Im 19. Jahrhundert ist die Entwicklung der physikalischen Diagnostik nicht ohne Widerstand und Ängste seitens der Ärztinnen und Ärzte vonstattengegangen. Vielleicht stehen wir mit den Entwicklungen der Digitalisierung in der Medizin wie dem Einsatz von Cloud Computing an einer ähnlichen Schwelle. Nicht immer ist uns dabei bewusst, wo unsere Daten gespeichert werden und wer diese bearbeitet. Ärztinnen und Ärzte unterstehen auch in der digitalen Welt dem Berufsgeheimnis und sind damit für die Einhaltung des gesetzlichen Datenschutzes verantwortlich. Das im vorliegenden Artikel enthaltene Merkblatt und die Praxisbeispiele sind eine ausgezeichnete Hilfestellung für alle, die ihre Daten in die Cloud auslagern möchten. Als weiteres Hilfsmittel bietet Ihnen, liebe Kolleginnen und Kollegen, die FMH beispielsweise den Rahmenvertrag für Clouddienste, dessen Gebrauch ich Ihnen ans Herz legen möchte. Sie finden ihn auf unserer Website.

Dr. med. Alexander Zimmer, Mitglied des FMH-Zentralvorstandes, Departementsverantwortlicher Digitalisierung/eHealth

Clouddienste im Gesundheitsalltag

Erik Dinkel[a], Philip Gut[b]

Universitätsspital Zürich: [a] lic. phil. I / Master of Arts UZH, Chief Information Security Officer; [b] Rechtsanwalt, Stv. Leiter Rechtsdienst

Cloud Computing ist aus dem Alltag von Spitälern und Arztpraxen nicht mehr wegzudenken. Der Anwendungsbereich reicht vom elektronischen Patientendossier bis hin zur Überwachung von Implantaten. Dabei stellen sich schnell Fragen zur Informationssicherheit und zu den Nutzungsbedingungen.

Spitäler, Arztpraxen und weitere Einrichtungen im Gesundheitswesen sind mit Entscheidungen zur Auslagerung von Informatikdienstleistungen in die Cloud konfrontiert. Solche Clouddienste können einen grossen Nutzen für alle Involvierten haben. Gleichzeitig birgt die zunehmende technische Abhängigkeit auch Risiken für die Sicherheit der Patientendaten. In diesem Artikel wird ein Merkblatt vorgestellt, das eine erste Orientierung für die Umsetzung von Cloudvorhaben ermöglichen soll.

Ein wolkiger Begriff kurz erklärt

Hinter der *Cloud* steht eine bodenständige technische Infrastruktur: Der Speicherplatz (Hosting), das Betriebssystem und die Software eines externen Anbieters werden genutzt. Dazu müssen Daten über das Internet transferiert werden. Abhängig davon, was aus der Cloud bezogen wird, spricht man von Infrastruktur als Service (IaaS), Plattform als Service (PaaS) oder Software als Service (SaaS). Bei Letzterer wird die Informatikdienstleistung komplett ausgelagert. Die Software und die Daten, die darin verarbeitet werden, sind auf den Rechnern des Anbieters und damit vollständig in der Cloud. Die nachfolgenden Ausführungen fokussieren auf Software als Service, gelten aber auch für die anderen Formen der Cloudnutzung.

Orientierungshilfe in der Cloud

Viele Publikationen zeigen die rechtlichen Rahmenbedingungen auf, unter denen Clouddienste im medizinischen Alltag eingesetzt werden können. Allerdings bestehen noch unterschiedliche Anschauungen darüber, inwieweit das Berufsgeheimnis die Benutzung von Clouddiensten zulässt. Denn Cloud Computing stellt immer eine Bearbeitung von Daten durch einen externen Anbieter dar. Sie erfolgt im Auftrag der auslagernden Spitäler oder Arztpraxen, die für die Daten verantwortlich bleiben. Das kann zu Verunsicherung führen.

