheitsdaten kann im Extremfall sehr gravierende Konsequenzen nach sich ziehen. Das Gefährdungspotential lässt sich an konkreten Beispielen aufzeigen (siehe Anhang «zu den Elementen der Risikoanalyse»). In der Praxis werden gestützt darauf aber unzutreffende Schlüsse gezogen. Manchmal gehen die Perspektiven dabei verloren.

Mit Blick auf diese Ausführungen wird klar: Es wäre falsch zu sagen, dass sich die Gefahr aus der Information selbst ergibt. Ein und dieselbe Information über die Gesundheit kann zu unterschiedlichen Gefährdungsrisiken für die Persönlichkeits- und Grundrechte der betroffenen Person führen, je nachdem, wer die Daten in welchem Kontext wie einsieht oder bearbeitet. Die Gefahr kann nicht abstrakt eingeschätzt werden, sondern muss im konkreten Fall angesehen werden.

Was ist das Problem einer unkontrollierten Kreiserweiterung?

Unkontrollierte Kreiserweiterung meint den Vorgang, dass eine offene Anzahl von Personen Gesundheitsdaten erhält und damit machen kann, was sie will. Auch Missbräuche sind dann möglich. Gerade bei Gesundheitsdaten ist es somit wichtig, vor unkontrollierter Kreiserweiterung zu schützen.

Zum Hintergrund:

- Gehen Daten an einen **offenen Empfängerkreis**, der in Bezug auf die so erhaltenen Personendaten **keiner Kontrolle** untersteht, entsteht eine unkontrollierbare Situation. Typisches Beispiel ist ein Data Breach. Eine grosse Vielzahl potenzieller Schädiger können eine grosse Vielzahl von potenziellen Schädigungshandlungen vornehmen, ohne dass sich dieses Risiko reduzieren lässt. Diese Risikosituation lässt sich nicht beherrschen.
- Gehen sie an eine **bestimmte Empfängerin**, die einer **Kontrolle** in Bezug auf die übermittelten Personendaten untersteht, kann man demgegenüber konkret bewerten, welches konkrete Risiko von der konkreten Empfängerin ausgeht. Diese Risikosituation lässt sich beherrschen.

Mit anderen Worten: Erst der Verwendungszusammenhang **(Kontext)** macht eine Datenbearbeitung risikoreich. Eine Aussage über den Gesundheitszustand eines Menschen kann je nach Verwendungszusammenhang eine andere Bedeutung erlangen. Beispielsweise haben Fitness-Messungen im Freizeit-Kontext eine andere Bedeutung, als wenn sie in eine medizinische Diagnose einfliessen oder eine Grundlage für Therapieentscheidungen sind. Im Anhang wird genauer aufgezeigt, inwiefern sich Risikoaussagen aus dem Kontext ergeben.

Greift man diese Erkenntnis für das vorliegende White Paper auf, wird klar: Der Verwendungszusammenhang bzw. der Verwendungszweck einer Bearbeitung ändert sich nicht dadurch, dass man Cloud-Services nutzt. Bei Nutzung von reifen Cloud-Services[3] werden die Gesundheitsdaten ja eben gerade nicht einer unbestimmten Vielzahl von Personen zugänglich gemacht. Die Daten werden bei einer bestimmten Empfängerin gespeichert, und zwar in kontrollierter Weise (dies sicherzustellen ist die Pflicht der Gesundheitsinstitution).

Eine unkontrollierte Kreiserweiterung liegt auch nicht vor, wenn z.B. eine ausländische Strafverfolgungsbehörde im Rahmen eines Gerichtsverfahrens eine Herausgabe gewisser Daten bei der Cloud-Anbieterin verlangt. Diesbezüglich sind die (theoretischen) Risiken konkret zu bewerten. Aber es tritt keine unkontrollierte Kreiserweiterung ein, solange der Vorgang vom Gericht rechtsstaatlich genügend beaufsichtigt wird und die Behörde die Daten nicht ihrerseits einer unbestimmten Vielzahl von weiteren Empfängerinnen offenlegt (z.B. durch Publikation oder dergleichen) oder zweckwidrig verwendet (ausserhalb der Strafverfolgung). Welche Verwendungshandlungen sie vornimmt, ist allerdings zu eruieren. Und daran muss die Risikobewertung (in konkreter Weise) anknüpfen.

Die Nutzung von Cloud-Services an sich ist somit nicht Auslöser dafür, von einer unkontrollierten Kreiserweiterung zu sprechen. Der Gang in die Cloud ist diesbezüglich vielmehr ein Vorgang wie jeder andere, auch wenn es um Gesundheitsdaten geht: Man muss mögliche Gefährdungen erkennen und deren Eintretenswahrscheinlichkeit (Probability) sowie deren Schädigungspotential (Impact) beschreiben. Daraus lässt sich im Sinne einer Synthese eine Risikoaussage treffen. Nicht mehr und nicht weniger ist verlangt.

[3] Der Begriff des **«reifen Cloud-Services»** ist ein Sammelbegriff. Eine Anbieterin eines reifen Cloud-Service soll in Bezug auf Leistungserbringung, Informationssicherheit und Governance einen kontrollierten Zustand herstellen. Tut sie dies, kann man ihre Cloud-Services als «reif» bezeichnen. Die Anbieterin eines reifen Cloud-Services muss die eigene IT-Infrastrukturen, die zur Leistungserbringung eingesetzten Personen und die dazu definierten Abläufe kontrollieren. Ausserdem muss sie bereit sein, der Kundin gegenüber Aufschluss zu geben, welche dieser Massnahmen sie erbringt, so dass die Gesundheitsinstitution als Kundin in der Lage ist, die Cloud-Anbieterin und ihre Leistungen in ihre Kontrolle einzubinden.

Konkrete Anwendungsfälle von Cloud-Nutzung im Gesundheitswesen

1. Einleitung

Das Gesundheitswesen ist hoch reguliert. Eine Vielzahl von Spezialgesetzen geben Rahmenbedingungen für die Tätigkeiten von Spitälern, anderen Erbringern von Gesundheitsleistungen, Forschenden, Herstellern von Medizinprodukten oder Medikamenten und weiteren Akteuren im Gesundheitswesen. Die gesundheitsrechtlichen Spezialgesetze und Ausführungsverordnungen[4] enthalten auch Regeln, welche die allgemeinen Regeln des Datenschutz- und Geheimnisrechts ergänzen oder für einen bestimmten Anwendungsfall (z.B. Forschung am Menschen oder genetische Untersuchungen am Menschen) konkretisieren. Die entsprechenden Regeln gelten unabhängig von der eingesetzten Infrastruktur oder Technologie. Beispielsweise entscheidet der Verwendungszweck darüber, ob es sich bei einer Software um ein Medizinprodukt handelt.
Der Entscheid, einen Cloud-Service einzusetzen, wirkt sich somit insofern «neutral» aus, als die Regeln ohnehin auch beim Einsatz einer «on-premises-Lösung» gelten. Die nachstehende Analyse einiger typischer Anwendungsfälle zeigt dies exemplarisch. Was sich ändert, sind die eingesetzten Mittel beispielsweise der Kontrollausübung – wobei gerade im Bereich der Informationssicherheit Cloud-Services Kontrollmöglichkeiten erhöhen, Gesundheitsinstitutionen aber auch organisatorisch sicherstellen müssen, dass sie die Kontrollmöglichkeiten konsequent einsetzen.

2. Klinikinformationssystem in der Cloud

Klinikinformationssysteme (KIS) sollen den Alltag in einem Spital umfassend abbilden. Für die datenschutzrechtlichen Aspekte sind dabei insbesondere Bestimmungen zur Dokumentationspflicht und zur Aufbewahrungspflicht relevant. Soweit sich aus der Bearbeitung im KIS erheblich erweiterte Nutzungszwecke ergeben, müsste auch dies datenschutzrechtlich erörtert werden. Im Folgenden werden die sich ergebenden rechtlichen Anforderungen (insb. aus dem Geheimnisrecht und dem kantonalen Datenschutzrecht) an das KIS eines Spitals erörtert. Keiner dieser Aspekte ist aber spezifisch Cloud-feindlich. Oder anders: Mit der Cloud werden diese Themen nicht problematischer, sondern oft besser adressiert, dazu Folgendes:

Inwiefern ändert die Cloud etwas für den Einsatz eines KIS im Spital?

Thema	Anforderung[5]	Einfluss der Cloud
Patientendossier	Informations-, Einsichts- und Herausgaberechte aus kantonalen Gesundheits- und Patientengesetzen[6]	neutral (funktionale Anforderung[7])
	Auskunfts-, Herausgabe-, Berichtigungs- oder Löschrechte gestützt auf Datenschutzrecht	neutral (funktionale Anforderung)
Gesamtsystem (KIS)	Alle zum Geheimnis verpflichteten Personen müssen ihr Berufsgeheimnis wahren können; dies, obwohl eine Gesamtorganisation am KIS angeschlossen ist (Geheimnispflichten).	neutral (Berechtigungskonzept nötig) (funktionale Anforderung)
	Schutz vor unberechtigten Zugriffen (Informationssicherheit, aufgrund Datenschutz- und Geheimnispflichten; ebenso gestützt auf Leistungsauftrag[8])	neutral (Cloud meist besser) (funktionale Anforderung)
	Schutz vor unberechtigter Veränderung (Informationssicherheit, aufgrund Datenschutz- und Geheimnispflichten; ebenso gestützt auf Leistungsauftrag)	neutral (Cloud meist besser) (funktionale Anforderung)
	Sicherung der Verfügbarkeit (Informationssicherheit, Datenschutz; ebenso gestützt auf Leistungsauftrag)	neutral (Cloud meist besser) (nicht-funktionale Anforderung)
	Prozesse für den Export von Patienteninformationen, Löschkonzept sowie Protokollierung von Zugriffen und Datenbearbeitungen (Good Governance).	neutral (funktionale Anforderung)

Die Darstellung zeigt, dass die gesetzlichen und vertraglichen Anforderungen an die Dokumentation, Aufbewahrung, Informationssicherheit und die Wahrung von Rechten der Patienten sich nicht ändern, wenn ein Spital sein KIS auf einer Cloud-Infrastruktur bereitstellen und betreiben lässt. Relevant sind meist die funktionalen Eigenschaften. Auch an der Anforderung an das Arztgeheimnis ändert sich nichts (siehe dazu z.B. Vorbehalt 1, unten).

