Der folgende Artikel zeigt die komplexen rechtlichen Grundlagen im Umfeld der medizinischen Dokumentation und der E-Health am Beispiel eines ausgewählten Kantons auf. U. Erlinger macht auch deutlich, dass die Anforderungen sich nicht nur auf Systeme beziehen, sondern zu einem beträchtlichen Teil Anforderungen an die Organisationsentwicklung werden – Entwicklung der Organisation Spital, aber auch der Organisation Arztpraxis.
Es besteht häufig grosse Unsicherheit über die rechtlichen Rahmenbedingungen und wie sie zu interpretieren sind – was heisst das für mich als Arzt im Spital, als Ärztin in der Arztpraxis? Diese Unsicherheit ist ein Grund für die Zurückhaltung gegenüber E-Health.
Hier erwarten wir von den Arbeiten im Koordinationsorgan eHealth des Bundes und der Kantone, insbesondere vom Teilprojekt Rechtliche Grundlagen, einen Beitrag zur Klärung. Wir finden es richtig, dass die Arbeitsgruppe des Teilprojekts Rechtliche Grundlagen empfiehlt, ein eigenes E-Health-Gesetz zu schaffen. Dieser Weg hat zwei Vorteile. Zum einen soll so viel als möglich für die Schweiz einheitlich geregelt werden – so sollen z. B. Zuweisungen von Patienten über die Kantonsgrenze nicht durch unterschiedliche kantonale E-Health-Regeln erschwert werden. Zum anderen ist es sinnvoll, diese Regelungen in einem eigenen Gesetz und nicht im KVG zu verankern – es geht ja um E-Health und nicht um E-Insurance. Bund und Kantone müssen hier die Weichen stellen, damit der potentielle Nutzen von E-Health für Patienten realisierbar wird.

Judith Wagner, Leiterin eHealth FMH

Medizinrechtliche Aspekte der elektronischen Dokumentation und des elektronischen Datenaustausches in der Medizin

E-Health im Kanton Zürich

Ulrich Erlinger

Einleitung

Weltweit wird etwa seit den achtziger Jahren vor allem in entwickelten Ländern ernsthaft versucht, die Krankengeschichten von Patientinnen und Patienten im Dienst einer besseren Verfügbarkeit und Kontrolle elektronisch zu verwalten. Rechtliche Aspekte des Datenschutzes standen schon von Beginn an im Vordergrund der Auseinandersetzung mit dem Thema [1–19]. Um mehr Vertrauen in die Datenverwaltung zu schaffen, wurden rechtliche Fragen behandelt und durch eine entsprechende Konzipierung der Datenverwaltungssysteme auch für die medizinische Forschung der Versuch unternommen, die Systeme sicherer zu machen [20, 21].

Die gegenwärtige medizinische Behandlung nach westlichen Standards ist charakterisiert durch einen hohen Spezialisierungsgrad vieler Leistungserbringer im ambulanten, teilstationären und stationären Bereich. Der zunehmend grosse Anteil an chronischen Patientinnen und Patienten vor dem Hintergrund der demographischen Entwicklung und der erwähnte Spezialisierungsgrad der Leistungserbringer sorgen dafür, dass an der Behandlung eines Individuums mehrere Leistungserbringer beteiligt sind, die im günstigen Fall über die Behandlung durch den Kollegen Bescheid wissen. Die zunehmenden interdisziplinären und multiprofessionellen Langzeitbehandlungen lassen den Bedarf für einen Austausch der medizinischen Daten stark ansteigen. Alle Interessenvertreter im Gesundheitswesen wünschen sich, dass der Datenfluss im Interesse der Patientin und des Patienten, ihr oder sein Einverständnis vorausgesetzt, möglichst ungehindert, schnell und sicher stattfinden sollte.

La cybersanté dans le canton de Zurich

Dans le cadre de la stratégie e-Health menée par la Confédération et les cantons, il est prévu d'accroître l'utilisation des supports électroniques pour la gestion et l'échange des données de patients, ce qui augmentera la disponibilité des données pour le traitement des personnes concernées et donc aussi pour le contrôle et l'amélioration de la qualité. La cybersanté est une condition importante à remplir pour améliorer la qualité thérapeutique et accroître l'efficacité de notre système de santé. Mais la complexité technique de la documentation informatique et des échanges électroniques de données, malgré les nombreux avantages qu'elle procure, est aussi une source d'incertitudes chez les médecins traitants. L'évaluation juridique de la cybersanté d'un point de vue médical contribue à clarifier la situation et à renforcer la confiance dans les structures électroniques.

