Nutzung medizinischer Schreibservices – eine datenschutzrechtliche Sicht

Ursula Uttinger, Michael Liebrenz

Im medizinischen Umfeld werden vermehrt administrative Aufgaben durch externe Dienstleister erbracht. Das Datenschutzgesetz kennt eine Datenbearbeitung durch Dritte – unter Berücksichtigung der allgemeinen Datenschutzgrundsätze. Doch nicht nur das Datenschutzgesetz ist zu beachten, denn im medizinischen Umfeld spielt die berufliche Schweigepflicht, die auch Hilfspersonen umfasst, eine wichtige Rolle. Bei einer klaren Regelung und Transparenz gegenüber den betroffenen Personen ist ein Outsourcing grundsätzlich möglich.

Einleitung

Das Schweizerische Gesundheitswesen nimmt gemessen an Qualität und Versorgungssicherheit, im internationalen Vergleich eine herausragende Stellung ein[1,2,3]. Dennoch sind die einzelnen Leistungserbringer, sei dies im Spital oder in der Praxis, zunehmend mit einem von finanziellen Überlegungen geprägten Umfeld konfrontiert [4], [5]Von der reinen medizinischen Qualität verschiebt sich der Fokus so auf Fragen der Wirtschaftlichkeit nicht nur von erbrachten Leistungen sondern auch von Planung, Organisation, Steuerung und Durchführung der Aktivitäten[6]. In der wirtschaftswissenschaftlichen Literatur wird im Bereich des Spitalwesens zunehmend eine Konzentration auf die Kernleistungen oder „Primär- und Sekundärprozesse“, d.h. all jene Leistungen, die dem „Geschäftszweck“, nämlich der Genesung des Patienten dienen (Diagnostik/Therapie), empfohlen[6]. Hingegen soll die Auslagerung von „Tertiärprozessen“ wie z.B. Betrieb, Instandhaltung, Unterhalt, Logistik, Catering, Konferenz und Veranstaltungsservice zumindest geprüft werden. Im kaufmännischen Bereich fallen unter diese Tertiärprozesse auch Bereiche wie ambulante und stationäre Leistungsabrechnung, Patientenadministration und Sekretariatsdienste[6].

In Bezug auf den letztgenannten Bereich ist über den Verlauf der letzten Jahre eine zunehmende Bereitschaft zu erkennen gewesen, vor allen Dingen das als besonders aufwendig geltende Transkribieren von initial von ärztlicher Seite diktierten medizinischen Berichten an externe Anbieter zu übertragen[7,8]. Sogenannte Medizinische Schreibbüros oder Medizinische Schreibservices bieten dabei meist disziplinenübergreifend (z.B. Radiologie, Chirurgie, Innere Medizin, Labormedizin aber auch Neurologie und Psychiatrie) das Transkribieren von umschriebenen (z.B. Verlaufseinträgen, Aufnahmeresümee, Austrittsberichte) und umfassenden Diktaten (z.B. Berichte an Krankenkassen und Taggeldversicherungen, IV Berichte und Gutachten aus den Bereichen Straf-, Zivil-, und Öffentliches Recht) an. Neben der erwähnten Konzentration auf die Primärprozesse gelten Kostensenkung, Kundenorientierung, Qualität und schnelle „Turn around“ Zeiten als weitere Vorteile des Outsourcing von Schreibdienstleistungen an spezialisierte Anbieter[9].

Verlässliche Zahlen über die Nutzung derartiger Dienstleistungen von Schweizer Spitälern oder von der in der Schweiz niedergelassenen Ärzteschaft liegen derzeit nicht vor. Allerdings spricht die zunehmende Anzahl von Angeboten in der Schweiz (- und Studien aus dem Ausland[10,11]) für einen Anstieg der Nachfrage. Dies könnte daran liegen, dass einerseits die zur Verfügung stehende elektronische Diktatsoftware bis anhin nicht voll die in sie gesetzten Erwartungen erfüllen konnte [12,13,14,15] und andererseits, dass diese Form der Dienstleistung durch den technischen Fortschritt mit der Möglich-

---

[1] MATHERS COLIN D, SADANA RITU, SALOMON JOSHUA A, MURRAY CHRISTOPHER JL, LOPEZ ALAN D: Healthy life expectancy in 191 countries, 1999. The Lancet 2001, 357:1685-1691.
[2] MATHERS COLIN D, IBURG KIM M, SALOMON JOSHUA A, TANDON AJAY, CHATTERJI SOMNATH, USTÜN BEDIRHAN, MURRAY CHRISOTOPHER JL: Global patterns of healthy life expectancy in the year 2002. BMC Public Health 2004, 4:66.
[3] HERZLINGER REGINA E, PARSA-PARSI RAMIN: Consumer-driven health care: lessons from Switzerland. Jama 2004, 292:1213-1220.
[4] LUNDSGAARD-HANSEN NIKLAUS, STETTLER FRITZ: Herausforderungen im Schweizer Spitalwesen. In Book Herausforderungen im Schweizer Spitalwesen, PricewaterhouseCoopers, 2006
[5] SCHÜPFER GUIDO, BABST RETO: Risiken und Nebenwirkungen von Sparprogrammen auf die stationäre Medizin in der Schweiz. PRAXIS (2002 to 2006) 2005, 94:1103-1111.
[6] KIRCHNER MICHAEL, KNOBLICH JENS: Outsourcing tertiärer Dienstleistungen. In Zukunftsorientierter Wandel im Krankenhausmanagement. Springer; 2009: 103-112
[7] LAWLER FRANK H, SCHEID DEWEY C, VIVIANI NANCY J: The cost of medical dictation transcription at an academic family practice center. Arch Fam Med 1998, 7:269-272.
[8] HINICKLE JUDY: RFP: Outsourcing Medical Transcription Perspectives 1995, Health Professions Institute, Fall 1995.:4.
[9] BIKMAN JEREME, WHITING STACILEE: Medical transcription outsourcing greased lightning? Healthcare financial management: journal of the Healthcare Financial Management Association 2007, 61:94-97.
[10] KSHETRI NIR, DHOLAKIA NIKHILESH: Offshoring of healthcare services: the case of US-India trade in medical transcription services. J Health Organ Manag 2011, 25:94-107.
[11] GHODESWAR BHIMRAO, VAIDYANATHAN JANARDAN: Business process outsourcing: an approach to gain access to world-class capabilities. Business Process Management Journal 2008, 14:23-38.
[12] PEZZULLO JOHN A, TUNG GLENN A, ROGG JEFFREY M, DAVIS LAWRENCE M, BRODY JEFFREY M, MAYO-SMITH WILLIAM W: Voice recognition dictation: radiologist as transcriptionist. Journal of digital imaging 2008, 21:384-389.