Das Cloudmerkblatt basiert auf dem Gesetz über die Information und den Datenschutz des Kantons Zürich vom 12. Februar 2007 samt Verordnungsrecht [1]. Die dortigen Grundsätze entsprechen der Regelung auf Bundesebene bzw. dem Bundesgesetz über den Datenschutz vom 19. Juni 1992 [2].

Das Merkblatt ist in die Spalten «Fragestellungen» und «zu erfüllende Anforderungen» aufgeteilt. Es liest sich von links nach rechts mit Fragen zu den datenschutzrechtlichen und den informationssicherheitstechnischen Anforderungen.

Fragestellungen

Als Erstes muss ganz links die Frage beantwortet werden, was für Daten bearbeitet werden und wie schutzwürdig diese sind. Bei Patientendaten sind nicht nur die datenschutzrechtlichen Bestimmungen, sondern

Nutzung von Cloud-Lösungen[1] - Datenschutz-Anforderungen (1/2)

1) Lösung, bei der Speicherplatz (Hosting), Betriebssystem, Runtime und Software eines Anbieters im Auftragsverhältnis genutzt und hierzu Daten über das Internet transferiert werden (Software as a Service) oder anderweitige Onlinedienste ohne End-to-End Verschlüsslung.
2) Daten können nur noch mit unverhältnismässigem Aufwand durch Dritte einer bestimmten Person zugeordnet werden und der Identifikationsschlüssel muss in Besitz des Auftraggebers sein. Sofern dies gegeben ist, können die Daten gegenüber dem Empfänger/Auftragnehmer als anonymisiert betrachtet werden.
3) Im Unterschied zur Pseudonymisierung ist eine Anonymisierung irreversibel; d.h. der Rückschluss auf eine Person ist niemals möglich.

Sofern Daten unter das Amtsgeheimnis fallen, ist eine Entbindung nötig.

Das Merkblatt «Nutzung von Cloud-Lösungen» kann als separates PDF heruntergeladen werden unter saez.ch → Ausgabe 36/2021 (© USZ).

auch das Berufsgeheimnis zu beachten. Als Zweites stellt sich die Frage, ob eine Person identifizierbar ist. Sofern das möglich ist, gelten die höchsten Schutzanforderungen.

Sind die Informationen anonymisiert, können die Daten ohne hohe Hürden ausgelagert werden. Dazwischen können die Daten aber auch pseudonymisiert sein. Das heisst, eine individuelle Person kann dann nur anhand eines Schlüssels oder aus den Umständen identifiziert werden. Sofern sich der Identifikationsschlüssel ausschliesslich im Besitz des Spitals oder der Arztpraxis befindet und eine Identifikation aus den Umständen nicht möglich ist, sind die Daten ausreichend pseudonymisiert und können aus Sicht des Anbieters als anonymisiert betrachtet und damit in der Cloud bearbeitet werden. Im Unterschied zur Pseudonymisierung ist die Anonymisierung irreversibel, weil z.B. niemand einen Schlüssel für die Re-Identifikation besitzt. Wenn personenbezogene Daten vollständig anonymisiert sind, gelten sie nicht mehr als Personendaten.