Was sich ändert: Es kommt zu einer Auslagerung der Datenbearbeitung. Das Spital muss die Weisungsgebundenheit und angemessene technische und organisatorische Schutzmassnahmen vertraglich absichern. Das ist machbar, wie die Erfahrung zeigt.

Anzumerken bleibt das Folgende: Häufig ist der Wechsel zu einem KIS als Cloud-Service nicht der erste Schritt eines Spitals in die «Cloud». Erfahrungsgemäss stehen vielmehr Anwendungen wie ein Patientenportal (z.B. zur Terminbuchung), Informationssicherheitslösungen oder Schulungslösungen am Anfang der Cloud-Transformation eines Spitals. Es lohnt sich, wenn ein Spital dabei in kleineren Umsetzungsprojekten die Methodik erarbeitet und erprobt, die auch für Risikoabklärungen und Umsetzungsmassnahmen im Rahmen der Umsetzung einer Cloud-Strategie für das KIS massgebend sind.

3. «Omics» in der Cloud

Biologische und genetische Eigenschaften von Menschen beeinflussen, ob ein Medikament oder eine Therapie für sie wirksam sind. Die für die Individualisierung der Behandlung und Pflege notwendigen Daten gewinnen Wissenschafter, Pharmaunternehmen und Ärzte unter anderem durch sogenannte **omics**-Untersuchungen. Dazu gehören die Untersuchung der genetischen Veranlagung eines Menschen **(Genomics)**, die Analyse der Zusammensetzung von Proteinen im Gewebe des Menschen **(Proteomics)** und die Analyse von Stoffwechselprodukten **(Metabolomics).** Aus den Resultaten solcher **omics**-Messungen und -Analysen lassen sich Hinweise auf bestehende Krankheiten oder Krankheitsrisiken wie auch Hinweise darauf ableiten, wie Patienten auf eine Medikation oder Behandlung voraussichtlich ansprechen werden.

4 Der Anhang enthält eine Liste von Gesetzen und Verordnungen, die gemeinsam mit allgemeinen gesetzlichen Bestimmungen (z.B. DSG oder kantonale Datenschutzgesetze) den gesetzlichen Rahmen für die Cloud-Nutzung im Gesundheitswesen bilden.

5 Die hier diskutierten Anforderungen ergeben sich einerseits aus Gesetzen (z.B. Patienten- oder Gesundheitsgesetze, Datenschutzgesetz, Strafgesetz), andererseits aus vertraglichen Verpflichtungen (Anschluss an elektronisches Patientendossier) oder aus Best Practice- oder Good Governance-Überlegungen, die sich teilweise auch aus beruflichen Sorgfaltspflichten ableiten.

6 Z.B. § 19 des Patientinnen- und Patientengesetzes des Kantons Zürich; § 39a des Gesundheitsgesetzes des Kantons Bern.

7 Z.B. Exportfunktionen und die Unterstützung automatischer Löschung sowie der Einstellung von Aufbewahrungsfristen.

8 Spitäler sind im Rahmen der kantonalen Leistungsaufträge verpflichtet, die Spitalversorgung der Bevölkerung in genügender Qualität und Sicherheit sicherzustellen.

Spezialgesetzliche Anforderungen[9] an omics-Messungen: Cloud-Relevanz?		
Thema	**Anforderung**	**Einfluss der Cloud**
Daten: Gesundheitsdaten (Bearbeitung	Einhaltung Datenschutzrecht (Bund und Kantone) und Persönlichkeitsrechte	neutral
	Informations-, Aufklärungs- und Einwilligungsanfordernisse	neutral
	Schutz der Vertraulichkeit	neutral
	Schutz der Integrität	neutral
	Auswertung nur mit Einwilligung	neutral
	Need-to-Know-Prinzip	neutral
	Protokollierungen zur Gewährleistung der Rückverfolgbarkeit von Bearbeitungsvorgängen	neutral
	sichere Datenübermittlung	neutral
	Datensparsamkeit	neutral
Handlungen: Übermittlung von genetischen Daten ins Ausland	Wenn Transfer ins Ausland ohne angemessenen Datenschutz beabsichtigt ist, gilt eine Pseudonymisierungspflicht[10]: Datenhaltung in einem solchen Ausland ist ohne Einwilligung der betroffenen Person unzulässig für genetische Daten, die nicht pseudonymisiert wurden	neutral
Handlungen: Klinische Versuche	Bewilligungs- und Meldeverfahren	neutral
	Anforderungen an die Datenaufbewahrung	neutral
Handlungen: genetische Untersuchung am Menschen	Diskriminierungsverbot	neutral

4. Künstliche Intelligenz/Machine-Learning in der Cloud

Künstliche Intelligenz (KI) und Machine Learning (ML) gewinnen in der Medizin an Bedeutung. Mögliche Einsatzgebiete sind die Diagnostik von Brustkrebs oder Lungenkrebs oder die Erkennung von Gehirnblutungen in der Computertomographie. Im Vordergrund steht, etwa im Bereich der Radiologie, die Entwicklung intelligenter Medizinsoftware, die mit jeder Diagnose «lernt».

Intelligente Software wird heute als Hilfsmittel für die Diagnose eingesetzt, wobei nicht Maschinen, sondern Ärzte die Diagnose stellen. Es wird aber auch an Einsatzformen von KI und ML geforscht, bei denen die Software zumindest Teile der Diagnose übernimmt, z.B. indem sie bei der Analyse grosser Datenmengen durch Aussonderung voraussichtlich unproblematischer Erkenntnisse eines Screenings die zu untersuchende Datenmenge reduzieren. Die Medizin erhofft sich von KI und ML Vorteile wie die Entlastung von Ärzten und die Steigerung der Effizienz wie auch der Präzision.

Aus rechtlicher Sicht stellen sich vor allem Fragen hinsichtlich der Qualifizierung intelligenter Software als Medizinprodukte-Software. Swissmedic und die Europäische Kommission legen Kriterien fest, bei deren Erfüllung Software als Medizinprodukt qualifiziert wird. Diese Kriterien beziehen sich in erster Linie auf die mit der Software verfolgten medizinischen Zwecke oder auf die Untersuchungszwecke. Die Art der Speicherung und Bearbeitung – «on-premises oder Cloud» – hat darauf keinen Einfluss. Entsprechend ändert der Entscheid «on-premises oder Cloud» nichts daran, ob Software ein Medizinprodukt ist oder nicht.

9 Zentral sind das Humanforschungsgesetz (HFG), die Humanforschungsverordnung (HFV), das Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG), die Verordnung zum GUMG (GUMV), das Bundesgesetz über Arzneimittel und Medizinprodukte (HMG) sowie die Verordnung über klinische Versuche (KlinV).

10 Pseudonymisierung genetischer Daten ist erforderlich für die Datenübermittlung in Länder, deren Gesetzgebung gemäss Beurteilung des Bundesrats (https://www.fedlex.admin.ch/eli/oc/2022/568/de#annex_1) keinen angemessenen Datenschutz gewährleisten.

Zusätzlich stellen sich Fragen der ärztlichen Sorgfalt beim Einsatz von KI/ML-gestützter Software sowie Haftungsfragen. Auch diesbezüglich gibt es aber keine Cloud-spezifischen Vorgaben. Ob Cloud oder nicht: Es gelten die allgemeinen Sorgfalts- und Haftungsregeln.

Aus datenschutzrechtlicher Sicht können im Bereich KI/ML Bestimmungen zu automatisierten Einzelentscheidungen relevant werden. Allerdings liegt eine automatisierte Einzelentscheidung erst dann vor, wenn eine Entscheidung mit Rechtsfolge oder erheblicher Beeinträchtigung ausschliesslich automatisiert (d.h. von einer Software oder Maschine) getroffen wird. Solange also intelligente Medizinsoftware nur hilfsweise eingesetzt wird, Ärzte aber die Diagnose stellen, werden die entsprechenden datenschutzrechtlichen Informationspflichten und Anhörungsrechte der betroffenen Person nicht relevant. Selbst wenn sie relevant wären, handelt es sich auch hier nicht um Bestimmungen, deren Anwendung davon abhängt, ob die automatisierte Bearbeitung «in der Cloud» oder «on-premises» stattfindet.

5. Medizinprodukte in der Cloud

Hersteller und Nutzerinnen von Medizinprodukten verwenden Cloud-Services in verschiedenen Ausprägungen. Beispielsweise können Plattformen für den Austausch von Analysedaten aus der Verwendung von Insulin-Pens auf einer auf IaaS[11] basierten Infrastruktur gespeichert sein. Die Plattform selbst kann dabei im SaaS-Modell[12] bereitgestellt sein, oder aber die im Medizinprodukt verwendete Software enthält SaaS-Komponenten. Zudem wird SaaS verwendet, um Daten aus verschiedenen Medizinprodukten mit weiteren Daten – z.B. durch Anbindung an ein KIS oder an ein Laborinformationssystem – zu kombinieren.

Auf die Qualifikation als Medizinprodukt hat die Verwendung von Cloud-Komponenten keinen Einfluss. Gemäss Swissmedic entscheidet allein der Verwendungszweck (Zweckbestimmung)[13] der Software darüber, ob es sich bei der Software um ein Medizinprodukt handelt.[14] «Cloud» ist kein Zweck, sondern ein technisches Umsetzungsthema («Weg ins Ziel»). Somit entscheidet der Einsatz von Cloud-Services nicht darüber, ob die Medizinprodukteregulierung überhaupt anwendbar ist.