Stadtärztlicher Dienst Zürich
Korrespondenz:
Dr. med. Ulrich Erlinger
Stadtärztlicher Dienst Zürich
Public Health / Suchtmedizin
Walchestrasse 31
Postfach 3251
CH-8021 Zürich
Tel. 044 412 48 05

ulrich.erlinger@zuerich.ch

www.stadt-zuerich.ch/stadtarzt

Patientinnen und Patienten wünschen sich zudem, dass sie bei Bedarf diesen Datenfluss kontrollieren, unterbinden und beenden können. Ausserdem haben vereinzelt Patienten das Bedürfnis, genau zu wissen, was über ihre Behandlung dokumentiert wird. Ärzte haben den Wunsch, dass sie bei ihrer klinischen Arbeit über alle behandlungsrelevanten Informationen verfügen und deshalb auch auf die von anderen Ärztinnen und Ärzten erhobenen für sie wichtigen Patientendaten zugreifen können. Gleichfalls wollen sie die von ihnen angefertigten Dokumentationen von medizinischen Behandlungen vor unberechtigtem Zugriff schützen. Sie wollen zum Wohle der Patientinnen und Patienten dokumentieren, sich durch die Dokumentation auch haftungsrechtlich absichern und gleichzeitig die Patientendaten rechtssicher verwalten oder sicher verwaltet wissen.

Technische Aspekte der kurz- und langfristigen elektronischen Datenspeicherung sind zentral für die Archivierung medizinischer Daten. Folgende Aspekte der Datenverwaltung stellen wichtige Bedrohungen dar: Hardware- und Softwareversagen, Kommunikationsprobleme im Netzwerk, Netzwerkprobleme, Kompatibilitätsprobleme zwischen Daten und Lesesoftware auf längere Sicht, Fehler der Systemadministratoren und anderer Nutzer, Naturkatastrophen (diese übrigens auch für alle anderen Dokumentationsformen), externe und interne Angriffe auf die Daten sowie ökonomische Krisen und Pleiten der Zulieferer von Hard- und Software, die zum Lesen und Verwalten der Daten notwendig sind [22].

Im Falle einer streng vertraulichen elektronischen Krankengeschichte stellt sich auch das Problem, dass die lesbaren Daten mit Meta- oder auch Verzeichnisdaten verknüpft sind, die sich an einer anderen Stelle befinden als die für den Nutzer sichtbare Datei. Diese Daten verschwinden nicht automatisch mit dem Löschen einer Krankengeschichte und enthalten in der Regel den Namen der oder des Behandelten [22]. Ein weiteres Problem ist das Löschen der Daten, das nur mit spezieller Software zu leisten ist. Das Problem der Dokumentenechtheit, also der nicht mehr abzuändernden Dokumentation, scheint gelöst.

Viele Ärzte machen sich Sorgen darüber, inwieweit sie für die elektronische Verwaltung der von ihnen erhobenen Daten verantwortlich sind. Nur wenige Medizinerinnen und Mediziner (der Autor ausgeschlossen) sind in der Informatik so bewandert, dass sie die Komplexität der elektronischen Datenverwaltung im Detail überblicken. Viele fragen sich, ob sie für Folgen möglicher struktureller Mängel des Datenmanagements Verantwortung tragen, wenn dadurch zum Beispiel vertrauliche Behandlungsdaten von unbefugten Dritten eingesehen werden können [23].

Arztrechtliche Grundlagen der Patientendatenverarbeitung in Zürich

Die Paragraphen 18 und 19 des kantonalen Patientinnen- und Patientengesetzes [24] regeln die Dokumentationspflicht der Behandelnden, die Aufbewahrungspflicht und das Einsichtsrecht der Behandelten. In §18 wird es dem Dokumentierenden freigestellt, ob die Dokumentation auf Papier oder elektronisch erfolgt. Die Erhebung der Daten setzt die Einwilligung des Behandelten voraus (§20). Die Behandelnden sind über diese Daten grundsätzlich zum Schweigen verpflichtet (§15). Die Möglichkeiten und Grenzen der Weitergabe von Informationen und Daten über eine medizinische Behandlung regeln die Paragraphen 13–16. Das Datenschutzgesetz der Schweiz deklariert diese Patientendaten im Artikel 3c als besonders schützenswerte Personendaten [25].