Praxisbeispiel 1: Rechnungsstellung und Inkasso mit Clouddienst in der Schweiz

- **Ausgangslage:** Ein Spital möchte für die Rechnungsstellung und das Inkasso einen Clouddienst in der Schweiz verwenden.
- **Merkblatt (von links nach rechts):** Die Rechnungsstellung an die Patientinnen und Patienten für die medizinische Behandlung und das Inkasso erfordert, dass mit dem Clouddienst Patientendaten in identifizierter Form bearbeitet werden können. Die Bearbeitung erfolgt in der Schweiz.
- **Spalte «zu erfüllende Anforderungen»:** Es zeigt sich, dass ein Vertrag zwischen Spital und Anbieter für die Auslagerung nötig ist. Der Vertrag muss sicherstellen, dass auch der Anbieter die datenschutzrechtlichen und informationssicherheitstechnischen Vorgaben an das Spital einhält. Der Anbieter muss insbesondere weisungsgebunden sein, die Patientendaten vertraulich behandeln und die Grundsätze des Datenschutzes wie die Zweckbindung sowie Verhältnismässigkeit einhalten. Klar ist, dass der Anbieter auch sorgfältig ausgesucht werden muss. Denn das Spital bleibt trotz Auslagerung stets verantwortlich für die ausgelagerten Daten. Eine Zustimmung der betroffenen Personen ist hingegen nicht erforderlich.

Nutzung von Cloud-Lösungen[1] - Datenschutz-Anforderungen (2/2)

Rechtliche Anforderungen (zwingend)

1

Eine **vertragliche Grundlage** für die Bearbeitung von personenbezogenen Daten muss vorhanden sein (Mindestinhalt AGB des Kt. ZH). Der Anbieter muss dabei sorgfältig ausgesucht (seriöser, verlässlicher Anbieter) werden und gegenüber dem Auftraggeber weisungsgebunden sein. Rechte und Pflichten des Anbieters müssen geregelt sein; Mitarbeitende des Anbieters müssen vertraglich auf die Geltung der ärztlichen Schweigepflicht hingewiesen werden. In hiervon abweichenden vertraglichen Grundlagen ist die nachweisbare explizite Einwilligung der betroffenen Person erforderlich.
Zweckbindung muss erfüllt sein; d.h. die betroffene Person hat dem Auftraggeber die Daten zu diesem Zweck anvertraut und der Anbieter wird verpflichtet, die Daten ausschliesslich zu diesem Zweck zu bearbeiten.
Verhältnismässigkeit muss gegeben sein: d.h. es dürfen nur Daten weitergegeben werden, welche auch effektiv für die Bearbeitung benötigt werden. Werden z.B. Vor- und Nachname für die Bearbeitung nicht benötigt, dürfen diese auch nicht weitergegeben werden.

2

Bei der Bearbeitung von Personendaten muss eine **Datenschutz-Folgenabschätzung** erstellt werden. Bei besonderen Risiken (z.B. bei einer grossen Menge von Personendaten oder bei der Nutzung neuer Technologien etc.) ist zudem eine die **Vorabkontrolle** durch die kantonale Datenschutzbeauftragte erforderlich.

3

Eine nachweisbare Information und **explizite Einwilligung** der betroffenen Person ist zwingend erforderlich. Gibt eine Patientin/ein Patient keine Einwilligung, muss nach Möglichkeit für die Behandlung eine alternative Lösung zur Verfügung stehen, sofern dies gemäss kantonalem Leistungsauftrag erforderlich ist. Alternativ zur schriftlichen Zustimmung des Patienten oder bei Amtsgeheimnissen kann über den Rechtsdienst eine Bewilligung durch die Gesundheitsdirektion des Kt. ZH eingeholt werden.

4

Der **Schutz im Empfängerstaat** muss mindestens jenem der Schweiz entsprechen (vgl. Liste EDÖB). Bei Anbietern in Empfängerstaaten, welche nicht auf der Liste des EDÖB geführt sind oder welche Sitz in den USA haben, muss eine Risikobeurteilung vorgenommen und vertragliche Äquivalenz mit dem schweizerischen Datenschutzniveau hergestellt werden.

5

Auch bei nicht personenbezogenen Daten muss eine **vertragliche Grundlage** für die Bearbeitung der Daten vorhanden sein. Der Anbieter muss dabei sorgfältig ausgesucht werden. Zweckbindung und Verhältnismässigkeit muss auch hier gewahrt sein.

Technische Anforderungen (risikobasiert)

A

Transfer der Daten muss **zwingend verschlüsselt** erfolgen (minimal mittels Verschlüsselungsprotokoll wie aktuelle Version TLS, IPsec, VPN).

