Nutzung von Cloud-Diensten im medizinischen Alltag

Cloud-Dienstleistungen sind praktisch und kostengünstig. Dabei geht leicht vergessen, dass mit den Vorteilen datenschutzrechtliche Probleme einhergehen, dass das Berufsgeheimnis einer Datenbearbeitung im Ausland entgegensteht und dass die Nutzungsbedingungen oft keine legale Möglichkeit für die Nutzung in der Patientenbetreuung ermöglichen.

Christian Peter

Die Cloud erfreut sich wachsender Beliebtheit, wobei sich die Nutzer nicht immer bewusst sind, dass sie überhaupt Cloud-Dienste in Anspruch nehmen. Neben icloud, SkyDrive und Diensten wie Dropbox oder Google Drive speichern auch Gratis-E-Mail-Anbieter (GMail oder Hotmail, resp. Outlook.com) die E-Mails ihrer Kundinnen und Kunden in einer Cloud ab, damit sie online abrufbar sind.

Cloud-Dienstleistungen sind kostengünstig oder sogar gratis und ermöglichen es zudem, dass grundsätzlich von überall her auf die Daten zugegriffen werden kann, und dies nicht nur an Arbeitsstationen, sondern auch mittels mobiler Geräte wie Smartphones oder Tablets. Dass einhergehend mit diesen Vorteilen auch datenschutzrechtliche Pro bleme bestehen können (A), dass das Berufsgeheimnis einer Datenbearbeitung im Ausland entgegensteht (B) und dass die zwingend zu akzeptierenden Nutzungsbedingungen oft keine legale Möglichkeit für die Nutzung in der Patientenbetreuung ermöglichen (C), geht leider oft vergessen.

Daher ist der Wahl des Service-Anbieters grösste Aufmerksamkeit zu schenken. Lediglich mit Anbietern, welche die Daten auf dem Computer des Benutzers vor dem Hochladen auf die Cloud verschlüsseln (client-side-encryption) [1], können die nachfolgenden Probleme umgangen werden.

A: Datenschutzrechtliche Schranken

Werden nicht anonymisierte Patientendaten in einem Cloud-Dienst gespeichert, stellt dies eine Datenbearbeitung durch Dritte dar [2]. Die Weitergabe von Personendaten zur Bearbeitung an Dritte ist aus Datenschutzsicht grundsätzlich zulässig, und zwar auch ohne Einwilligung des Patienten, sofern die Daten vom Dritten (Cloud-Anbieter) nur so bearbeitet werden, wie der Cloud-Nutzer es selber tun dürfte und keine gesetzliche (s. unten B) oder vertragliche Geheimhaltungspflicht die Bearbeitung durch einen Dritten verbietet. Der Cloud-Nutzer (Ärztin oder Arzt) muss sich jedoch vergewissern, dass der Cloud-Anbieter die Datensicherheit gewährleistet [3]. Somit

L'utilisation de services cloud dans le quotidien du médecin

Même si les services cloud, ou «nuage» en français, (par ex. icloud, SkyDrive et des services comme Dropbox, Google Drive mais aussi des fournisseurs de messagerie gratuits comme Gmail, Hotmail ou Outlook.com) connaissent une popularité croissante, il convient de faire preuve d'une grande prudence lors de leur utilisation. Les médecins doivent choisir leur fournisseur de services cloud avec le plus grand soin et s'assurer (au moyen d'un contrat écrit) que la sécurité des données est garantie. De plus, les données doivent être uniquement sauvegardées sur des serveurs situés dans des pays où les normes en matière de protection des données sont les mêmes qu'en Suisse et où aucune loi autorisant une transmission étendue des données n'existe. Le secret médical impose également une condition supplémentaire: aucune donnée de patient ne doit être sauvegardée à l'étranger sans le consentement de ce dernier (en d'autres termes, les serveurs doivent être situés en Suisse). En outre, en acceptant les conditions d'utilisation des services gratuits, on accorde généralement aux fournisseurs des droits sur les données, ce qui n'est pas compatible avec le secret médical. C'est la raison pour laquelle seuls les services conçus sur mesure ou qui cryptent les données directement sur l'ordinateur de l'utilisateur (client-side-encryption) avant de les transmettre au serveur (par ex. Wuala) sont autorisés dans le milieu médical. Les services gratuits mentionnés plus haut sont certes pratiques, mais ils ne sont pas adaptés pour les données de patients.