Verantwortung

Die Verantwortung für den Inhalt der ärztlichen Dokumentation und der Dokumentation der pflegerischen Massnahmen haben die behandelnden Ärztinnen und Ärzte [26]. Das ändert sich weder durch die Einführung der elektronischen Krankengeschichte noch durch die Arbeitsteilung zwischen Pflege- und Arztdienst [27, 28], wobei nicht ganz sicher ist, inwieweit die behandelnden Ärztinnen und Ärzte auch für die Daten verantwortlich sind, die im Rahmen des medizinischen Behandlungsprozesses von Mitgliedern anderer beteiligter Berufsgruppen erhoben werden, die vor dem Gesetz nicht als selbständige Leistungserbringer gelten [28, 29]. Klar ist aber, dass die Daten, die von im Gesetz beschriebenen Hilfspersonen der behandelnden Ärztinnen und Ärzte, also vor allem den Pflegenden, erhoben werden, ebenfalls der Geheimhaltungspflicht unterliegen [23]. Auch für das gesetzeskonforme Datenmanagement (eindeutige Zuordnung der einzelnen gespeicherten Daten zu den Personen, die die Daten erhoben haben, und zu den Personen, über die die Daten erhoben wurden), das Zugriffsmanagement (die Gestaltung der Vertraulichkeit durch die Regelung der Zugriffsrechte für Personengruppen im Gesundheitsbetrieb), das Netzmanagement (die Absicherung der elektronischen Übertragungswege) und das Revisionsmanagement (Langlebigkeit und Lesbarkeit) tragen die Ärzte die Verantwortung, sofern sie auch für die Organisation ihrer Arbeit

verantwortlich sind, wie zum Beispiel in einer eigenen Praxis. Inwieweit diese Verantwortung durch eine Produktehaftung des Herstellers der verwendeten Software abgedeckt ist, hängt nicht zuletzt davon ab, ob der niedergelassene Arzt den Empfehlungen folgt, die der Hersteller für den Einsatz seiner Software für das EDV-System in der Praxis gibt. Wenn Ärzte aufgrund einer Leistungsvereinbarung oder im Vertragsverhältnis für eine Institution ärztliche Leistungen dokumentieren und diese Institution nicht leiten, ist davon auszugehen, dass die Verantwortung für eine Verletzung des Datenschutzes oder anderer gesetzlicher Pflichten im Zusammenhang mit der medizinischen Dokumentation entsprechend den intern geregelten Verantwortlichkeiten und Kompetenzen zwischen der Organisation und der Ärzteschaft geteilt wird. Verletzungen des Datenschutzes, die aufgrund von strukturellen Mängeln im Datenmanagement sowie im Netz- und Revisionsmanagement entstehen, sind dabei wahrscheinlich als Verschulden der Institution zu werten. Diese Einschätzung leitet sich ab aus der Rechtspraxis zum Organisationsverschulden, basierend auf §55 des Schweizerischen Obligationenrechts [30, 31].

Empfehlungen

Die nachfolgenden Empfehlungen sollen insgesamt einen Weg aufzeigen, mit dem die Ärzte dem von allen Beteiligten gewünschten Austausch von Medizindaten besser vertrauen können.

Die grundsätzliche Empfehlung ist in diesem Zusammenhang, dass sich Ärztinnen und Ärzte, die für die Organisation ihrer Arbeit selbst verantwortlich sind und ein elektronisches Dokumentationssystem verwenden, bewusst machen, dass neben den traditionellen Pflichten im Zusammenhang mit der Vertraulichkeit der Daten auch eine Verantwortung für das gesetzeskonforme Datenmanagement, das Zugriffsmanagement, das Netzmanagement und das Revisionsmanagement entsteht. Ärzte in Institutionen, die sie nicht selbst leiten, können davon ausgehen, dass die Verantwortung für die letztgenannten Bereiche ausser dem Zugriffsmanagement von der Leitung des Gesamtunternehmens getragen wird. Die Ärzteschaft kann in diesem Fall, wie es zum Beispiel im Spital üblich ist, von dieser Verantwortung entlastet werden. Möglicherweise kann es vertrauensbildend wirken, wenn die Übernahme dieser Verantwortung in Leistungsvereinbarungen zwischen der Institution und den ärztlichen Diensten explizit erwähnt wird.