B

Anbieter muss die Daten **gemäss aktuellem Stand der Technik schützen**. Dabei sind insbesondere folgende Punkte zu beachten:

- Der Anbieter ist gemäss einem gängigen Standard (z.B. ISO 27001) zertifiziert.
- Prüfresultate (Zertifizierungen) müssen dem Auftraggeber bei Verlangen zur Verfügung gestellt werden.
- Der Anbieter muss über ein Informationssicherheitskonzept verfügen und den Auftraggeber bei Nachfrage über dessen Stand informieren.
- Daten sind vor Ort kryptographisch verschlüsselt.
- Der Anbieter verfügt über Prozesse, mit welchen sichergestellt wird, dass der Verlust von Daten und/oder der Missbrauch dem Auftraggeber zeitnah gemeldet wird.
- Der Anbieter verfügt über eine Liste aller Nutzer, welche auf Daten zugreifen können inkl. Administratoren.
- Zugriffe sind in Log nachvollziehbar.
- Zugriffe entsprechen dem Need-to-Know-Prinzip und wird regelmässig überprüft.
- Der Auftraggeber hat das Recht, bei Bedarf einen Audit des Anbieters durchzuführen.

C

Der für die Nutzung der Cloud verantwortliche Bereich, muss vor Nutzung der Cloud ein angemessenes **Risk Assessment** durchführen. Dabei geht es darum, Risiken zu identifizieren und diese anhand ihrer Eintretenswahrscheinlichkeit und ihrer Auswirkungen zu beurteilen sowie geeignete Massnahmen zur Minderung der Risiken zu definieren.
Insbesondere stellen sich folgende Fragen:

- Ist eine **Strong Authentication** bzw. 2 Faktor Authentisierung eingerichtet?
- Wie wird der **Zugriff über private Geräte** verhindert? Kann sich ein Nutzer auch über ein privates Gerät Zugriff auf die Cloud verschaffen? Kann **Single-Sign-On** eingerichtet werden?
- Wie ist der **Zugriff von Extern durch Dritte** auf die Cloud geregelt (z.B. externe Forscher, Ärzte anderer Spitäler etc.)?
- Wie wird verhindert, dass Mitarbeitende in einer neuen Funktion oder **nach Austritt weiter Zugriff** auf die Daten haben?
- Ist die Datenübertragung **verschlüsselt** (z.B. mittels https)?
- Was geschieht, wenn das System **nicht zur Verfügung steht**? Bestehen alternative Betriebsmöglichkeiten?

D

Sofern die Daten nicht weiter benötigt werden und keine gesetzliche Aufbewahrungspflicht besteht, sind diese **nach Gebrauch zu vernichten**.

Als Letztes stellt sich die Frage, ob die Daten in der Schweiz oder im Ausland bearbeitet werden; mit anderen Worten, ob die Cloud in der Schweiz oder im Ausland betrieben wird. Bei Bearbeitungen in der Schweiz greift das Schweizer Recht inklusive Berufsgeheimnis, womit die Daten auch bei einer Auslagerung an einen externen Anbieter mit gleichem juristischem Niveau geschützt sind. Erfolgt ein Datentransfer ins Ausland, müssen allenfalls zusätzliche Vorkehrungen zur Gewährleistung eines äquivalenten Schutzes getroffen werden.