keit der elektronischen Übermittlung auch grosser Sprachdatenpakete grenzüberschreitend und über grosse Distanzen hinweg, auf immer geringere technische Hindernisse trifft und – anders als bei den anderen genannten Tertiärprozssen - mögliche Kostenvorteile und Effizienzsteigerungen so schnell realisiert werden können [8,9].

Vor dem Hintergrund dieser Entwicklung stellen sich sowohl aus medizinischer als auch aus juristischer Sicht eine Reihe von Fragen, deren zentralste sicher diejenige ist, ob die Nutzung von derartigen Schreibservices eine Verletzung der ärztlichen Schweigepflicht darstellt.

Der vorliegende Artikel – der sich an Ärzte, Juristen und andere Interessierte gleichermassen richtet – soll einen Überblick über die gegenwärtig aktuelle Rechtslage geben. Zur besseren Lesbarkeit wurde dabei ein Format gewählt, welches den Fragen von medizinischer Seite die Antworten des Juristen direkt gegenüberstellt.

Wo liegt der Unterschied zwischen einer Arztsekretärin, die im Spital oder in der Praxis angestellt ist und der Nutzung eines externen Schreibservices in Bezug auf die ärztliche Schweigepflicht?

Die ärztliche Schweigepflicht ist als berufliche Schweigepflicht in Art. 321 StGB[16] geregelt. Das Berufsgeheimnis umfasst dabei nicht einzig die ausdrücklich angeführten Berufe, sondern auch „ihre Hilfspersonen".

Als Hilfsperson versteht man eine Person, die den Geheimnisträger unterstützt inklusive untergeordnete Hilfskräfte, sofern diese auch mit den vertraulichen Informationen in Kontakt kommen[17]. Diese Hilfspersonen unterliegen den gleichen Schweigepflichten, müssen aber unter der „Leitung und Aufsicht" des Geheimnisträgers tätig sein. Im Sinne von Art. 321 StGB kann der Kreis der Hilfspersonen sehr weit gezogen werden, wobei es vor allem auf die Aufgabe und nicht auf die offizielle Funktion ankommt[18].

Eine Arztsekretärin in einem Spital oder in einer Praxis ist eine Hilfsperson im Sinne von Art. 101 OR[19], d.h. sie unterstützt bei der Erfüllung der Tätigkeit (Erfüllungsgehilfe)[20,21]. Inwiefern haftpflichtrechtlich der strengere Art. 55 OR[22] (Geschäftsherrenhaftung) anwendbar sein könnte, muss im Einzelfall untersucht werden[23,24]. Im Unterschied zur Hilfsperson wird beim Outsourcing eine Tätigkeit durch einen Dienstleister selbständig vorgenommen – meist auch längerfristig und in eigenen Räumlichkeiten[25].

Aus datenschutzrechtlicher Sicht ist ein Outsourcing eine Datenbearbeitung durch Dritte, welche in Art. 10a DSG geregelt ist. Grundsätzlich ist eine Datenbearbeitung durch Dritte möglich, sofern keine gesetzliche oder vertragliche Geheimhaltungspflicht dem entgegensteht[26]. Bereits in der Botschaft zum Datenschutzgesetz war festgehalten worden, dass die Übertragung der Datenbearbeitung nicht eingeschränkt werden sollte[27].

Es dürfte unbestritten sein, dass das Berufsgeheimnis von Art. 321 StGB eine gesetzliche Geheimhaltungspflicht darstellt. In der Botschaft war man noch davon ausgegangen, dass gerade das Berufsgeheimnis von Art. 321 StGB eine solche

---

[13] QUINT DOUGLAS J: Voice recognition: ready for prime time? J Am Coll Radiol 2007, 4:667-669; discussion 670-661.
[14] HOYT ROBERT, YOSHIHASHI ANN: Lessons learned from implementation of voice recognition for documentation in the military electronic health record system. Perspectives in health information management/AHIMA, American Health Information Management Association 2010, 7.
[15] AL-AYNATI MAAMOUN M, CHORNEYKO KATHERINE A: Comparison of voice-automated transcription and human transcription in generating pathology reports. Arch Pathol Lab Med 2003, 127:721-725.
[16] SR 311.0: Art. 321 StGB Verletzung des Berufsgeheimnisses
1. Geistliche, Rechtsanwälte, Verteidiger, Notare, Patentanwälte, nach Obligationenrecht zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Chiropraktoren, Apotheker, Hebammen, Psychologen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
[17] TRECHSEL STEFAN/VEST HANS, in Trechsel Stefan/Pieth Mark/Hrsg), Schweizersiches Strafgesetzbuch, Praxiskommentar, 2. Auflage, Zürich/St. Gallen 2012, Art, 321 N13.
[18] OBERHOLZER NIKLAUS, in Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht II, Art. 111 – 392 StGB, 3. Auflage, Basel 2013, Art, 321 N 10.
[19] SR 220: Art. 101 OR Haftung für Hilfspersonen
[1] Wer die Erfüllung einer Schuldpflicht oder die Ausübung eines Rechtes aus einem Schuldverhältnis, wenn auch befugterweise, durch eine Hilfsperson, wie Hausgenossen oder Arbeitnehmer vornehmen lässt, hat dem andern den Schaden zu ersetzen, den die Hilfsperson in Ausübung ihrer Verrichtungen verursacht.
[20] VOLLENWEIDER ANNE-CORINNE, Die Haftpflicht für medizinische Eingriffe, namentlich von Hilfspersonen, Rechtsguteachten gdk, 2001, Ziff. 2.2.2
[21] Vgl. auch Schweizerische Gesellschaft der Vertrauens- und Versicherungsärzte (SGV), Empfehlung Datenschutz Anhang 1, Mustervertrag Hilfsperson VA und VAD
[22] SR 220: Art 55OR Haftung des Geschäftsherrn
[1] Der Geschäftsherr haftet für den Schaden, den seine Arbeitnehmer oder andere Hilfspersonen in Ausübung ihrer dienstlichen oder geschäftlichen Verrichtungen verursacht haben, wenn er nicht nachweist, dass er alle nach den Umständen gebotene Sorgfalt angewendet hat, um einen Schaden dieser Art zu verhüten, oder dass der Schaden auch bei Anwendung dieser Sorgfalt eingetreten wäre.
[2] Der Geschäftsherr kann auf denjenigen, der den Schaden gestiftet hat, insoweit Rückgriff nehmen, als dieser selbst schadenersatzpflichtig ist.
[23] VOLLENWEIDER ANNE-CORINNE, (Fn 20) Ziff. 2.2.2
[24] RUSCH ARNOLD F./BORNHAUSER PHILIP R Korrektiv zur Freizeichnung von der Hilfspersonenhaftung in AJP 10/2010, S. 1232.
[25] Vgl. auch Rundschreiben 2008/7 „Outsourcing Banken", Ziff. 1 f.
[26] SR 235.1: Art. 10a DSG Datenbearbeitung durch Dritte
[1] Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn:
a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und
b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.
[27] Bbl 1998 II 463f.