Die Vertraulichkeit der Patientendaten ist durch die Minimierung der Zugriffsrechte der Behandelnden auf das klinisch Notwendige zu gewährleisten. Die Papierkrankengeschichte war im Spital vornehmlich dem ärztlichen Dienst zugänglich. Im Zeitalter der elektronischen Krankengeschichte haben potentiell alle Behandelnden mit einem Zugang zum EDV-System rund um die Uhr Zugriff auf alle Behandlungsdaten. Dies erfordert eine neue und differenziertere Regelung der Zugriffsrechte und auch eine Veränderung der Kultur: Nur die Behandelnden des konkreten Patienten sollten einen stufengerechten Zugriff haben. Dabei soll im Vordergrund stehen, dass die Behandlungsqualität durch einen Zugriff anderer Berufsgruppen potentiell steigt. Für das Zugriffsmanagement ist am ehesten die Leitung des Arztdienstes verantwortlich, denn sie definiert in Zusammenarbeit mit den anderen Berufsgruppen das klinisch Notwendige.

Bei der Übermittlung besonders schützenswerter Personendaten müssen im Interesse des Absenders und des Empfängers die höchstmöglichen Sicherheitsstandards genutzt werden. Dies gilt insbesondere für die Übermittlung über das Internet. Wenn die verfügbare Technik sicher genug ist, um Bank- und Börsengeschäfte über das Internet abzuwickeln, ist auch eine ausreichende Sicherung von Patientendaten bei der Übermittlung zwischen Institutionen möglich. Die Verantwortung für das Netzmanagement liegt bei den an der Übermittlung beteiligten Partnerorganisationen einschliesslich des gewählten Netzbetreibers. Für die Auswahl dieser Partner einer Gesundheitsinstitution ist die Leitung des Gesamtunternehmens verantwortlich.

Zusammenfassung

Für eine zukunftsgerichtete Medizin mit optimal funktionierenden Behandlungsketten in modernen Versorgungsnetzwerken muss ein elektronischer Austausch von Behandlungsdaten geschaffen werden. Nur so kann dem Druck auf die moderne Medizin in Richtung einer Qualitätsverbesserung und einer Effizienzsteigerung begegnet werden. Auch die Auswertung aggregierter Patientendaten in Institutionen und Gesundheitsbehörden muss verbessert werden, um kurzfristiger über die Volksgesundheit Informationen zu gewinnen, Bedrohungen für die Gesundheit der Bürgerinnen und Bürger rechtzeitig zu erkennen und Angebotsstrukturen an den unterschiedlichen Bedarf an Gesundheitsleistungen in der Bevölkerung anzupassen.

In der Bevölkerung, also bei den potentiellen Patientinnen und Patienten, und auch bei vielen Ärztinnen und Ärzten besteht jedoch noch Misstrauen gegenüber der elektronischen Verwaltung und Weitergabe ihrer Behandlungsdaten.

Bei vielen Ärzten in der Praxis kommt neben den Sicherheitsbedenken die Befürchtung hinzu, die elektronische Datenverwaltung könne Mehrarbeit und -kosten verursachen [32].

Das Misstrauen entspricht nicht den wahren Bedrohungen, wenn die technischen Möglichkeiten der Informationstechnologie im Sicherheitsbereich ausgeschöpft werden und den Akteuren klar ist, wer für welche Bereiche des Datenmanagements Verantwortung trägt. Gemäss der Erfahrung des Autors mit elektronischen Dokumentationssystemen in der Klinik ist mittelfristig dadurch eine deutliche Zeitersparnis und durch die raschere Verfügbarkeit der Dokumentation eine grössere Behandlungsqualität möglich.

Literatur

1 Beggs-Baker S, et al. Legal issues and measures for protection of individual privacy in computerized health information systems. Lex Sci.1974;10(3): 90-104.

2 Boyer BB. Computerized medical records and the right to privacy: the emerging federal response. Buffalo Law Rev., 1975; 25(1):37-118.

3 Smith AW, Jones A. Computerizing medical records: legal and administrative changes necessary. Healthspan. 1991;8(11):3-6.

4 Field RI. Overview: computerized medical records create new legal and business confidentiality problems. Healthspan. 1994;11(8):3-7.