Wenn eine Software als Medizinprodukt qualifiziert wird, sind die Anforderungen an die Produktsicherheit und an das Qualitätsmanagement der involvierten Akteure einzuhalten. Diese Anforderungen ergeben sich aus Gesetzen, Verordnungen und Industrie-Standards.[15] Eine Analyse der gesetzlichen Anforderungen zeigt, dass im Kontext «Cloud» keine Anforderungen gelten, die nicht auch ausserhalb des Cloud-Kontexts gelten würden. Allerdings sind Cloud-spezifische Aspekte der Informationssicherheit und weiterer Aspekte der Produktsicherheit bei der Einhaltung der Anforderungen mitzuberücksichtigen.

Informationssicherheit

Gesetze und weitere Vorgaben verlangen zu Recht eine hohe Informationssicherheit im Gesundheitswesen. Dies gilt namentlich auch für die Vorgaben an Software, wenn sie als Medizinprodukt gilt. Ob für genügende Informationssicherheit gesorgt wurde, kann man nicht abstrakt beantworten. Man muss die konkrete Lösung ansehen. Allfällige technische Herausforderungen der Regulierung zu Medizinprodukten können hier nicht ausgeleuchtet werden. Letztere sind insbesondere auch im Hinblick auf technische Industriestandards, aus denen weitere Anforderungen hervorgehen können, im Einzelfall zu prüfen.

11 **Infrastructure-as-a-Service**; diese Art von Cloud-Services können die Gesundheitsinstitution davon entbinden, eigene Rechenzentren, eigene Hardware und eigene Serversoftware zu betreiben.

12 **Software-as-a-Service**; diese Art von Cloud-Services dienen dazu, dass die Gesundheitsinstitution gewisse Software (Betriebssoftware oder Anwenderapplikationen) nicht selbst betreiben und warten muss.

13 Die Definitionen von Medizinprodukten in Art. 3 MepV und Art. 3 IvDV zählen Zwecke auf, die Hardware oder Software als Medizinprodukt qualifizieren.

14 Swissmedic, Merkblatt Medizinprodukte-Software, 26. Mai 2021.

15 Relevant sind das HMG, das HFG, die MepV, die IvDV sowie die KlinV-Mep. Ergänzend gilt es eine Reihe von Industrie-Standards einzuhalten, namentlich in Bezug auf die Informationssicherheit, das Risikomanagement, das Qualitätsmanagement und die Qualitätssicherung bei Software für Medizinprodukte und bei medizinischer Gerätesoftware.

III HÄUFIGE VORBEHALTE UND MÖGLICHE LÖSUNGSANSÄTZE AUS RECHTLICHER SICHT

Einleitung

Ungeachtet dessen, dass man sich über die grundlegenden Werte einig ist, die es zu schützen gilt, gibt es in der öffentlichen Diskussion über die Cloud Missverständnisse. Weil das Schutzbedürfnis gross ist, ist es eine häufige Auffassung, dass der Einsatz von IT-Infrastrukturen Dritter herausfordernd sei. Ein Cloud-Service kann für die Gesundheitsinstitution zunächst oft komplexer erscheinen als die vertraute, eigene IT-Infrastruktur. Gesundheitsinstitutionen schliessen dann darauf, dass sie die Cloud nicht beherrschen können. Wohl aus solchen Gründen bestehen Vorbehalte gegen die Cloud. Nachdem sich die Gesundheitsinstitution aber mit der Funktionsweise des Cloud-Service und in vielen Fällen auch mit dem damit verbundenen Zugewinn an Informationssicherheit vertraut gemacht hat, lässt sich die neue Cloud-Infrastruktur einfacher verwalten, führt zu Kostenersparnissen und höherer Informationssicherheit. Ähnlich halten auch rechtliche Vorbehalte einer sachlichen Prüfung oft nicht stand. Auf einige in der öffentlichen Diskussion geäusserte Vorbehalte soll im Folgenden eingegangen werden.

Angetroffene Vorbehalte im Einzelnen

Vorbehalt 1: «Das Arztgeheimnis steht der Cloud-Nutzung entgegen.»

«Wir sind an das Arztgeheimnis gebunden. Dieses können wir bei der Nutzung von Cloud-Services nicht einhalten. Ausserdem ist die Auftragsbearbeitung nach Schweizer Datenschutzrecht unzulässig, wenn die Verpflichtungen zur Wahrung des Berufsgeheimnisses nicht eingehalten werden können. Deshalb steht das Arztgeheimnis der Cloud-Nutzung entgegen.»

Antwort: Der Vorbehalt ist unbegründet. Das Arztgeheimnis lässt sich auch bei der Cloud-Nutzung schützen und einhalten.

Bei der Nutzung von Cloud-Services kommt es zu einer Auslagerung der Datenbearbeitung. Im öffentlichen Diskurs wird oft vorschnell angenommen, eine Auslagerung in die Cloud sei gar nicht möglich, ohne dass die Cloud-Anbieterin Einsicht in die Daten erhält. Oder es wird vorgebracht, dass nur bei verschlüsselter Speicherung verhindert wird, dass Aussenstehende Kenntnis erhalten von geheimnisgeschützten Daten.

Dem Arztgeheimnis (auch «Patientengeheimnis» genannt) müssen die Geheimnisträger Sorge tragen – nicht nur aufgrund drohender Strafe. Der Geheimnisschutz ermöglicht es Patientinnen, ihren Ärzten auch unangenehme oder schambehaftete Beschwerden anzuvertrauen. Nur dies ermöglicht eine sorgfältige Untersuchung und Diagnose unter Einbezug der Patientin. Entsprechend ist es verständlich und wichtig, dass Ärzte Cloud-Services sorgfältig evaluieren – auch und gerade mit Blick auf mögliche Verletzungen des Arztgeheimnisses.

Der Umstand, dass die Cloud-Anbieterin das Gesamtsystem kontrolliert und theoretisch die technische Macht zum Datenzugriff haben könnte, kann die Ärztin zum Schluss verleiten, sie würde der Cloud-Anbieterin unweigerlich die Möglichkeit eröffnen, die auf der Cloud-Infrastruktur gespeicherten Daten tatsächlich wahrzunehmen. Dem ist aber nicht so. Bei reifen Cloud-Services ist es im alltäglichen normalen Gebrauch der Lösung (Normalbetrieb) weder notwendig noch vernünftigerweise zu erwarten, dass Aussenstehende – z.B. Supportmitarbeiterinnen der Cloud-Anbieterin – auf die Informationen «schauen» und diese tatsächlich wahrnehmen. Nur Maschinen – nicht Menschen – greifen im Normalbetrieb auf die Daten. Die Cloud-Anbieterin muss technische und organisatorische Massnahmen bereitstellen, um dies abzusichern. Verschlüsselungstechniken spielen dabei je nach Anbieterin bereits heute eine grosse Rolle. Die Bedeutung von Massnahmen der Verschlüsselung, der Kapselung von Informationen und des gesteuerten Routings wird in Zukunft weiter zunehmen.

Das Arztgeheimnis (gemäss Art. 321 StGB) ist aber nur verletzt, wenn Aussenstehende (Menschen) die in den Daten gespeicherten Informationen tatsächlich wahrnehmen. Bei diesem tatsächlichen Wahrnehmen spricht man von «Klartextzugriff». Für die Strafbarkeit ist weiter erforderlich, dass die Ärztin oder ihre Hilfsperson (z.B. Praxisassistentin) die Informationen aktiv offengelegt hat oder es schuldhaft und pflichtwidrig unterlassen hat, die Daten angemessen vor Klartextzugriffen zu schützen. Das ist, wie in mehreren Rechtsgutachten bereits dargelegt, nicht der Fall, wenn man reife Cloud-Services einsetzt.

Entscheidend ist, dass die Cloud-Kundin die von der Cloud-Anbieterin eingesetzte Cloud-Infrastruktur und die von der Cloud-Anbieterin zugesicherten Abläufe versteht. Denn wirksam kontrollieren kann nur, wer versteht, wie die Datenbearbeitung bei der Cloud-Anbieterin aussehen soll. Dies bedingt die Bereitschaft der Cloud-Anbieterin, sich mit den Bedürfnissen seiner Kundinnen auseinanderzusetzen und belastbare Antworten zu liefern.

Einige Cloud-Anbieterinnen benötigen allenfalls in sehr spezifischen, vom Kunden gewünschten Situationen im Supportfall Zugriff auf die Umgebung des Kunden. Wenn die Behandlung der Supportanfrage nicht mit Beispieldaten möglich ist, kann es dabei eventuell beiläufig zu einem Klartextzugriff auf Patientendaten kommen. Wenn die Ärztin ohne Rücksprache mit ihren Patientinnen handeln möchte, muss sie solche Cloud-Anbieterinnen mit vertraglichen und organisatorischen Massnahmen in den Kreis derjenigen nehmen, die zur Arztpraxis im weiteren Sinne und somit zur Verantwortungssphäre der Ärztin gehören. Zu entsprechenden vertraglichen Zusicherungen sind heute viele Cloud-Anbieterinnen bereit.

Vorbehalt 2: «Cloud erhöht das Risiko von Diskriminierungen.»

«Gesundheitsdaten sind besonders sensible und schützenswerte Daten. Der unbefugte Zugriff auf oder die Weitergabe solcher Daten stellt ein hohes Risiko für die Persönlichkeit und Grundrechte der Patienten dar, insbesondere das Risiko, diskriminiert zu werden. **Die Nutzung von Cloud-Services erhöht die Wirkung und/oder die Wahrscheinlichkeit der Diskriminierung.** Dies ist angesichts der Sorgfaltspflicht von Angehörigen der Gesundheitsberufe inakzeptabel.»