gesetzliche Geheimhaltung darstellt, die einer Datenbearbeitung durch Dritten entgegensteht, ausser die betroffenen Personen willigten ein[28] .

Wie bereits dargelegt wird inzwischen der Kreis der Hilfspersonen weit gezogen und gemäss neuerer Lehre ist ein Outsourcing auch bei einer beruflichen Schweigepflicht möglich, sofern der Outsourcingnehmer zu einer entsprechenden Geheimhaltung verpflichtet wird[29],[30]. Einer Auftragsdatenbearbeitung steht nichts entgegen[31].

Werden die Daten durch einen Dritten bearbeitet, bleibt die Verantwortung für die Datenbearbeitung beim Auftraggeber. Dieser sollte die den Umständen angemessenen Sorgfaltspflichten anwenden. Er ist auch verpflichtet, seine Sorgfaltspflichten wahrzunehmen: Nebst der sorgfältigen Auswahl ist er auch für eine klare Instruktion verantwortlich. Zudem hat er sich zu vergewissern, dass die Datensicherheit gewährleistet wird.

Der Unterschied zwischen einer Arztsekretärin im Spital und einem externen Schreibservice besteht vor allem darin, dass die Arztsekretärin aufgrund ihrer Anstellung bereits als Hilfsperson des Arztes gilt und damit der beruflichen Schweigepflicht von Art. 321 StGB untersteht. Bei der Nutzung eines externen Schreibservices handelt es sich demgegenüber um ein Outsourcing und die berufliche Schweigepflicht muss explizit auf diesen übertragen werden.

Idealerweise wird die Datenbearbeitung schriftlich geregelt. Folgende Punkte sollten in einer Vereinbarung enthalten sein:

- Rahmen der Datenbearbeitung
- Hinweis auf gesetzliche Bestimmungen (z.B. Art. 321 StGB)
- Keine Weitergabe an weitere Dritte ohne Wissen des Auftraggebers
- Ort der Datenbearbeitung
- Pflichten bezüglich Datensicherheit und Datenschutz[32]

Fazit: Sowohl die Arztsekretärin als auch der externe Schreibservice unterstehen der beruflichen Schweigepflicht, letztere jedoch nur, wenn diese vertraglich auf den Schreibservice übertragen wurde.

Ist eine Anonymisierung oder Pseudonymisierung der Expl. oder auch der behandelnden Ärzte, einzelner Institutionen im Diktat, welches extern geschrieben werden soll, notwendig?

Vorgängig ist auf den Unterschied zwischen Anonymisierung und Pseudonymisierung einzugehen:

Anonymisierung

Durch die Anonymisierung werden Personendaten unwiderruflich so verändert, dass die betroffene Person weder direkt noch indirekt wieder identifiziert werden kann[33]. Es ist notwendig, dass keinerlei Merkmale oder Informationen direkt auf die betroffene Person schliessen lassen. Bei der Bearbeitung anonymisierter Daten ist weder das Datenschutzgesetz anwendbar noch kann das Berufsgeheimnis verletzt werden, da es dabei nicht mehr um Personendaten im Sinne des Datenschutzgesetzes handelt beziehungsweise der Geheimnisherr nicht mehr rückbestimmbar ist.

Eine Anonymisierung der Daten empfiehlt sich nicht, da auch der Auftraggeber die Daten nicht mehr auf eine Person bestimmen kann oder nur mit unverhältnismässig grossem Aufwand. Ausnahme: Es handelt sich um einen Forschungsbericht, bei dem nicht die betroffenen Personen im Zentrum stehen und die Veröffentlichung anonymisiert erfolgen soll.

Pseudonymisierung

Durch eine Pseudonymisierung werden Personendaten mittels Identifikatoren oder Aliase ersetzt, um die Bestimmbarkeit einer Person zu erschweren[34]. Mit der Pseudonymisierung soll bei Bedarf ein Bezug zu einer bestimmten Person wieder hergestellt werden können[35]. Durch Kenntnisse bestimmter Parameter und Verfahren kann wieder ein klarer Bezug zu einer Person hergestellt werden.