Korrespondenz:
Dr. iur. Christian Peter
HEP & Partner GmbH
Effingerstrasse 55
CH-3008 Bern

**christian.peter[at]
hep-partner.ch**

muss die Ärztin oder der Arzt den Cloud-Anbieter sorgfältig auswählen und sicherstellen, dass dieser die notwendigen Voraussetzungen für eine datenschutzkonforme Datenbearbeitung erfüllt und insbesondere die Datensicherheit gewährleisten kann. Weil das Mass der Sorgfalt von der Vertraulichkeit der zu bearbeitenden Daten abhängt, muss die Ärzteschaft ein hohes Mass an Sorgfalt an den Tag legen.

Vorkommnisse wie im Juni 2011, als bei Dropbox die Daten vieler Nutzer für 4 Stunden für alle User einsehbar waren [4] und andere bekannte Mängel [5], müssen zur Sorge Anlass geben.

Sicherheit kann der Nutzer nur erhalten, wenn er mit dem Cloud-Dienstanbieter eine individuelle Vereinbarung getroffen hat.

Ungenügende Datensicherheit

Die Ärztin oder der Arzt muss sich bei der Wahl ihres/seines Cloud-Dienstleistungsanbieters vergewissern, dass die Daten gegen folgende Risiken abgesichert sind: unbefugte oder zufällige Vernichtung, zufälliger Verlust, technische Fehler, Fälschung, Diebstahl oder widerrechtliche Verwendung, unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. Sicherheit hierüber kann der Nutzer nur erhalten, wenn er mit dem Cloud-Dienstanbieter eine individuelle, auf die eigenen Bedürfnisse abgestimmte Vereinbarung getroffen hat [6]. Denn die von den Cloud-Dienstanbietern selber verfassten Nutzungsbestimmungen, denen die Kundinnen und Kunden zwingend zustimmen müssen, werden diesen Anforderungen oft in keiner Weise gerecht (s. unten C). Ein Grossteil der Datensicherheitsrisiken kann jedoch minimiert werden, wenn die Daten zusätzlich ausserhalb der Cloud abgespeichert werden.

Ein weiteres datenschutzrechtliches Hindernis stellt der Umstand dar, dass die Cloud-Dienstanbieter die Daten regemässig im Ausland speichern.

Datenbekanntgabe ins Ausland

Mit den Cloud-Diensten werden dem Nutzer Speicherressourcen zur Verfügung gestellt. Leider ist bei vielen Angeboten nicht erkennbar, in welchem Land die Server stehen, auf denen die Daten gespeichert werden. Liegt ein Server ausserhalb der Schweiz, ist dies von zusätzlicher datenschutzrechtlicher Relevanz, weil Personendaten nur ins Ausland bekannt gegeben werden dürfen, wenn dieses Land über eine Gesetzgebung verfügt, die einen angemessenen Schutz gewährleistet. Einen solchen weisen die Mitgliedstaaten der EU und des EWR sowie Israel und Argentinien auf. Die USA fallen gemäss Eidgenössischem Datenschutz- und Öffentlichkeitsbeauftragtem (EDÖB) nur darunter, wenn der Cloud-Anbieter dem «Safe Harbor Framework» beigetreten ist [7]. Ohne einen solchen Beitritt oder einen angemessenen Datenschutz dürfen Personendaten ins Ausland nur bekanntgegeben werden, wenn die betroffene Person im konkreten Einzelfall eingewilligt hat.