Antwort: Der Vorbehalt ist unbegründet. Dass bei Verwendung reifer Cloud-Services das Risiko der Diskriminierung erhöht wird, lässt sich nicht sachlich begründen.

Es ist zutreffend, dass Gesundheitsdaten besonders schützenswerte Personendaten darstellen. Das bei Gesundheitsdaten latent vorhandene Diskriminierungsrisiko muss man adressieren und abmildern – auch, aber nicht nur in Cloud-Umsetzungsprojekten.

Nicht zutreffend ist, dass der Beizug einer Cloud-Anbieterin per se zu einem Zugriff durch unbefugte Dritte führt. Jedenfalls sollte man dies nicht so pauschal behaupten. Es kommt auf die Qualität der Cloud-Anbieterin an. Eine Anbieterin mit schlechten Schutzmassnahmen kann ein Risiko einer ungewollten «Kreiserweiterung» begründen. Dann kann es zu erhöhten Risiken kommen.

Im umgekehrten Fall – Verwendung eines reifen Cloud-Service – wird die Wahrscheinlichkeit von unbefugten Zugriffen reduziert. Somit ist auch das Risiko einer Diskriminierung reduziert. Dass in einem Szenario des alltäglichen und normalen Gebrauchs der Lösung (Normalbetrieb) ohne Data Breach bei der Cloud-Anbieterin das Risiko der Diskriminierung erhöht wird, lässt sich aber nicht sachlich begründen. Zu erwähnen ist in diesem Kontext, dass das Risiko eines Data Breach bei der Cloud-Anbieterin wiederum durch technische Massnahmen reduziert werden kann (und auch im Rahmen anderer IT-Infrastruktur nicht auszuschliessen ist).

Vorbehalt 3: «Cloud lässt sich nicht kontrollieren.»

«Das Verschieben von Daten in die Infrastruktur einer Cloud-Anbieterin führt zum Verlust der direkten Kontrolle über Infrastruktur und Daten. Das Gesetz verlangt eine solche direkte Kontrolle, da Patienten nicht schlechter gestellt werden dürfen, als wenn das Spital seine eigene Infrastruktur nutzen würde.»

Antwort: Der Vorbehalt ist unbegründet. Cloud Computing bedeutet zwar einen Paradigmenwechsel, aber bei technisch versierter Umsetzung keinen Kontrollverlust und ermöglicht gegebenenfalls sogar eine erhöhte Kontrolle und Informationssicherheit.

Gesundheitsinstitutionen bewegen sich in einer sehr komplexen Umgebung. Sie sollen die Chancen der Digitalisierung in Angriff nehmen, aber wichtige Ziele nicht aus den Augen verlieren. Es ist eine sehr herausfordernde Situation, in der sich Gesundheitsinstitutionen heute befinden. Wie passt die Cloud hier rein?

Die Antwort liest sich zunächst wie eine Bürde: Gesundheitsinstitutionen müssen ihre Organisation im Griff haben. Das gilt selbstverständlich auch für die Nutzung von Cloud-Services durch Gesundheitsinstitutionen. Die Leitungsgremien müssen die Situation insgesamt kontrollieren. Sie können auch über eingesetzte Drittanbieterinnen wie eben Anbieterinnen von Cloud-Services nicht einfach hinweggehen.

Für Gesundheitsinstitutionen, die bislang einen Bogen um Cloud-Services gemacht haben, kann es auf den ersten Blick herausfordernd wirken, einen Cloud-Service in die eigene Organisation einzubinden. Die diesbezügliche Analyse ist vielschichtig und basiert auf der Prüfung einer Vielzahl von Faktoren. Es gilt dabei weiterhin: Wer kontrollieren will, muss verstehen.

Beispiel «Speicherort»

Befürchtung: Man kann nicht nachvollziehen, wo die Daten in der Cloud gespeichert sind.

Einordnung: Die Cloud-Kundin kann heutzutage den Speicherort in den meisten Cloud-Services selbst aus bestehenden Optionen auswählen. Man sollte Cloud-Anbieterinnen auswählen, die vertraglich zusichern, den Speicherort nur auf Weisung der Cloud-Kundin zu wechseln.

Beispiel «Bearbeitungen im Ausland»

Befürchtung: Man kann nicht mehr nachvollziehen, wo die Daten in der Cloud bearbeitet werden.

Einordnung: Viele Cloud-Anbieterinnen können mittels Prozessbeschreibungen klare Aussagen dazu machen, welche Dienste in welcher Weise zu einem Auslandsbezug führen.

Beispiel «Unterauftragsbearbeiter»

Befürchtung: Man kann nicht mehr nachvollziehen, wer auf Daten zugreift.

Einordnung: Eine detaillierte Kenntnis bis auf die einzelnen involvierten Individuen bei der Cloud-Anbieterin und/oder beim Unterauftragsbearbeiter muss die Gesundheitsinstitution nicht erwerben. Sie kann auf konzeptionelle Antworten abstellen. Dies umfasst die Identität der eingesetzten Unterauftragsbearbeiter und Angaben dazu, welche Hilfsdienste sie einbringen bzw. in welcher Weise sie mit den Daten in der Cloud umgehen.

Damit das Kontrollziel erreicht wird, müssen die richtigen Kenntnisse an Bord geholt werden. Es braucht einen transversalen Blick auf die Situation. Um einen solchen zu erlangen, kann die Geschäftsleitung sich helfen lassen. Wer aber gänzlich auf externe Ressourcen abstellt, macht sich abhängig vom Beratungsansatz. Es sollte das Ziel der Gesundheitsorganisation sein, nicht nur kurzfristige Compliance zu bedienen, sondern sich eher vollständig und somit transformierend auf die Cloud-Situation einzustellen. Wer eine Cloud-Transformation als Chance für die eigene Organisationsentwicklung und den Ausbau der Informationssicherheit erkennt, erwirbt echte Kontrolle (statt Compliance-Dokumentation) und macht einen grossen Fitness-Schritt in Richtung Zukunft. Ein solcher Ansatz ist sowieso eine gute Idee. Es ist vorteilhaft, sich gleich richtig darauf einzulassen (diese Chance verpasst man jedoch mit einem reinen Compliance-Ansatz).

Kontrollieren kann man nur, was man versteht. Der Umkehrschluss trifft ebenfalls zu. Genügendes Verständnis über Abläufe, welche die Kontrollziele erfüllen, führt zu Kontrolle.

Das Verständnis muss sich auf die wesentlichen Aspekte der Cloud-Infrastrukturen, Standorte, Sicherheitsarchitektur und -kontrollen, der vertraglichen Zusicherungen sowie der anwendbaren gesetzlichen und regulatorischen Anforderungen beziehen.

Gesundheitsinstitutionen können diese Antworten erarbeiten. Sie können mithin auch in der neuen Welt des Cloud Computing umfassend Kontrolle ausüben. Die Mittel der Kontrollausübung sind den neuen Gegebenheiten angepasst und oft anders gelagert, als man dies aus der alten Zeit kannte, wie eigenes Personal noch physische Geräte bedient hat.

Nur dass etwas anders ist, lässt aber keinen Schluss auf Kontrollverlust zu. Mittlerweile lässt sich mit modernen Instrumenten wie Cloud-Services bessere Kontrolle erzielen als bisher. Zugleich ist aber zutreffend: Pauschalaussagen sind nicht möglich. Die konkret eingesetzte IT-Infrastruktur muss sich im Rahmen der Prüfmethodik einer Prüfung unterziehen und die entsprechenden Tests bestehen.

Kontrollverlust: Kristallisationspunkt, Massstab und Ansatzpunkt der Prüfmethodik

Die folgenden **Anforderungen**, sollten mit **Testfragen** geprüft werden:

- Vertraulichkeit: Ist die Vertraulichkeit der zu schützenden Informationen gegeben?
- Verfügbarkeit: Ist die Verfügbarkeit gegeben?
- Integrität: Kann die Gesundheitsinstitution die Information vor ungewollter Veränderung schützen?
- Integrität: Kann die Gesundheitsinstitution von Dritten die Löschung bestimmter Informationen verlangen, die aus der IT-Infrastruktur abfliessen?
- Accountability: Änderungen an oder Zugriffe auf Daten müssen zu jedem Zeitpunkt eindeutig nachvollziehbar sein («Audit Trail»)
- Business Continuity: Kann die Gesundheitsinstitution auch nach Beizug einer Cloud-Anbieterin ihren Geschäftsbetrieb langfristig aufrechterhalten?
- Rückführbarkeit: Kann die Gesundheitsinstitution sicherstellen, dass sie jederzeit darüber bestimmen kann, mit welcher IT-Anbieterin sie arbeiten will?

Die folgenden **Kontrollpunkte** sind wichtig, um entscheiden zu können, ob die Gesundheitsinstitution weiterhin Kontrolle hat über die IT-Infrastrukturen, die sie beiziehen will:

- Zugang: Können nur berechtigte Personen kontrollierten Zutritt zu den IT-Infrastrukturen erhalten?
- Zugriff: Können nur berechtigte Personen kontrollierten Zugriff auf die IT-Infrastrukturen nehmen?
- Klartextzugriff: Kommt es im Rahmen der generellen Bereitstellung der Cloud-Services zum Zugriff auf Inhalte der Kundendaten durch die Cloud-Anbieterin?
- Support: Gibt es klare und zugesicherte Zugriffsprozesse auf Daten in Supportfällen (wo Support überhaupt notwendig wird)?

Für alle der vorstehend konkretisierten Punkte ist zu eruieren, welche Bedeutung allfällige Ereignisse der beschriebenen Art (z.B. eine Person kann Zutritt zum Rechenzentrum erhalten) haben und wie sich solche Ereignisse in Bezug auf die rechtlich relevanten Testfragen (siehe vorstehend) auswirken.
Die Kontrollpunkte werden mittels Massnahmen angegangen und es wird dann geprüft, ob diese Massnahmen geeignet sind, in Bezug auf den zu prüfenden Kontrollpunkt von einem angemessenen Risiko auszugehen. Massnahmen werden unterteilt in solche technischer, organisatorischer oder vertraglicher Natur.