Anforderungen

Durch die Beantwortung der Fragen zur Datenbearbeitung ergeben sich unter «zu erfüllende Anforderungen» in der rechten Spalte des Merkblatts 16 verschiedene Lösungen. Sie zeigen in vereinfachter Form, welche rechtlichen und informationssicherheitstechnischen Anforderungen bei der Umsetzung berücksichtigt werden müssen. Auf der zweiten Seite des Merkblatts sind sie im Detail erläutert. Die Unterteilung der Antworten in datenschutzrechtliche und informationssicherheitstechnische Aspekte gibt zu-

Praxisbeispiel 2: Patientenbefragung mit einem Clouddienst im Ausland

- **Ausgangslage:** Nach einem Spitalaufenthalt werden Patientinnen und Patienten zu ihrer Zufriedenheit befragt. Dazu erhalten sie über einen ausländischen Clouddienst eine E-Mail, die sie zu einer Online-Umfrage führt. Der Clouddienst wertet die Umfrage aus und informiert das Spital über die Ergebnisse.
- **Merkblatt (von links nach rechts):** Der Clouddienst benötigt zur Kontaktierung der Personen deren Namen und die E-Mail-Adresse. Die Daten werden im Zusammenhang mit der Behandlung im Spital bearbeitet. Es handelt sich folglich um Patientendaten, welche die Identifikation einer Person ermöglichen. Die Daten werden im Ausland bearbeitet.
- **Spalte «zu erfüllende Anforderungen»:** Es muss ein Vertrag vorliegen, mit dem das Spital seine Pflichten dem Clouddienst überbindet und mindestens ein äquivalentes Datenschutzniveau wie in der Schweiz gewährleistet. Hinzu kommt, dass die angeschriebenen Personen über die Bearbeitung ihrer Daten im Ausland informiert werden und ausdrücklich einwilligen müssen. Wichtig ist, dass die Einwilligung freiwillig erfolgt. Das bedeutet, dass eine Wahlfreiheit zwischen der Patientenumfrage mit dem Clouddienst im Ausland und einer Alternative wie z.B. der Abgabe von Fragebögen beim Austritt vorliegt. Neben den weiteren rechtlichen Voraussetzungen muss immer auch die Informationssicherheit gemäss der rechten Spalte «zu erfüllende Anforderungen/ technisch» gewährleistet sein.

Praxisbeispiel 3: Pseudonymisierte oder anonymisierte Patientenbefragung

- **Ausgangslage:** Die Patientenbefragung erfolgt direkt durch das Spital. Der Clouddienst unterstützt nur technisch. Die Patientinnen und Patienten werden nicht namentlich, sondern mit einer Laufnummer angeschrieben. Die Identifikation einzelner Personen ist nur über einen Identifikationsschlüssel möglich, den das Spital hält. Auch die E-Mail-Adressen der Personen bleiben im Spital.
- **Merkblatt (von links nach rechts):** Das Spital kann die Patientinnen und Patienten mit dem Schlüssel identifizieren. Es handelt sich somit um pseudonymisierte Patientendaten. Wird hingegen auch auf eine Laufnummer verzichtet, sind Umfrage und Daten anonym. Es handelt sich nicht mehr um personenbezogene Daten. Der Schutz durch das Berufsgeheimnis entfällt. Es ist in beiden Fällen unerheblich, ob die Daten in der Schweiz oder im Ausland bearbeitet werden. Die Einholung einer Patienteneinwilligung ist nicht erforderlich. Es reicht aus, in der E-Mail, welche durch das Spital verschickt wird, auf die externe Durchführung der Umfrage hinzuweisen. Auch hier müssen zusätzlich die informationssicherheitstechnischen Anforderungen beachtet werden.
- **Bei Registern/Überwachungssystemen:** Dasselbe gilt bei internationalen Registern und Überwachungssystemen von Vitaldaten (z.B. Herzschrittmacher, Blutzuckerspiegel, Augendruck), in welchen die darin geführten Daten nur über einen vom Spital gehaltenen Schlüssel den Personen zugeordnet werden können. Bei einer solchen Pseudonymisierung von Personendaten stellt sich allerdings immer die Frage, ob diese ausreichend stark ist. Es empfiehlt sich deshalb, bei Datenbearbeitungen im Ausland im Zweifelsfall mindestens zusammen mit der Information die implizite Zustimmung der Patientinnen und Patienten einzuholen.

dem Anhaltspunkte dafür, welche Fachpersonen nötigenfalls beigezogen werden können.