Der Umstand, dass Cloud-Dienstleistungsanbieter regelmässig Sub-Provider z. B. bei Auslastung der eigenen Speicherkapazitäten zuziehen, stellt den Nutzer vor die praktischen Schwierigkeiten: Er weiss nicht, wo seine Daten gespeichert werden, ob sein Cloud-Dienstleistungsanbieter seinen Sub-Providern die nötigen rechtlichen Pflichten auferlegt hat und in welchem Land dieser Sub-Provider beheimatet ist.

Zudem könnten nationale Gesetze, wie z. B. der amerikanische «Patriot Act», der Justiz, Polizei oder Geheimdiensten weitreichende Möglichkeiten bieten, um die Herausgabe von Daten aus der Cloud zu verlangen und europäische Schutzbestimmungen zu umgehen. In den USA domizilierte Cloud-Anbieter können durch die dortigen Behörden sogar dazu gezwungen werden, Daten ihrer Kunden auszuliefern, und zwar auch solche Daten, die gar nicht in den USA gespeichert sind [8].

B: Schranken aufgrund des Berufsgeheimnisses

Neben dem Datenschutzrecht müssen Ärztinnen und Ärzte sowie ihre Hilfspersonen auch das Berufsgeheimnis beachten. Zwar ist heute die Auslagerung von Patientendaten an externe Informatikdienstleister wie Cloud-Anbieter gängige Praxis, weil damit die Ärztinnen und Ärzte ihrer eigentlichen (Arzt-)Tätigkeit nachgehen können. In dieser Funktion sind auch Schweizer Cloud-Dienstanbieter (sog. Swiss Cloud) Hilfspersonen, die auch dem Berufsgeheimnis unterstehen, und die Weitergabe von Patientendaten ist zulässig [9].

«Ohne Einwilligung stellt die Nutzung eines ausländischen Cloudangebots eine Berufsgeheimnisverletzung dar.»

Keine Hilfsperson ist jedoch ein Cloud-Dienstanbieter, der seine Cloud-Server im Ausland hat (wie z. B. Dropbox, icloud, SkyDrive oder web.de), weil in einem solchen Fall das Schweizer Strafrecht nicht zur Anwendung gelangt oder nicht gleich effektiv durchgesetzt werden kann. Daher bedingt eine Auslagerung von nicht anonymisierten Patientendaten in eine ausländische Cloud die Einwilligung der Patientinnen und Patienten. Dies auch dann, wenn ein angemessenes Datenschutzniveau besteht (wie z. B. beim Dienst «web.de» und in Deutschland). Die Patientin oder der Patient muss daher darüber infor-

In einer Cloud sind Patientendaten nur äusserst selten sicher aufbewahrt.

miert werden, welche Daten in eine ausländische Cloud ausgelagert werden, zu welchem Zweck, und sie resp. er muss darein einwilligen. Ohne Einwilligung stellt die Nutzung eines ausländischen Cloudangebots eine Berufsgeheimnisverletzung dar [10]. Unbedenklich ist die Auslagerung der Daten, wenn es sich um verschlüsselte und somit anonymisierte Daten handelt, die nicht dem Berufsgeheimnis unterstehen.

C: Bedenken aufgrund der Nutzungsbestimmungen

Auch wenn die Nutzungsbestimmungen von Gratis-Cloud-Diensten nur selten gelesen werden, bedeutet dies nicht, dass sie keine Wirkung entfalten. Sie bringen zudem zum Ausdruck, was der Anbieter mit den Daten alles machen will oder sogar macht.

Bei Google Drive räumt man Google (und ihren Partnern) das Recht ein, die abgespeicherten Inhalte weltweit zu verwenden, zu hosten, zu speichern, zu vervielfältigen, zu verändern, damit der genutzte Dienst verbessert wird oder neue entwickelt werden. Diese Rechtseinräumung bleibt auch dann bestehen, wenn die Dienste nicht mehr verwendet werden [11].