Bei einer Pseudonymisierung handelt es sich folglich weiterhin um Personendaten – die betroffenen Personen sind für jene Personen bestimmbar im Sinne von Art. 3 lit. a DSG[36], welche die Zuordnungsregel beziehungsweise den Schlüssel

[28] Bbl 1998 II 464.
[29] ROSENTHAL DAVID, in Rosenthal David, Jöhri Yvonne Hrsg, Handkommentar zum Datenschutzgesetz, Art. 10a N107
[30] WIDMER URSULA, Rechtliche Rahmenbedingungen für das Outsourcing im Spitalbereich – Weitergabe von Patientendaten, in: datamaster September 2007, S. 20
[31] ROSENTHAL DAVID, (Fn 29) Art. 10a N 103 ff.
[32] Vgl. auch Muster für Geheimhaltungserklärung beim Outsourcing, Datenschutzbeauftragter Kanton Zürich.
[33] ISO/IEC 29100:2011, Information technology – Security techniques – Privacy Framework, Pkt 2.2.
[34] ISO/IEC 29100:2011, Information technology – Security techniques – Privacy Framework, Pkt 2.24.
[35] Datenschutzstelle Fürstentum Liechtenstein: Richtlinie über die Anwendung der Anonymisierung/ Pseudonymisierung, S. 5 f
[36] SR 235.1 Art. 3 DSG Begriffe:
a. *Personendaten (Daten):* alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;

kennen; das Datenschutzgesetz ist grundsätzlich anwendbar. Für weitere Personen sind es jedoch keine Personendaten, da diese keinen Bezug zu einer bestimmten Person herstellen können[37].

Eine Pseudonymisierung der Daten bei externen Schreibservicen wäre sicherlich die idealste Lösung. Dadurch ist das Berufsgeheimnis gewahrt, auch die datenschutzrechtlichen Grundsätze gegenüber dem Auftragnehmer sind eingehalten, da dieser aus seiner Sicht anonyme Daten erhält. Entscheidend ist, wie die Pseudonymisierung erfolgt und dass es dadurch keinesfalls zu Verwechslungen kommt. Die Datenrichtigkeit muss gewahrt bleiben. Die Verantwortung für die Richtigkeit der Daten liegt beim Inhaber der Datensammlung, dem Auftraggeber.

Die Richtigkeit der Daten – Art. 5 DSG[38] - ist ein datenschutzrechtlicher Grundsatz. Eine Verletzung desselben stellt eine Persönlichkeitsverletzung dar[39]. Insbesondere muss dabei das Risiko für die betroffene Person bei falschen oder unrichtigen Daten bedacht werden.

Wie oben dargelegt, kann ein externer Dienstleister in die berufliche Schweigepflicht eingebunden werden. Insofern stellt sich die Frage, ob der Aufwand und das Risiko einer Pseudonymisierung notwendig und sinnvoll ist.

Das Datenschutzgesetz fordert eine Verhältnismässigkeit bei der Datenbearbeitung[40]. Die FMH hat in diversen Artikeln auf die Verhältnismässigkeit der Datenbearbeitung hingewiesen und wenn immer möglich eine Anonymisierung gefordert[41], um die Verhältnismässigkeit bezüglich der Anzahl Personen, die Zugriff/Informationen über Patienten erhalten, klein zu halten.

Die Verhältnismässigkeit, übernommen aus dem öffentlichen Recht, erfordert, dass die Datenbearbeitung geeignet und notwendig ist, sowie in einem vernünftigen Verhältnis zur Persönlichkeitsbeeinträchtigung steht[42].

Es muss sowohl der Zweck als auch die Art und Weise der Bearbeitung verhältnismässig sein[43]. Als verhältnismässig kann auch gelten, wenn der Eingriff des Persönlichkeitsverlustes geringer wiegt als ein allfälliger Effizienzverlust oder Kostennachteile[44].

In der medizinischen Forschung ist die Pseudonymisierung heute absolut üblich und der Aufwand scheint absolut vertretbar[45]. Ganz anders sieht es aus bei der Nutzung eines medizinischen Schreibservices. Publizierte Erfahrungen mit Programmen oder von Möglichkeiten, die eine Pseudonymisierung in diesem Bereich fördern würden, lagen den Autoren beim Verfassen dieses Artikels nicht vor. In der Praxis werden deshalb den Schreibbüros häufig vollständige Daten übermittelt (z.B. bei Verlaufsberichten, Diktaten von Befunden) oder nur diskret verschlüsselt, z.B. durch die Verwendung von Initialen statt des Vollnamens oder durch das Weglassen und später nachträgliches Einfügen von Versicherten-Nummern, Adresse und Geburtsdatum (im Gutachtensbereich).

Man muss dabei aber mitberücksichtigen, dass die medizinische Forschung nicht eine Hilfstätigkeit darstellt, vielmehr werden die medizinischen Daten intensiv genutzt. Bei einem Schreibservice besteht die Dienstleistung gerade darin, dass der Arzt von administrativen Tätigkeiten entlastet wird. Es ist klar eine Hilfstätigkeit.

Fazit: Zwar wäre eine Pseudonymisierung wünschenswert. Sofern mit dem Schreibservice vertraglich die Rahmenbedingungen, der Umfang der Datenbearbeitung, die Sorgfaltspflichten klar geregelt und die berufliche Schweigepflicht übertragen wird, kann von einer Pseudonymisierung abgesehen werden.

Wie soll im Diktat mit Daten, die Rückschlüsse auf das Individuum zulassen z.B. Versicherten-Nummer, Geburtsdaten etc., umgegangen werden?

Solange man sicherstellt, dass der Outsourcingpartner sich an die Schweigepflichten hält, stellen solche Daten, die auf eine bestimmbare Person schliessen lassen, kein Problem dar. Will man die Daten pseudonymisieren, sollte das Thema der Datenrichtigkeit und des zusätzlichen Aufwandes nicht vernachlässigt werden.

Es ist aber, wie bereits dargelegt, zu begrüssen, dass wenn immer möglich mit pseudonymisierten Daten gearbeitet wird.