Vorbehalt 4: «Cloud erhöht die Risiken; denn es gibt unzählige Unterauftragsbearbeiter.»

«Für uns als Spital ist es wichtig, auch die Kontrolle über Anbieterinnen von IaaS-Lösungen zu behalten, die von Anbieterinnen von E-Health-Software als Unterauftragsbearbeiter verwendet werden. Die Vergabe von Unteraufträgen ist aber problematisch, da wir die IaaS-Anbieterinnen nicht direkt kontrollieren werden.»

Antwort: Der Vorbehalt ist unbegründet. Kontrolle lässt sich auch beim Beizug weiterer Unterauftragsbearbeiter einhalten. Es braucht hierzu insbesondere vertragliche und organisatorische Schutzmassnahmen.

Das Datenschutzrecht lässt den Beizug von Unterauftragsbearbeitern durch Cloud-Anbieterinnen zu. Es sind dazu Voraussetzungen einzuhalten, was aber in der Praxis regelmässig gelingt.
Die beigezogene Cloud-Anbieterin darf weitere Anbieterinnen (Unterauftragsbearbeiter) zur Ausführung ihrer Leistungen beiziehen. Soweit diese Zugriff auf Personendaten erhalten (es genügt Zugriff auf verschlüsselte Daten, d.h. ohne Klartextzugriff), muss Folgendes umgesetzt sein: Die Genehmigung der Gesundheitsinstitution ist erforderlich, kann aber allgemein und im Voraus erteilt werden. Die Nutzung weiterer Anbieterinnen durch die Cloud-Anbieterin ist daher keine Kreiserweiterung, solange die Gesundheitsinstitution die Risiken kontrolliert und im Griff hat.

Pauschale Genehmigung mit Widerrufsvorbehalt

In Bezug auf Cloud-Services ist die Variante der allgemeinen Genehmigung mit Widerspruchsrecht branchenüblich und sachgerecht. Bei dieser Variante ist die Cloud-Anbieterin verpflichtet, Kundinnen über den Beizug neuer oder den Ersatz bisheriger Unterauftragsbearbeiter zu informieren und ihnen zu ermöglichen, dem Beizug zu widersprechen, was auch durch das Einräumen eines Kündigungsrechts erreicht werden kann.

Die Gesundheitsinstitution sollte sich versichern, dass spezifische Anforderungen, die sich aus gesetzlichen Vorgaben ergeben (z.B. Zusicherungen bezüglich der geheimnisrechtlichen Einbindung von Hilfspersonen, etc.), von der primären Systemanbieterin (SaaS-Anbieterin) abgebildet werden und auch relevante Unterauftragsbearbeiter entsprechende Regelungen in ihren Standardverträgen getroffen haben. Mindestens sollte eine durch Dokumentation erhärtete Erläuterung der wesentlichen Zusammenhänge vorhanden sein.

Vorbehalt 5: «Es braucht eine ausdrückliche gesetzliche Grundlage.»

«Spitäler mit einem Leistungsauftrag eines Kantons müssen bei der Bearbeitung von Gesundheitsdaten die **kantonalen Datenschutzgesetze** einhalten. Die kantonalen Gesetze verlangen, dass alle Datenbearbeitungen auf einer **gesetzlichen Grundlage beruhen**. Diese Rechtsgrundlage muss auch die Cloud-Nutzung abdecken.»

Antwort: Der Vorbehalt ist unbegründet. Auch Spitäler mit kantonalem Leistungsauftrag können Cloud-Services ohne ausdrückliche Grundlage im Gesetz nutzen. Es braucht für die Datenbearbeitung und bestimmte Verwendungszwecke eine Rechtsgrundlage in einem Gesetz – nicht aber für die eingesetzte Technologie (z.B. Cloud Computing).

Die Bundesverfassung und kantonale Verfassungen verlangen, dass staatliches Handeln auf einer gesetzlichen Grundlage basiert. Wenn Behörden in ihrem Tätigkeitsbereich Personendaten bearbeiten (müssen), brauchen sie im Grundsatz eine ausdrückliche Spezialermächtigung. Datenbearbeitungen durch Behörden soll es ohne gesetzliche Grundlage nicht geben. Das Erfordernis des Rechtssatzes ist rechtsstaatlich von grosser Bedeutung. Als Kontrollregel verfolgt die Bestimmung die folgenden Kardinalziele (im Sinne eines sog. Ausdehnungsverbots): (a) Kontrolle über wichtige Themen (umfasst Datenschutz), (b) Schutz vor Ausufern des Staats ohne Legitimierung im Rechtssatz. Die alleinige Tatsache, dass eine Behörde mit einer Aufgabe betraut wird, soll nicht für grenzenlose Datenbearbeitungen missbraucht werden.

Wenn das Gesetz sicherstellt, dass (a) die Tragweite der Datennutzung im Wesentlichen bekannt ist bzw. sich aus dem Kontext erschliessen lässt (Transparenzgebot) und (b) die Verwendungszwecke der Datennutzung nicht ausufern (Bestimmtheitsgebot), ist dem Erfordernis Genüge getan. Damit die Verwendungszwecke nicht ausufern, müssen sie im einschlägigen Rechtssatz beschrieben sein. Die zur Umsetzung der Schritte im Lebenszyklus von Daten eingesetzte Technologie ist kein eigenständiger Verwendungszweck. Dass für die Zwecke der Datenanalyse Technologien wie z.B. Cloud Computing («Weg ins Ziel») eingesetzt werden, ändert nichts am Verwendungszweck.

Es gehört nicht zum Erfordernis des Rechtssatzes, dass auch *die Mittel der Aufgabenerfüllung* im Einzelnen limitiert werden. Aus diesem Grund wird für die sog. «administrative Hilfstätigkeit» keine eigenständige gesetzliche Grundlage verlangt. Als *administrative Hilfstätigkeit* ist die Beschaffung jener notwendigen Sachgüter oder Leistungen gemeint, die die Verwaltung zur Erfüllung ihrer öffentlichen Aufgabe benötigt. Beispiele dafür sind die Beschaffung von Büromaterial, der Abschluss von Werkverträgen für die Errichtung einer öffentlichen Baute oder eben das Beiziehen einer IKT-Leistungserbringerin. Sofern für die eigentliche, legitimierungsbedürftige Tätigkeit des Staats das Erfordernis der gesetzlichen Grundlage eingehalten ist, *ist die dazu gehörende administrative Hilfstätigkeit von der gesetzlichen Grundlage miterfasst und muss nicht explizit genannt werden.* Für diese leitet sich die gesetzliche Grundlage unmittelbar aus der Rechtsgrundlage für die jeweilige öffentliche Aufgabe ab. Eine besondere gesetzliche Grundlage ist für Tätigkeiten im Rahmen der Bedarfsverwaltung nicht erforderlich.

Im Rahmen eines Umsetzungsprojekts ist die Einhaltung des Datenschutzrechts sicherzustellen, namentlich alle Anforderungen an die Datensicherheit, mithin die Technik, und die Einhaltung der Datenbearbeitungsgrundsätze. Kantonale Datenschutzaufsichtsbehörden beaufsichtigen das Umsetzungsprojekt des Spitals mit kantonalem Leistungsauftrag. Es besteht somit bereits ein genügender Schutz durch das Datenschutzrecht. **Die Meinung, dass neue Technologien stets in einem Gesetz im formellen Sinn geregelt sein müssten, lässt sich demgegenüber nicht aufrechterhalten.**

Es wird in der öffentlichen Diskussion vorgebracht, die Bürgerinnen dürften beim Einsatz von Cloud-Services nicht schlechter gestellt werden, als wenn die öffentliche Institution dieselbe Aufgabe ohne Einsatz von Cloud-Services erfüllen würde. Bei diesem Standpunkt schwingt der Gedanke mit, der Einsatz von Cloud-Services sei allenfalls nicht verhältnismässig.

In dieser pauschalen Form hält dies einer rechtlichen Überprüfung nicht stand. Beim Entscheid für eines aus zahlreichen geeigneten Mitteln hat die Behörde im Rahmen der Bedarfsverwaltung einen grossen Ermessensspielraum. Bei der Wahl des Mittels hat die Behörde das öffentliche Interesse an einer effizienten, wirtschaftlichen und sicheren Abwicklung von öffentlichen Aufgaben genauso im Blick zu halten wie die berechtigten Datenschutzinteressen betroffener Personen.

Es braucht somit eine Einzelfallbetrachtung in Bezug auf konkrete Cloud-Services, Bearbeitungsarten und den Kontext sowie die Arten verarbeiteter Daten. Cloud-Services lassen sich durchaus so einsetzen, dass bei der Durchführung derselben Verwaltungsaufgabe keine relevanten Grundrechtseingriffe vorkommen.

Vorbehalt 6: «Eine Cloud mit Risiken für Behördenzugriffe aus dem Ausland ist unzulässig.»

«Das Risiko des Zugriffs durch ausländische Strafverfolgungsbehörden oder Nachrichtendienste verbietet die Nutzung von Cloud-Services.»

Antwort: Der Vorbehalt ist unbegründet. Die Diskussion über dieses Thema nimmt heute zu viel Platz ein; das Thema kann mit technischen, organisatorischen und vertraglichen Massnahmen gelöst werden.

Die Behördenpraxis in allen Ländern dieser Welt sollte in zwei Kategorien eingeteilt und unterschieden werden. Die Unterscheidung ist wichtig, weil grundlegend unterschiedliche Überlegungen anzustellen sind:

1 Überwachung: Der Staat beabsichtigt Datenanalysen über eine grosse Zahl von Personen. Eine unbestimmte Vielzahl von Personen ist davon tangiert. Es geht um die Überwachung der Gesellschaft und womöglich um vielfältige oder unbestimmte Schutzziele. Wir möchten aber nicht in einem Überwachungsstaat leben.