Mit icloud erklärt man sich einverstanden, dass Apple auf die Kontoinformationen und «ihre Inhalte zugreifen, diese nutzen, aufbewahren und/oder an Strafverfolgungsbehörden, andere Behörden und/oder sonstige Dritte weitergeben darf, wenn Apple der Meinung ist, dass dies vernünftigerweise erforderlich oder angemessen ist, ...» [12].

Und bei Dropbox wird den Kunden klargemacht, dass «die in der Dropbox gespeicherten Daten gegenüber Dritten offengelegt werden, wenn wir hinreichenden Grund zu der Annahme haben, dass diese Offenlegung erforderlich ist, um (a) einem Gesetz oder einer Vorschrift zu entsprechen oder einer bindenden rechtlichen Forderung nachzukommen, (b) eine Person vor Tod oder schwerer Körperverletzung zu schützen, (c) Betrug oder Missbrauch von Dropbox oder seinen Nutzern zu verhindern oder (d) die Schutzrechte von Dropbox zu schützen.»[13].

Durch solche sehr weitreichende und zum Teil auch unbestimmte Formulierungen in den Nutzungsbedingungen wird den Cloud-Anbietern ein weiter Spielraum für die Nutzung der Daten eingeräumt, die mit dem Berufsgeheimnis und den Pflichten der Ärztin oder des Arztes an die Datensicherheit nicht vereinbar sind.

Fazit

Die Nutzung von Cloud-Dienstleistungen ist im ärztlichen Bereich nur zulässig, wenn die Daten vor dem Hochladen auf dem Computer des Benutzers verschlüsselt werden und erst dann in die Cloud geladen werden (z. B. Wuala [14]) und die Datensicherheit gewährleistet ist oder wenn sichergestellt wird, dass der Cloud-Dienstanbieter die Daten so bearbeitet, wie der Arzt oder die Ärztin es selber tun dürfte, und die Daten in der Schweiz gespeichert werden. Diese Garantien hat man bei den wenigsten Cloud-Dienstleistungsanbietern.

Dropbox, Google Drive, icloud, Skydrive oder Gratis-E-Mail-Anbieter wie GMail oder Hotmail resp. Outlook.com können wertvolle Dienste leisten: Für Patientendaten sind sie jedoch nicht geeignet.

Referenzen

1 Vgl. auch Empfehlungen der FMH in: Rechtliche Grundlagen im medizinischen Alltag. S. 48.

2 Schwaninger D, Lattmann S. Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke. In: Jusletter. 11. März 2013.

3 Widmer U. Gesundheitsdaten in der Cloud in: Scharter P, Taeger J (Hrsg.)«D»A«CH» Security. 2011; S. 171.

4 Entschuldigung des Dropboxgründers Arash Ferdowsi: https://blog.dropbox.com/2011/06/yesterdays-authentication-bug/

5 www.welt.de/wirtschaft/webwelt/article106278350/Diese-Gefahren-lauern-beim-Cloud-Dienst-Dropbox.html

6 Siehe den Muster-Outsourcing-Vertrag des EDÖB.

7 www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de

8 www.heise.de/newsticker/meldung/Studie-US-Behoerden-koennen-umfangreich-auf-Cloud-Daten-zugreifen-1763750.html

9 Peter C. Die Zulässigkeit der Auslagerung der Bearbeitung der Patientendaten von Spitälern an externe Informatikdienstleister. In: Jusletter. 22. Juni 2009; Rz. 3.

10 Widmer U. Gesundheitsdaten in der Cloud. In: Scharter P, Taeger J (Hrsg.)«D»A«CH» Security 2011. S. 174.

11 www.google.com/policies/terms/

12 www.apple.com/legal/internet-services/icloud/de/terms.html

13 https://www.dropbox.com/dmca#privacy

14 www.wuala.com/de/about/