---

[37] ROSENTHAL DAVID, (Fn 29), Art. 3 N 36.
[38] SR 235.1 Art. 5 DSG Richtigkeit der Daten
[1] Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.
[2] Jede betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden.
[39] ROSENTHAL DAVID, (Fn 29), Art. 5 N4.
[40] Art. 4 Abs. 2 DSG: [2] Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.
[41] Stellungnahme der FMH zum Arztgeheimnis und Datenschutz, November 2010; LANG GABRIELA, KUHN HANSPETER, MEYER BEATRIX, INGENPASS PETRA, WAGNER JUDITH, Gewährleistung des Datenschutzes – externe und professionelle Kodierrevision macht es möglich, in Schweizerische Ärztezeitung, Nr. 34, 2010, S. 1267
[42] ROSENTHAL DAVID, (Fn 29), Art. 4 N 19
[43] ROSENTHAL DAVID, (Fn 29), Art. 4 N 20
[44] ROSENTHAL DAVID, (Fn 29), Art. 4 N 29
[45] Vgl. EU-Projekt „linked2safety“

Muss die Nutzung von Schreibservices dem Patienten offengelegt werden? Muss eine mündliche gar schriftliche Einwilligung der Expl./Pat. bei Nutzung von Schreibservices vorhanden sein?

Der Hintergrund des Berufsgeheimnisses besteht im Vertrauensverhältnis, das zwischen Klient und Arzt nicht leichtfertig verletzt werden soll[46]. Der Patient kennt den Arzt persönlich, er sieht auch, wer bei ihm arbeitet. Werden die Daten aber Dritten weitergegeben, ist für den Patienten nicht mehr erkennbar, wer auch noch etwas über seine Gesundheit erfährt. Arbeitet seine Nachbarin beim Arzt, dürfte ihm dies bekannt sein; arbeitet aber sein Nachbar beim Schreibservice, ist ihm nicht bewusst, dass dieser Informationen über ihn erhalten könnte, wenn er nicht über die Datenweitergabe beziehungsweise das Outsourcing informiert wird.

Auch die FMH empfehlen grösstmögliche Transparenz[47]. Transparenz wird ebenfalls bei der Ärztekasse in den Allgemeinen Geschäftsbedingungen zwischen Arzt und Ärztekasse vorausgesetzt. Dem Arzt wird entsprechendes Informationsmaterial zur Verfügung gestellt, um seine Patienten über die Zusammenarbeit mit der Ärztekasse zu informieren[48].

Durch die hergestellte Transparenz hat der Patient die Möglichkeit zu entscheiden, ob er damit einverstanden ist. Falls er damit nicht einverstanden ist, kann er dies mitteilen[49]. Die Anforderungen an die Einwilligung sind gesetzlich nicht geregelt. So genügt grundsätzlich eine stillschweigende oder konkludente Einwilligung[50]. Wichtig ist demgegenüber, dass die Einwilligung auf einer freien Entscheidfindung beruht, die betroffene Person genügend Informationen im Konkreten hat[51].

Werden Dritte involviert, sollte man die betroffenen Personen mindestens informieren, so dass sich diese durch Widerspruch dem Outsourcing widersetzen könnten. Aus Beweisgründen empfiehlt sich eine schriftliche Einwilligung.

In der Praxis wird heute meist auf diese Transparenz verzichtet. Dies keineswegs weil man dem Patienten etwas verschweigen will, sondern vielmehr weil man die möglichen Interessen und Gefahren für den Patienten nicht im Fokus hat.

Das Berufsgeheimnis basiert ja auf dem Vertrauen, das man in eine bestimmte Person hat. Allenfalls sucht ein Patient gerade deswegen einen bestimmten Arzt auf, weil er darauf vertraut, dort keine Bekannten anzutreffen. Werden aber Hilfskräfte beansprucht, die für den Patienten nicht erkennbar sind, kann allenfalls genau die Absicht des Patienten durchkreuzt werden. Es ist für ihn nicht erkennbar, dass seine Krankheitsgeschichte einer Drittperson zur Kenntnis gelangt – auch wenn sich diese Person an das Berufsgeheimnis hält –, der er niemals seine Krankheit anvertraut hätte.

Schreibservices haben Datenschutzerklärungen[52]. Sind diese bindend? Sollten von Seiten der Auftraggeber eigene Erklärungen vorbereitet werden?

Eine allgemeine Antwort kann nicht gegeben werden. Wie bei allen Verträgen, Allgemeinen Geschäftsbedingungen (AGB) muss der Inhalt im Einzelfall geprüft werden. Es ist davon auszugehen, dass ein Schreibservice mit einer Datenschutzerklärung versucht, Vertrauen zu gewinnen, und entsprechend freundlich tönende Formulierungen wählt. Gleichzeitig werden die Formulierungen eher zu den eigenen Gunsten sein[53].

Werden die Datenschutzerklärungen vom Auftraggeber akzeptiert, sind diese bindend, sofern diese einen Vertragsbestandteil darstellen und nicht die Ungewöhnlichkeitsregel zur Anwendung kommt, weil ungewöhnliche Klauseln in den AGB enthalten sind[54]. Es gilt der Grundsatz der Vertragstreue: Pacta sunt servanda[55] .

Da die Einhaltung des Datenschutzes und der beruflichen Schweigepflicht im Interesse des Auftraggebers ist – er ist auch weiterhin dafür verantwortlich – ist es sinnvoll, wenn er eine Datenschutzerklärung ausformuliert und vom Outsourcingnehmer unterzeichnen lässt.

[46] OBERHOLZER Nilklaus, (Fn 18) Art. 321 N 4
[47] Rechtliche Grundlagen im medizinischen Alltag – ein Leitfaden für die Praxis, Hrsg. Schweizerische Akademie für Medizinische Wissenschaften und der Verbindung der Schweizer Ärzte und Ärztinnen FMH, 2. Auflage, 2012, S. 99ff.
[48] AGB der Ärztekasse, vom 28.3.2013, Ziff. 3.9
[49] ROSENTHAL DAVID, (Fn 29), Art. 4 N 51.
[50] ROSENTHAL DAVID, (Fn 29), Art. 10a DSG, N 111 und Art. 4 N77.
[51] ROSENTHAL DAVID, (Fn 29), Art. 4 N 67ff.
[52] AAMT (American Association for Medical Transcription) speaks out on confidentiality, privacy, and patient care documentation. J Am Assoc Med Transcr 1995, 14:42, 44-47.
[53] GRASSEGGER HANNES, Schlechter Deal, in Das Magazin 23/2014, S. 18 ff.
[54] BGE 135 III 1f.
[55] WIEGAND WOLFGANG, in Honsell Heinrich/Vogt Nedim Peter/ Wiegand Wolfgang (Hrsg.), Basler Kommentar, 5. Auflage, Basel 2011, Art. 18 OR N97.