2 Strafverfolgung: Der Staat beabsichtigt, ein Strafverfahren gegen eine beschuldigte Person zu führen. Es geht um Einzelne und nicht um eine unbestimmte Vielzahl von Personen. Es geht auch nicht um unbestimmte Schutzziele, sondern darum, dass Beweiserhebungen gegen eine ins Verfahren involvierte oder noch zu involvierende Einzelperson ermöglicht werden.

Im ersten Fall **(Überwachung)** geht es darum, ob und zu welchen Zwecken Überwachungshandlungen rechtsstaatlich und gesellschaftlich akzeptabel sind. Man kann differenzieren zwischen Massenüberwachung (z.B. permanent aufzeichnende Videokameras, wobei alle Aufnahmen in einer neuen Datensammlung gespeichert und allenfalls weiter untersucht werden) und systematisierter Datenerhebung (auch «Bulk Data Collection», z.B. das Durchforsten einer Datensammlung eine grosse Personenmenge betreffend anhand von Suchkriterien «Telefonnummer» oder «E-Mail-Kennung», wobei nur positive Treffer in einer neuen Datensammlung gespeichert und allenfalls weiter untersucht werden). Datenschutzrechtlich werden diese Themen im grenzüberschreitenden Kontext in den Regeln über die Bekanntgabe ins Ausland adressiert und gelöst.[16] In der Praxis kann das Risiko bezüglich dieser Art der Auslandseinmischung durch die Wahl der Speicherorte (z.B. in der Schweiz) oder technische Massnahmen (z.B. Verschlüsselung) verringert resp. über weite Strecken gänzlich ausgeschlossen werden.

Im zweiten Fall **(Strafverfolgung)** muss man beurteilen, inwiefern die Verfahrensrechte der betroffenen Person im sie tangierenden Strafverfahren gewahrt werden. Ausserdem ist zu entscheiden, wer dafür sorgen soll, dass dem so ist (der eigene Staat, ein ausländischer Staat oder allenfalls eine Cloud-Anbieterin). Anlass für diese Betrachtung ist z.B. der US CLOUD Act, der US-amerikanischen Strafverfolgungsbehörden erlaubt, von der im eigenen Staat aktiven Cloud-Anbieterin zu verlangen, dass diese Daten der Cloud-Kundin sichert (Legal Hold), damit sie anschliessend in ein Strafverfahren eingebracht werden können.[17] Dies soll auch dann möglich sein, wenn die Daten im Ausland gespeichert sind[18] (solange die Cloud-Anbieterin die Möglichkeit hat, die Daten tatsächlich herauszugeben[19]).

16 Sowohl die Adäquanzentscheide gemäss Art. 16 Abs. 1 DSG (inkl. zukünftig die Regeln zum Swiss-US Data Privacy Framework) als auch die Mechanismen rund um Transfers unter den EU-Standardvertragsklauseln (Art. 16 Abs. 2 lit. d DSG) adressieren und lösen für die Gesundheitseinrichtung diese Fragestellung.

17 Siehe zum US CLOUD Act bereits ausführlich unsere Ausführungen im White Paper «Public Cloud für Public Services – Lösungen für gängige Vorbehalte» (Link).

18 Es soll somit das möglich sein, was (für gewisse Daten: Subscriber Information, aber nicht Inhaltsdaten) in Art. 18 der Cyber Crime Convention (CCC) vorgesehen ist. Dieser Hinweis ist interessant, weil die Schweiz sich diesem internationalen Abkommen angeschlossen hat.

19 Man spricht im US-amerikanischen Recht hierbei von „Possession", „Custody" und „Control". Der juristische Widerstand geht entgegen den Abläufen von sofortigem Klartextzugriff aus, sobald ein US-amerikanischer Staatsanwalt bei der Cloud-Anbieterin einen Legal Hold beantragt. Dies ist aber nicht der Fall. Die Analyse der rein rechtlichen Begriffe wie z.B. Possession, Custody und Control greift zu kurz.

US CLOUD Act im Resultat: Was ändert sich denn überhaupt?

Im Resultat – was ändert sich denn genau mit dem US CLOUD Act? Unter dem geltenden Konzept der internationalen Rechtshilfe erhalten z.B. die USA von der Schweiz Inhaltsdaten (auch «Content» oder gemäss Terminologie der Cyber Crime Convention: «Computer Data»), allenfalls unter Auflagen. Wenn man schon von Risikoüberlegungen spricht, sollte auch der Status Quo in die Betrachtung einbezogen werden. Auch heute schon liefert die Schweiz Inhaltsdaten (Computer Data) in die USA.

Die Diskussion um den US CLOUD Act betrifft den Aspekt **Strafverfolgung**. Aber sie wird meist zu abstrakt geführt. Juristen diskutieren Zugriffsmöglichkeiten mit rein juristischen Denkansätzen. Aber diese Prüfung beantwortet die eigentlich interessierende Fragestellung nicht, nämlich: (1) ob es faktisch Klartextzugriffe von ausländischen Behörden gibt und (2) ob dann die grundlegenden Werte unserer Rechtsordnung noch eingehalten sind. Was wir als Gesellschaft eigentlich wollen und was die Patientin will: Die Patientin muss vor missbräuchlicher Datenverwendung geschützt sein («unkontrollierte Kreiserweiterung»). Man kann aber im Kontext US CLOUD Act nicht ernsthaft von einer «unkontrollierten Kreiserweiterung» oder einem rechtlich relevanten Kontrollverlust reden. In der Diskussion geht der Fokus auf das Wesentliche verloren.

US CLOUD Act: Den Fokus auf das Wesentliche nicht verlieren

Das Spital muss Patientendaten gegen Missbräuche schützen. Man kann den US CLOUD Act aber keinesfalls als ein Missbrauchsrisiko betrachten. Der US CLOUD Act steht den eingangs genannten grundlegenden Werten nicht entgegen. Wichtig ist, dass Fragestellungen rund um den Geheimnisschutz erst dann auftreten, wenn es bereits möglich ist, der betroffenen Person rechtliches Gehör oder zumindest der Gesundheitsinstitution Mitwirkungsrechte zu geben. Dies wird ausführlich im öffentlich zugänglichen Rechtsgutachten für die Stadt Zürich erörtert.[20]

Dies vorausgeschickt geht es nun nur (aber immerhin) noch um die Frage, ob mit dem dann noch verbleibenden Risiko von ausländischen Zugriffen im Cloud-Kontext angemessen umgegangen werden kann. Im Rahmen der Umsetzungsprojekte sollten dazu sämtliche Massnahmen technischer, organisatorischer und vertraglicher Art geprüft und inventarisiert werden, soweit sie dem Zweck dienen, Daten der Kundin vor Herausgabe an ausländische Behörden zu schützen. Sowohl die Cloud-Anbieterin als auch die Kundin (im Rahmen des Umsetzungsprojekts) können in der Pflicht sein, solche Massnahmen umzusetzen.

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

Massnahmen gegen Behördenzugriff		
Massnahme	**Nutzen gegen Überwachung**	**Nutzen gegen Strafverfolgung**
«Defend Your Data»-Klauseln	Ja	Ja
Kein Zugriff auf Inhalte der Kundendaten durch die Anbieterin[21]	Nein	Ja
Anerkennung von Amts- und Berufsgeheimnissen[22]	selten[23]	Ja
Vertraulichkeitszusagen	Nein	Ja
Standort des Rechenzentrums: Schweiz	Ja	Ja
Organisatorisches (z.B. Zugriffsbeschränkungen durch die Kundin involvierende Genehmigungsprozesse)	selten[24]	Ja[25]
Verschlüsselung	Ja	Ja
Weitere technische Massnahmen	Ja	Ja

«Defend Your Data» meint Klauseln, die gegen die Herausgabe von Daten an Strafverfolgungsbehörden schützen sollen, wobei die Cloud-Anbieterin eine umfassende **Verteidigungskaskade** umsetzen soll:

Verteidigungskaskade	
Direkte **Weiterverweisung** der anfragenden ausländischen Behörden an die Kundin	
falls dies nicht gelingt:	Umgehende **Benachrichtigung** der Kundin (sowie Bemühungen zwecks Beseitigung eines allfälligen Verbotes der Benachrichtigung)
falls dies nicht gelingt:	Gerichtliche **Anfechtung** von: (a) Rechtsmängeln nach US-Recht[26] (b) Konflikten mit Schweizer Recht[27]

21 Kein Klartextzugriff der Cloud-Anbieterin im Rahmen der generellen Bereitstellung der Cloud-Services; klare und zugesicherte Zugriffsprozesse auf Daten in Supportfällen (wo überhaupt notwendig).

22 Z.B. Art. 320 StGB, Art. 321 StGB; Art. 62 nDSG.

23 Der Nutzen ist nicht voraussehbar und kann nicht als belastbare Massnahme im Bereich der Massenüberwachung dargestellt werden.

24 Der Nutzen ist nicht voraussehbar und kann nicht als belastbare Massnahme im Bereich der Massenüberwachung dargestellt werden.

25 Kann im Bereich des Zugriffsschutz gegen Massnahmen der ausländischen Strafverfolgung in den USA als Massnahme behandelt werden, «Control» bei der US-amerikanischen Anbieterin zu verneinen.

26 Wenn man es abstrahiert beschreibt: «nach dem Recht der anfragenden Behörde».

27 Auch sog. «blocking statutes» sind in diesem Kontext zu nennen. Als solche gelten auf jeden Fall die Verbote an ein schweizerisches Unternehmen, auf schweizerischem Boden einer ausländischen Behörde zu helfen, ohne die eigene zuständige Behörde zu involvieren und das Vorgehen mit ihr abzustimmen (Art. 271 StGB, ähnlich: Art. 273 StGB). Auch die Geheimnispflichten nach Art. 320 StGB und Art. 321 StGB können dazugezählt werden.