Wenn Daten in einer Cloud bearbeitet werden, braucht es einen Vertrag. Das ergibt sich aus der Spalte «zu erfüllende Anforderungen / **rechtlich**». Darin müssen dem externen Anbieter dieselben Pflichten auferlegt werden, die das Spital oder die Arztpraxis hat. Denn sie bleiben gegenüber den Patientinnen und Patienten verantwortlich. Allem voran muss der Anbieter verpflichtet werden, die Sicherheitsvorkehrungen einzuhalten und die anvertrauten Daten nur zum vereinbarten Zweck zu bearbeiten.

Kommen neue Technologien zum Einsatz oder wird eine besonders grosse Menge von besonders schützenswerten Personendaten bearbeitet, braucht es nach dem Gesetz über die Information und den Datenschutz des Kantons Zürich zudem eine Datenschutz-Folgenabschätzung sowie eine Vorabkontrolle durch die kantonalen Datenschutzbeauftragten.

Findet die Bearbeitung in einer Cloud im Ausland statt, ist das nur zulässig, wenn das Datenschutzniveau im Empfängerstaat mindestens dem der Schweiz entspricht. Ist das nicht der Fall, muss eine Absicherung über Datenschutzvertragsklauseln erfolgen, die von den Datenschutzbehörden genehmigt sind. Bei Datenbearbeitungen im Ausland kann die Rechtsdurchsetzung erschwert sein und es gelangt auch ausländisches Recht zur Anwendung. Es ist angesichts der Risiken ratsam, dass die Patientinnen und Patienten bei einer Bearbeitung ihrer identifizierbaren Daten im Ausland informiert werden und in eine solche Bearbeitung einwilligen.

Die bearbeiteten Daten müssen schliesslich gemäss der Spalte «zu erfüllende Anforderungen/**technisch**» nach dem aktuellen Stand der technischen Informationssicherheit geschützt sein. Dies bedeutet, dass die Daten bei der Übertragung und vor Ort z.B. durch Verschlüsslung und rollenbasierte Zugriffe angemessen geschützt werden.

Der hohe Nutzen von Clouddiensten ist unbestritten, denn sie ermöglichen eine Ressourcenoptimierung für Patientinnen und Patienten, Spitäler und Arztpraxen gleichermassen. Clouddienste ziehen bei allen Vorteilen aber auch Risiken und rechtliche Fragen nach sich, denen mit Hilfe des Cloudmerkblatts begegnet werden kann. So bleiben Cloudprojekte nicht «wolkig» und können auf den Boden gebracht werden.

Literatur
1 IDG; LS 170.4.
2 DSG; SR 235.1.

Philip Gut
Universitätsspital Zürich
Stab Spitaldirektion
Rämistrasse 100
CH-8091 Zürich
philip.gut2[at]usz.ch

Das Wichtigste in Kürze

- Immer mehr Spitäler und Arztpraxen lagern Informatikdienstleistungen an externe Clouddienste aus. Dabei stellen sich rechtliche Fragen zum Schutz der Patientendaten, für die das abgebildete Merkblatt eine Orientierungshilfe bietet.
- Das Merkblatt gibt Auskunft darüber, welche rechtlichen und technischen Anforderungen je nach Datenart und Verschlüsselungsform und bei der Datenverarbeitung im In- oder Ausland anfallen.

L'essentiel en bref

- De plus en plus d'hôpitaux et de cabinets médicaux externalisent leurs services informatiques à des services de cloud externes. Cela soulève des questions juridiques sur la protection des données des patients, pour lesquelles l'aide-mémoire présenté ici fournit des conseils.
- L'aide-mémoire informe sur les exigences juridiques et techniques qui s'appliquent selon le type de données et la forme de cryptage et selon si les données sont traitées dans le pays ou à l'étranger.