Was ist bei grenzüberschreitender Nutzung (CH/EU/ausserhalb EU) zu beachten? Was ändert sich, wenn der externe Anbieter - zur Auftragsakquise - zwar ein Büro in der Schweiz unterhält, das Diktat dann aber zur Transkription in ein EU bzw. Nicht-EU Land weiterleitet?

Am 28. Juni 2012 wurde im Radio Télévision Suisse berichtet, dass Röntgenberichte des Universitätsspitals Genf aus praktischen und ökonomischen Gründen in Marokko geschrieben würden. Schon damals wurde die Frage nach dem Berufsgeheimnis und dem Datenschutz gestellt[56].

Bei einer grenzüberschreitenden Datenbearbeitung ist zu unterscheiden zwischen Ländern mit einem gleichwertigen Datenschutzniveau und anderen. Die EU hat einen gleichwertigen Datenschutz; wobei auch Staaten wie Uruguay oder Israel über einen gleichwertigen Datenschutz verfügen[57]. Der eidg. Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) ist gemäss Art. 31 Abs. 1 lit. d DSG[58] verpflichtet, eine Liste der Länder mit gleichwertigem Datenschutz zu führen. Diese ist auf der Homepage des EDÖB hinterlegt und kann heruntergeladen werden.

Handelt es sich um ein Drittland, das einen gleichwertigen Datenschutz besitzt, kann der Auftraggeber auf eine eigene Prüfung bezüglich der Angemessenheit des Datenschutzes verzichten[59]. Die Daten können dort bearbeitet werden.

Ist das Land nicht auf der Liste des EDÖB, müssen zusätzliche Sicherheitsmassnahmen umgesetzt werden[60]. Bei einem Schreibservice drängt sich eine vertragliche Lösung auf; es könnte auch die Einwilligung der betroffenen Person im Einzelfall eingeholt werden[61]. Diese Variante dürfte nur dann in Frage kommen, wenn die Nutzung des ausländischen Schreibservices ein Spezialfall darstellt und man nicht regelmässig mit diesem zusammenarbeitet.

Es gibt verschiedene Musterverträge[62]. Wichtig ist die Regelung bezüglich Sub-Kontrakten: Solche sollten grundsätzlich nicht erlaubt sein, es sei denn der Auftraggeber wird darüber informiert und ist damit ausdrücklich einverstanden. Die Art und Weise der Datenbearbeitung wie auch die Rechte der betroffenen Personen sind klar zu regeln[63]. Im Vertrag sollte festgehalten werden, dass das Schweizer Recht anwendbar sei sowie dass der Gerichtsstand in der Schweiz ist.

Es spielt im Weiteren keine Rolle, ob der Anbieter der Schreibdienste ein Büro in der Schweiz hat oder direkt im Ausland domiziliert ist. Entscheidend ist, wo die Datenbearbeitung erfolgt. Deshalb sollte beim Outsourcing vertraglich klar festgehalten werden, wo die Datenbearbeitung erfolgt und welche Rechte der Datenexporteur hat, um die Einhaltung der Verpflichtungen überprüfen zu können. Dies könnte durch jährliche Audits, Stichproben/Überprüfungen vor Ort oder auch Berichte erfolgen[64].

Eine andere Frage ist jedoch kritisch zu prüfen: Inwiefern kann ein Datenbearbeiter im Ausland als Hilfsperson gelten, die den Regelungen von Art. 321 StGB unterliegen?

Schwaninger/Lattmann vertreten mit Verweise auf Ursula Widmer die Meinung, dass eine Datenbearbeitung im Ausland nur mit Einwilligung der betroffenen Person möglich sei, da der Dritte dann nicht mehr als Hilfsperson im Sinne von Art. 321 StGB anzusehen sei. Insbesondere sei die schweizerische Strafgesetzgebung nicht oder nur beschränkt durchetzbar[65]. Im Zürcher Handkommentar zum Datenschutzgesetz wird zumindest zur Vorsicht gemahnt, wenn eine Datenbearbeitung im Ausland erfolgen soll und ein Berufsgeheimnis tangiert wird. Der Fokus liegt dabei auf Fabrikations- und Geschäftsgeheimnisse, weshalb auch auf Art. 273 StGB (Wirtschaftlicher Nachrichtendienst)[66] hingewiesen wird[67].

Vorliegend geht es aber keineswegs um Geschäftsgeheimnisse, vielmehr geht es um Personendaten, Patientendaten. Der Arzt bleibt für das Tun seiner Hilfsperson verantwortlich. Es liegt also im originären Interesse des Auftraggebers, dass der Auftragnehmer sich an die Vorgaben hält und kein Geheimnisverrat begeht. Die ärztliche Schweigepflicht geht zurück auf den Eid des Hippokrates[68] und ist grundsätzlich weltweit verbreitet. Insbesondere in allen Ländern der EU, aber