Je nach Situation und Schutzbedürftigkeit ist auch zu prüfen, ob man gesteigerte oder gar annähernd absolute Sicherheit vorkehren will (z.B. Verschlüsselungstechnologien) für den Fall, dass die eher rechtlich geprägte Verteidigungskaskade nicht greifen sollte. Dies wird jedoch nur in selteneren Fällen angezeigt oder sinnvoll sein. Absoluten Schutz gegen Zugriffe im Rahmen eines Strafverfahrens (z.B. nach dem US CLOUD Act) schuldet das Spital nicht. Oft wird gerade der Ansatz «Bring Your Own Key» (BYOK) überschätzt. «Hold Your Own Key» (HYOK) bringt zwar mehr Sicherheit für die Diskussion über Behördenzugriffe, dies aber oft zum Preis von nicht zu rechtfertigenden Zusatzrisiken. In vielen Fällen wird selbst bei HYOK ein (weiterer) Provider eingebunden, was die gewonnene Schutzwirkung sogleich wieder relativiert.

Verschlüsselung: Eine gute Massnahme, umrankt von Mythen

Eine umfassende Verschlüsselung aller ruhenden Kundendaten ist kaum je zwingend. Wo eine solche möglich ist, ohne das Service-Design bzw. die Nutzungsmöglichkeiten der Cloud-Services erheblich zu beeinträchtigen, kann es sich aber durchaus lohnen, z.B. das Schlüsselmanagement durch das Spital selbst in Betracht zu ziehen.

Die vorstehend skizzierten Massnahmen (Verteidigungskaskade und weitere Massnahmen) führen in ihrer Gesamtheit erfahrungsgemäss zu einem faktisch sehr weitgehenden Schutz vor ausländischen Behördenzugriffen.

US CLOUD Act: Das Spital muss die Aufgabe der Eidgenossenschaft nicht lösen

Die digitale Welt stellt uns vor neue Herausforderungen. Wenn die Schweiz ihren Strafverfolgungsanspruch durchsetzen will, kann dies mit dem Gestaltungsanspruch anderer Staaten im Konflikt stehen (dasselbe gilt auch umgekehrt). Innerstaatliche Interessen des einen Staats können Zugriff auf Daten bedingen, die in der territorialen Hoheit eines anderen Staats liegen. Die Eidgenossenschaft sollte sich dem Thema annehmen; diesen internationalen Konflikt muss ein Spital aber nicht lösen. Das Spital muss demgegenüber nur (aber immerhin) den eigenen Betrieb im Einklang mit dem geltenden Recht organisieren. Dazu gehört, dass es das Arztgeheimnis schützen muss. Der US CLOUD Act ist hier jedoch kein Hindernis.

Vorbehalt 7: «Die Cloud steht mit der Datensouveränität im Widerspruch.»

«Gesundheitsdaten müssen in der Schweiz gespeichert werden und dürfen nicht international übermittelt werden.»

Antwort: Der Vorbehalt ist unbegründet. Datensouveränität ist eine Handlungsaufforderung an die Eidgenossenschaft, aber nicht Schranke für die Gesundheitsinstitution. Diese muss sich notwendiger-, aber auch ausreichenderweise an das geltende Recht der Schweiz halten.

Im Zuge der Digitalisierung fokussieren sich die Bemühungen um Souveränität – die Rückgewinnung der Kontrolle, die viele Nationalstaaten in vergangener Zeit zunehmend verlieren – vermehrt auf die vernetzte Wirtschaft. Datensouveränität als wichtiger Teilaspekt der Digitalen Souveränität formuliert, was im Zusammenhang mit Daten zu tun ist, um den Staat souverän werden zu lassen. Datensouveränität meint im Hinblick auf die Souveränitätsdiskussion die Verengung des Blicks auf alle Fragen zu Daten.

Datensouveränität ist eine Aufgabenstellung, der sich die Eidgenossenschaft annehmen muss. Sie muss dazu im zwischenstaatlichen Bereich Massnahmen treffen. Das kann zu besonderen Formen von Staatsverträgen führen, wobei die zentralen Forderungen aus schweizerischer Sicht – Garantieverantwortung und Ansatzpunkte, wie der zwischenstaatliche Handel im digitalen, grenzüberschreitenden Verkehr verbessert werden kann – in den Vordergrund zu stellen wären. Ein zentraler Aspekt der Garantieverantwortung besteht darin, den Zugang zum Recht zu sichern.

Unternehmen wie Gesundheitsinstitutionen müssen sich an das geltende Recht halten. Soweit dieses die Kernelemente der Garantieverantwortung abbildet, wird die Gesundheitsinstitution somit auch Aspekte der Datensouveränität in ihre Projektziele integrieren.

Mehr als das geltende Recht muss ein Spital aber nicht einhalten. Aus der Datensouveränität bzw. digitalen Souveränität ergeben sich für die Gesundheitsinstitution keine über das geltende Recht hinausgehenden Handlungs- oder Unterlassungspflichten.

Diese Kompetenzabgrenzung gilt in demselben Mass wie für private Gesundheitsinstitutionen auch für öffentlich-rechtliche Spitäler oder andere Gesundheitsinstitutionen der öffentlichen Hand, wie ein kürzliches für die Stadt Zürich erstelltes Rechtsgutachten ergeben hat.[28]

Die praktische Erfahrung zeigt, dass Institutionen im Gesundheitswesen (ebenso wie solche im Finanzwesen und in der öffentlichen Hand) sehr oft aus guten Gründen mehr erreichen wollen, als was das Gesetz verlangt. Sie möchten ihren Betrieb langfristig sichern. Die Informatikabteilungen solcher Institutionen widmen der Kontinuitätsplanung zu Recht viel Aufmerksamkeit. Motivation dafür ist aber nicht das Recht und auch nicht die Souveränitätsdebatte, sondern ganz einfach, was eine gute und umsichtige Unternehmensführung gebietet.

Fazit: Was bleibt von den Vorbehalten? Nachdem hier die wichtigsten Vorbehalte gegen die Cloud als solche im Bereich des Gesundheitswesens erörtert wurden, wird klar: Die Skepsis gegenüber der Cloud lässt sich nicht sachlich begründen. Man sollte den Fokus verlegen und die internen Energien darauf verwenden, wie man sich und v.a. die Patientinnen *mit* der Cloud optimal schützt.

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

IV ANHÄNGE

Zu den Elementen der Risikoanalyse

1. Eine künftige Gefahr kann nur mit Risikoaussagen beschrieben werden
Wenn wir wüssten, was die Zukunft bringt, wären auch Gesundheitsdaten auf elektronischen Systemen einfacher zu verwalten. So ist es aber nicht. Somit muss die Gesundheitsinstitution eine Prognose über die Zukunft aufstellen und prüfen, wie risikobehaftet die Verwaltung eines bestimmten Systems im konkreten Kontext ist. Dass der Entscheid «Cloud» oder «Nicht-Cloud» nicht per se mehr oder weniger Risiken nach sich zieht, liegt auf der Hand. Jeder Systementscheid verlangt eine gesonderte Risikobetrachtung. Einen Wechsel in ein System mit grösserer Sicherheit nicht zu unternehmen, birgt ebenso Risiken wie der Entscheid, einen Wechsel vorzunehmen und im neuen System (ebenfalls) Risiken anzutreffen.

Risikoaussagen sollten wie folgt gemacht werden:
- Der SOLL-Zustand ist zu beschreiben
- Für den SOLL-Zustand sollten mögliche Gefahren identifiziert werden
- Jede der identifizierten Gefahren sollte in Bezug auf die Wahrscheinlichkeit ihres Eintretens bewertet werden (Verortung nach Eintretenswahrscheinlichkeit, oft als **Probability** bezeichnet)
- Jede der identifizierten Gefahren sollte weiter in Bezug auf das Schädigungspotential bewertet werden (Verortung nach Schädigungspotential, oft als **Impact** bezeichnet)

2. Risikoaussagen als Synthese aus Probability und Impact
Die Kombination von Probability und Impact lässt dann eine Risikoaussage zu.

Eine Befürchtung, die nicht sehr wahrscheinlich eintritt und, wenn doch, wenig Schaden anrichtet, ist ein **kleines Risiko**.

Umgekehrt ist eine mit grosser Sicherheit eintretende Gefahr, die, wenn sie eintritt, jeweils auch grossen Schaden anrichtet, ein **grosses Risiko** (das Durchqueren eines Lawinenhangs von mehr als 30° Neigung nach Niederschlag birgt eine grosse Gefahr für Leib und Leben, und es ist sehr gut möglich, dass sich eine Lawine löst, wenn man den Hang durchquert).

Ein Ereignis mit potenziell grossem Schädigungspotential, das aber kaum je eintritt (Meteoriteneinschlag), wird anders bewertet **(kleines Risiko)** als ein Ereignis mit mittelmässigem Schädigungspotential, dessen Eintreten sehr wahrscheinlich ist **(mittleres Risiko)**.

3. Verdeutlichung an einem Beispiel (Information über die Blutgruppe)
Ob ein Schädigungspotential vorliegt und wie es sich realisiert, hängt vom **Kontext** ab. Was hier wichtig ist: Die Art der Information ist nicht notwendigerweise massgebend. Einen Automatismus in Bezug auf Risikoaussagen gibt es diesbezüglich nicht. Dies gilt ungeachtet der Tatsache, dass es im Gesundheitswesen um besonders schützenswerte Personendaten geht. Mit anderen Worten: Es gibt keine Abkürzungen, um zu einer adäquaten Risikobewertung zu gelangen. Man muss sich die Arbeit machen und ein Risiko konkret bewerten. Die Ausführungen in diesem Anhang sollen dies verdeutlichen.