---

[56] http://www.rts.ch/info/regions/geneve/4105659-les-rapports-de-radiographie-des-hug-sont-parfois-rediges-au-maroc.html (besucht am 13. September 2014)
[57] Vgl. Staatenliste des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (Stand des Datenschutzes weltweit)
[58] SR 235.1 Art. 29 Abs. 1 DSG Der Beauftragte hat insbesondere folgende weiteren Aufgaben:
d Er begutachtet, inwieweit die Datenschutzgesetzgebung im Ausland einen angemessenen Schutz gewährleistet.
[59] Datenübermittlung ins Ausland kurz erklärt, Eidg. Datenschutz- und Öffentlichkeitsbeauftragter, Ziff. 10.
[60] Merkblatt Cloud Computing, Datenschutzbeauftragter Kanton Zürich, 2012, Ziff. 4.4.
[61] SR 235.1 DSG Art. 6 Grenzüberschreitende Bekanntgabe
2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:
a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;
b. die betroffene Person im Einzelfall eingewilligt hat;
[62] Mustervertrag für das Outsourcing für Datenbearbeitung im Ausland des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten, Modal Contracts for the transfer of personal data to third countries des Europarates
[63] ROSENTHAL DAVID, (Fn 29), Art. 6 N39.
[64] ROSENTHAL DAVID, (Fn 29), Art. 6 N40.
[65] SCHWANINGER DAVID / LATTMANN STEPHANIE S., a.a.O. Ziff. 3.
[66] SR 311.0 Art. 273 StGB
Wer ein Fabrikations- oder Geschäftsgeheimnis auskundschaftet, um es einer fremden amtlichen Stelle oder einer ausländischen Organisation oder privaten Unternehmung oder ihren Agenten zugänglich zu machen,
wer ein Fabrikations- oder Geschäftsgeheimnis einer fremden amtlichen Stelle oder einer ausländischen Organisation oder privaten Unternehmung oder ihren Agenten zugänglich macht,
wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe, in schweren Fällen mit Freiheitsstrafe nicht unter einem Jahr bestraft. Mit der Freiheitsstrafe kann Geldstrafe verbunden werden.
[67] ROSENTHAL DAVID, (Fn 29), Art. 10a N 108.
[68] Griechischer Arzt, 460-370 v.Chr. – vgl. auch http://de.wikipedia.org/wiki/Eid_des_Hippokrates besucht am 8.7.2014

auch in Nord- und Lateinamerika, Australien, Neuseeland ist das Arztgeheimnis bekannt und wird ähnlich der schweizerischen Gesetzgebung eigenständig sanktioniert (beispielsweise: Deutschland § 203 StGB[69], Österreich § 121 StGB[70], Frankreich: Art. 226-13 Code Penal[71], England, Wales und Australien – common law[72] Kanada: z.B. Québec 60.4 Code des profession[73], Italien: Art. 622 del codice penale[74]).

Es ist also ersichtlich, dass die Verletzung eines Berufsgeheimnisses in vielen Ländern eigenständig sanktioniert werden können – abgesehen von den datenschutzrechtlichen Pflichten, deren Verletzung teilweise mit härteren Sanktionsandrohungen versehen sind, als in der Schweiz. Selbst Banken könnten Dienstleistungen ins Ausland auslagern, sofern sie „ihre Prüfrechte wahrnehmen und rechtlich durchsetzen können[75].“

Aus diesen Gründen ist nicht nachvollziehbar, weshalb eine Auslagerung ins Ausland zwar aus datenschutzrechtlichen Gründen erlaubt, aufgrund des Berufsgeheimnisses verboten sein soll, sofern im Zielland das Berufsgeheimnis geregelt ist. Es ist vor der Auftragserteilung zu prüfen, welches die Rahmenbedingungen bezüglich der ärztlichen Schweigepflicht im Zielland sind; ist das Berufsgeheimnis klar geregelt, ist eine Datenbearbeitung möglich. Dass der Vertragspartner sorgfältig ausgewählt, instruiert und auch ab und zu überprüft wird, sollte eine Selbstverständlichkeit sein. Zusätzlich empfiehlt es sich, die Pflichten vertraglich nochmals festzuhalten.

Ist die Nutzung von sogenannte „Cloud Service“s, also das Zwischenspeichern von Diktaten auf Servern im Ausland, zulässig?

Cloud Service, Cloud Computing – diese Begriffe werden oft parallel genutzt[76], wobei in der Literatur Cloud Computing gebräuchlicher ist. Eine allgemein akzeptierte Definition von Cloud Computing[77] ist diejenige des National Institute of Standards and Technology: „Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können[78]."

Cloud Computing ist ein typisches Outsourcing, eine Datenbearbeitung durch einen Dritten[79]. Es gelten die bereits genannten Voraussetzungen für eine Datenbearbeitung durch einen Dritten und die Anforderungen an Hilfspersonen (vgl. Frage 1).

Im Merkblatt „Cloud Computing“ des Datenschutzbeauftragten des Kantons Zürich, welches sich an die öffentlichen Organe des Kantons Zürich richtet, wird verlangt, dass eine Datenbekanntgabe ins Ausland nur möglich ist, wenn ein „gleichwertiges Datenschutzniveau besteht und/oder zusätzliche Sicherheitsmassnahmen umgesetzt werden[80].“ Auftraggeber unterstehen dabei mehrheitlich dem Amtsgeheimnis, weshalb eine analoge Anwendung auch für Auftraggeber mit Berufsgeheimnis anzunehmen ist. Im Leitfaden der FMH wird zusätzlich darauf hingewiesen, dass auf eine vorgängige Verschlüsselung der Daten zu achten ist[81].

---

[69] § 203 StGB Verletzung von Privatgeheimnissen
1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung anvertraut worden oder sonst bekanntgeworden ist,
wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

[70] § 121 StGB Verletzung von Berufsgeheimnissen
(1) Wer ein Geheimnis offenbart oder verwertet, das den Gesundheitszustand einer Person betrifft und das ihm bei berufsmäßiger Ausübung eines gesetzlich geregelten Gesundheitsberufes oder bei berufsmäßiger Beschäftigung mit Aufgaben der Verwaltung einer Krankenanstalt oder eines anderen Gesundheitsdiensteanbieters (§ 2 Z 2 des Gesundheitstelematikgesetzes 2012, BGBl. I Nr. 111/2012) oder mit Aufgaben der Kranken-, der Unfall-, der Lebens- oder der Sozialversicherung ausschließlich kraft seines Berufes anvertraut worden oder zugänglich geworden ist und dessen Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse der Person zu verletzen, die seine Tätigkeit in Anspruch genommen hat oder für die sie in Anspruch genommen worden ist, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

[71] Article 226-13 Code pénal:
La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.

[72] http://en.wikipedia.org/wiki/Legal_professional_privilege (besucht am 9.7.2014)

[73] Le professionnel doit respecter le secret de tout renseignement de nature confidentielle qui vient à sa connaissance dans l'exercice de sa profession. - http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_26/C26.htm besucht am 9.7.2014

[74] Art. 622 codice penale - Rivelazione di segreto professionale
Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.

[75] Rundschreiben FINMA 2008/7 Outsorucing Banken, N 49.

[76] SCHWANINGER DAVID / LATTMANN STEPHANIE S., Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, in: Jusletter 11. März 2013, N1f.

[77] Vgl. auch Bundesamt für Sicherheit in der Informationstechnik - Cloud Computing Grundlagen.

[78] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf besucht am 29.6.2014

[79] MITTELBERGER PHILIPP/BINDER GABRIELA, Datenschutzrechtliche Chancen und Risiken von Cloud Computing in: Jus & News 2011/2, S. 163 ff. Ziff. 3.

[80] Merkblatt Cloud Computing Datenschutzbeauftragter Kanton Zürich, V 1.1., August 2012, Ziff. 4.4.

[81] Rechtliche Grundlagen im medizinischen Alltag – ein Leitfaden für die Praxis, Hrsg. Schweizerische Akademie für Medizinische Wissenschaften und der Verbindung der Schweizer Ärzte und Ärztinnen FMH, 2. Auflage, 2012, S. 48

Zentral dürfte sein, wie die Rechte der betroffenen Personen durchgesetzt werden können. Eine Datenbearbeitung sollte kritisch hinterfragt und begleitet werden. Wichtig ist, dass die Datensicherheit gewährleistet ist. Es empfiehlt sich, wie bei jedem Outsourcing, eine Risikoanalyse durchzuführen. Die European Network and Information Securitiy Agency (ENISA), eine von der Europäischen Union 2004 gegründete Agentur, hat sich vertieft mit Chancen und Risiken des Cloud Computing auseinandergesetzt; das Ergebnis zeigt ein ausgeglichenes Bild. Im Einzelfall muss eine Abwägung vorgenommen werden[82].

Sind bezüglich des elektronischen Versandes von Diktaten aus juristischer Perspektive besondere Anforderungen an Hard- und Software zu stellen?

Grundsätzlich wird bei den datenschutzrechtlichen Anforderungen an die Datensicherheit nicht zwischen Hard- und Software unterschieden. Das Gesetz spricht allgemein von „automatisierter Bearbeitung“[83].

Es existieren zwar Definitionen für Hard[84]- und Software[85], in der Praxis ist eine Trennung nicht so einfach, wie Beispiele immer wieder zeigen[86]. Entscheidend ist vielmehr, dass die technischen Systeme insgesamt die Einhaltung des Datenschutzes ermöglichen[87].

Fazit

Eine Arbeitsteilung ist Teil unserer Kultur und hat sich in den letzten Jahrhunderten verstärkt. Das Auslagern von Tätigkeiten – Outsourcing – ist die logische Fortsetzung dieser Entwicklung. Auch im medizinischen Umfeld findet schon länger eine Arbeitsteilung statt.

Die Nutzung von medizinischen Schreibservices – ein klassisches Outsourcing – muss dabei unter dem Aspekt von Datenschutz, beruflicher Schweigepflicht und Datensicherheit beurteilt werden. Wie ausführlich dargelegt, ist die Nutzung eines inländischen Schreibservices problemlos möglich, sofern der Auftraggeber die Pflichten dem Auftragnehmer überträgt und dabei nicht vergisst, dass er die Oberverantwortung weiterhin trägt. Werden ausländische Schreibservices beauftragt, ist vorgängig das Berufsgeheimnis im Zielland zu prüfen. Ist ein solches gegeben, gilt auch hier: Ein Outsourcing ist möglich, die Oberverantwortung bleibt beim Auftraggeber, ein schriftlicher Vertrag, in welchem die Aufgaben klar umschrieben und die Pflichten geregelt sind, empfiehlt sich.

Zudem sollte gegenüber den Patientinnen und Patienten transparent dargelegt werden, dass mit einem medizinischen Schreibservice zusammengearbeitet wird. Dies kann mittels Informationsmaterial oder/und bei der Patientenanmeldung auf dem Anmeldeformular erfolgen. Wichtig ist, dass die betroffene Person informiert ist. Dies ermöglicht ihr allenfalls Vorbehalte anzubringen oder eine Weitergabe der Daten zu verbieten.

Uttinger Ursula, lic. iur. / exec. MBA HSG, Geschäftsführerin Activita Care Management AG, Präsidentin Datenschutz-Forum Schweiz, Dozentin für Datenschutz an diversen Hochschulen

Liebrenz Michael, Dr. med., Psychiatrie und Psychotherapie FMH, Research Fellow Division of Law, Ethics, and Psychiatry Columbia University New York (USA), Leiter Gutachtenstelle für Zivil- und Öffentlichrechtliche Fragestellungen, Psychiatrische Universitätsklinik Zürich

[82] www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport - bersucht am 29.6.2014

[83] SR 235.11 Verordnung zum Bundesgesetz über den Datenschutz (VDSG) Art. 9.
1 Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden:
a.Zugangskontrolle: unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren;
b. Personendatenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;
c. Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;
d. Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können;
e. Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;
f. Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;
g. Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;
h. Eingabekontrolle: in automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.

[84] http://www.pc-typ.de/fachbegriffe-lexikon/hardware/ besucht am 28.6.2014

[85] http://www.itwissen.info/definition/lexikon/Software-SW-software.html besucht am 28.6.2014

[86] http://www.heise.de/security/meldung/Verkaufsstopp-fuer-China-Phone-mit-Spionagetrojaner-2235466.html besucht am 28.6.2014

[87] Kriterienkatalog für die Datenschutzzertifizierungen, Fürstentum Liechtenstein, Version 1.0, Dezember 2013, Ziff. 2.