Die abstrakte Information, dass eine unbestimmte Anzahl Menschen die «Blutgruppe 0» hat, ist eine anonyme Information (das Datenschutzrecht kommt nicht zur Anwendung; **Szenario 01**). Berichtet eine Ärztin, dass sie in ihrer Laufbahn von seither 35 Jahren mittlerweile 8'000 Patientinnen mit Blutgruppe 0 behandelt hat **(Szenario 02)**, äussert sie aggregierte Information – die Aussage ist statistischer Art und beruht auf echten Personendaten, aber Bezüge zu echten Personen sind nicht mehr erkennbar. Eine Gefährdung ist im ersten Fall (anonyme Information, die in einem Lehrbuch stehen könnte) objektiv ausgeschlossen. Im zweiten Fall entsteht eine gewisse (minimale) Gefährdung allenfalls dann, wenn auf Basis der Angabe eine Untersuchung gegen die Ärztin geführt würde, in deren Rahmen der Beweis, dass sie eine so hohe Anzahl von solchen Patientinnen betreut hat, geprüft wird. Ungeachtet dessen: Das Risiko ist in beiden Fällen sehr gering.

Ist die Information «Blutgruppe 0» jedoch mit einer Person verknüpft und damit individualisiert, muss man weitere Szenarien unterscheiden, um das Risiko zu beschreiben, was Folgendes zeigen soll:

• **Szenario 03:** Jemand berichtet an einer Party im Zwiegespräch beiläufig, dass er auch Blutgruppe 0 habe. Die Information ist individualisiert. Besondere Massnahmen zum Schutz der Information gibt es nicht. Die Information geht beim Gesprächspartner aber bald vergessen; sie interessiert ihn nicht. Man kann kaum ein Risiko erkennen. Selbst wenn statt der Blutgruppe eine Information über eine bestehende, unheilbare Krankheit ausgetauscht worden wäre: Man könnte von geringer Gefährdung ausgehen.

• **Szenario 04:** Jemand speichert seine Blutgruppeninformation im elektronischen Patientendossier. Es geht also um die Aussage «Ich habe die Blutgruppe 0». Es gibt in Verordnungen vorgeschriebene Schutzmassnahmen. Die betroffene Person darf eine sehr hohe Erwartung an die technische Sicherheit und den Schutz ihrer Daten haben.

• **Szenario 05:** Die Arbeitgeberin stand an der Party (Szenario 03) zufällig am Nebentisch und hat die Information mitgehört. Vielleicht leitet sie daraus etwas ab. Ob Blutgruppenwerte im konkreten Kontext ein Schädigungspotential haben? Allenfalls nicht. Würde es sich stattdessen um eine Angabe zu einer unheilbaren Krankheit handeln, die normalerweise in Kürze Arbeitsunfähigkeit von mehreren Monaten bis Jahren nach sich zieht, erkennt man: Anders als in Szenario 03 ändert sich die Risikobewertung für Szenario 05, wenn sich die Art der Information ändert. In Szenario 03 gab es trotz veränderter Situation keine signifikant andere Risikobewertung, nun schon; denn die Arbeitgeberin könnte ein Interesse haben, das Arbeitsverhältnis zu beenden. Man sieht: Der besondere Kontext verändert die Risikobewertung. Die Information per se hat die Risikosituation demgegenüber nicht verändert.

Resultierende Aussage: Nur weil besonders schützenswerte Personendaten bearbeitet werden, resultiert kein maximaler «Ausschlag» auf der Prüfskala (Impact bzw. Probability). Es wäre nicht haltbar zu sagen, dass bei Gesundheitsdaten stets ein Höchstrisiko vorliegt. Es ist nicht der Datensatz (die Information), der zur Risikobewertung führt, sondern der **Kontext**.

Nachdem die Bedeutung von Kontext herausgeschält wurde, soll eine weitere «Steigerungsform» durchgesprochen werden. In den folgenden Beispielen ist «echtes Blut» Teil der Abläufe, und nicht «nur» Information darüber:

• **Szenario 06:** Ein Kind spielt Fussball. Während des Spiels trifft ein Ball das Kind am Kopf. Es tritt Nasenbluten auf. Das Kind wirft das blutige Taschentuch in den Mülleimer. Die Müllabfuhr leert den Eimer tags darauf. Es liegt auf der Hand: Es handelt sich um eine Alltagssituation. Obwohl eine Blutprobe im Mülleimer lag und obwohl man daraus Angaben über die Blutgruppe hätte ableiten können, liegt ein sehr geringes Risiko vor, dass die Blutgruppeninformation tatsächlich auf diesem Weg erhoben (oder gar in der Folge missbraucht) wird. Und wenn doch, ist sehr diffus, welche Gefahr sich daraus ableiten würde. Die Bezüge zum Kind sind kaum sichtbar. Es müsste jemand mit sehr hoher krimineller Energie bereits hinter dem Kind her sein. Jedenfalls aus heutiger Perspektive in der Schweiz darf man sagen: Es ist nicht unsere Erfahrungswelt, dass so viel kriminelle Energie an jeder Ecke lauert. Es liegt ein geringes Schädigungspotential bei geringer Eintretenswahrscheinlichkeit vor.

• **Szenario 07:** Ein potenzieller Täter wird einer schweren Straftat bezichtigt (z.B. Gewaltdelikt). Den Ermittlungsbehörden fehlt ein Nachweis, um den Täter überführen zu können. Anhand der Information über die Blutgruppe könnte der Täter überführt werden. Ein Kind des Beschuldigten hat beim Onlinedienst 23&me eine DNA-Probe hinterlegt. Die Ermittlungsbehörden stossen auf diese Information und können aus den Angaben über das Kind auf die Blutgruppe des Beschuldigten schliessen[29]. Dies ermöglicht, den Täter anschliessend der Straftat zu überführen. Es liegt aus Sicht der betroffenen Person (Täter) ein erhebliches Schädigungspotential vor. Zunächst (wie sein Kind sich bei 23&me registriert hatte) musste man von geringer Eintretenswahrscheinlichkeit sprechen. Mit Blick auf die Energie der Strafverfolgungsbehörden im aktuellen Fall, hat sich das Risiko der Eintretenswahrscheinlichkeit verändert. Die Strafverfolgungsbehörden hatten die Schwere des Falls zum Anlass genommen, erhebliche Abklärungen zu treffen (was sie normalerweise nicht tun). Die Bereitschaft, so viel Energie auf den Fall zu verwenden, hat die Risikoanalyse erheblich verändert. Das Beispiel zeigt: Es ist abermals der Kontext und nicht die Information per se, welche die Risikoanalyse konkret beeinflusst.

4. Was bleibt

Was bedeutet dies nun konkret für eine Gesundheitsinstitution? Eines jedenfalls ist klar: Der Umstand, dass potenziell jeweils der maximale Nachteil denkmöglich ist, darf nicht zum Schluss führen, dass zwingend ein unkontrollierbares oder hohes Risiko vorliege. Dies gilt auch dann, wenn es um die Verwaltung von Gesundheitsdaten geht. Wenn man von einem unkontrollierbaren Risiko ausginge und so den Weg in die Cloud als unzulässig ansähe, würde man den **Kontext ausblenden**. Dieser ist aber zur Bewertung des Risikos entscheidend. Die Verbotshaltung ist unzulässig. Es gilt der risikobasierte Ansatz, für den alle Umstände (auch diejenigen, die für einen Cloud-Einsatz sprechen; wie z.B. massiv höhere Verarbeitungskapazitäten, grössere Ausfallsicherheit oder umfassendere Cybersicherheit auf dem immer neusten Stand etc.) im gegebenen Kontext zu würdigen sind.

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

Verzeichnis gesetzlicher Grundlagen

1. Datenschutz
- Datenschutzrecht des Bundes: DSG, VDSG (SR 235.1; SR 235.11)
- Datenschutzrecht der Kantone: z.B. IDG-ZG, IDG-BS und Verordnungen zu den IDG
- Europäisches und internationales Datenschutzrecht, je nach Kontext: z.B. EU-DSGVO

2. Strafrecht
- Amtsgeheimnis: Art. 320 StGB (SR 311.0)
- Arztgeheimnis: Art. 321 StGB (SR 311.0)
- Art. 62 nDSG (SR 235.1)

3. Gesundheitsrechtliche Spezialerlasse des Bundes
- Humanforschungsgesetz (HFG), Humanforschungsverordnung (HFV), (SR 810.30; SR 810.301)
- Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG), Verordnung über genetische Untersuchungen beim Menschen (GUMV) (SR 810.12; SR 810.122.1)
- Heilmittelgesetz (HMG), Medizinprodukteverordnung (MepV) (SR 812.21; SR 812.213)
- Verordnung über klinische Versuche (KlinV) (SR 810.305)
- Medizinprodukteverordnung (MepV) (SR 812.213)
- Verordnung über In-vitro-Diagnostika (IvDV) (SR 812.219)
- Verordnung über klinische Versuche mit Medizinprodukten (KlinV-Mep) (SR 810.306)
- Bundesgesetz über das elektronische Patientendossier (EPDG) (SR 816.1)
- Ausführungsverordnungen zum EPDG (SR 816.11; SR 816.111)

4. Gesundheitsrechtliche Spezialerlasse der Kantone
- Kantonale Spitalgesetze; z.B. Spitalgesetz Kt. BL, SpiG Kt. AG
- Kantonale Gesundheitsgesetze; z.B. GesG Kt. ZH, LS Kt. GE
- Kantonale Patientengesetze; z.B. Patientinnen -und Patientengesetz Kt. ZH
- Kantonale Leistungsaufträge der Spitäler

5. Sozialversicherungsgesetze des Bundes
- Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) (SR 830.1)
- Bundesgesetz über die Krankenversicherung (KVG) (SR 832.10)
- Bundesgesetz über die Unfallversicherung (UVG) (SR 832.20)

LAUX
LAWYERS AG
ZURICH | BASEL

BÜRO ZÜRICH
A Schiffbaustrasse 10
Postfach · CH 8031 Zürich
T +41 44 880 2424
W www.lauxlawyers.ch

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