5 Reed K. Computerization of health care information: more automation, less privacy. J Health Hosp Law. 1994;27(12):353-68, 384.

6 Berger J. Patient confidentiality in a high tech world. J Pharm Law. 1996;5(1):139-45.

7 Byars WB. Legal challenges created by computerized medical records. Top Health Inf Manage. 1996;16(4):61-5.

8 McKenzie DJ. Medical records networking: banking on security. Infocare. 1996:34-5, 37-9.

9 Waller AA, Darrah JM. Legal requirements for computer security: electronic medical records and data interchange. Behav Healthc Tomorrow. 1996;5(1):45-7.

10 Turkington RC. Medical record confidentiality law, scientific research, and data collection in the information age. J Law Med Ethics. 1997;25(2-3): 113-29, 82.

11 Hussong SJ. Medical records and your privacy: developing federal legislation to protect patient privacy rights. Am J Law Med. 2000;26(4):453-74.

12 Shomaker TS, Ashburn MA. The legal implications of healthcare communications: what every pain physician needs to know. Pain Med. 2000;1(1): 89-96.

13 Kluge EH. Advanced patient records: some ethical and legal considerations touching medical information space. Methods Inf Med. 1993;32(2): 95-103.

14 Goldman B. Are medical computing and the law on a collision course? CMAJ. 1987;137(5):430-2.

15 Haugh R. Banking on privacy. Hospitals must protect patient information – and their own liability – as banks balk at HIPAA. Hosp Health Netw. 2004;78(2):50-4, 56, 2.

16 Steward M. Electronic medical records. Privacy, confidentiality, liability. J Leg Med. 2005;26(4): 491-506.

17 Krishna R, Kelleher K, Stahlberg E. Patient confidentiality in the research use of clinical medical databases. Am J Public Health. 2007;97(4):654-8.

18 Quantin C, Allaert FA, Fassa M, Riandey B, Avillach P, Cohen O. How to manage secure direct access of European patients to their computerized medical record and personal medical record. Stud Health Technol Inform. 2007;127:246-55.

19 Robeznieks A. Getting personal. Legal liability, patient-data overload among issues making physicians uneasy over emergence of personal health records. Mod Healthc. 2007;37(21):40-2.

20 Behlen FM, Johnson SB. Multicenter Patient Records Research: Security Policies and Tools. J Am Med Inform Assoc. 1999;6(6):435-43.

21 Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ. 2001;322(7281):283-7.

22 Gladney H. Preserving Digital Information. Berlin, Heidelberg, New York: Springer; 2007.

23 Honsell H. Die Verletzung des Berufsgeheimnisses bei der Heiltätigkeit. In: Honsell H (Hrsg.). Handbuch des Arztrechts. Zürich: Schulthess; 1994. S. 339-61.

24 Patientinnen- und Patientengesetz des Kantons Zürich. 2004, Kanton Zürich; Schweiz.

25 Bundesgesetz über den Datenschutz (DSG). 1992.

26 Fellmann W. Arzt und das Rechtsverhältnis zum Patienten. In: Kuhn W, Poledna T (Hrsg.). Arztrecht in der Praxis. Zürich: Schulthess; 1997. S. 103-231.

27 Kuhn W, Poledna T (Hrsg.). Arztrecht in der Praxis. Zürich: Schulthess; 1997.

28 Landolt H. Rechtliche Herausforderungen an die Pflegewissenschaft. Managed Care. 2005;6:22-3.

29 Deutsch E. Schweigepflicht des Arztes. In: Deutsch E (Hrsg.). Medizinrecht – Arztrecht, Arzneimittelrecht und Medizinprodukterecht. Berlin, Heidelberg: Springer; 1999. S. 262-69.

30 Heine G. Organisationsverschulden aus strafrechtlicher Sicht: Zum Spannungsfeld von zivilrechtlicher Haftung, strafrechtlicher Geschäftsherrenhaftung und der Strafbarkeit von Unternehmen. In: Niggli MA, Amstutz M (Hrsg.). Verantwortlichkeit im Unternehmen: Zivil- und strafrechtliche Perspektiven. Basel: Helbing & Lichtenhahn; 2007. S. 93-125.

31 Kuhn H. «It is forbidden to crash this airplane». Critical Incident Reporting Systeme und Recht – Lehren aus den USA und aus der Luftfahrt1. In: Poledna WF, Poledna T (Hrsg.). Die Haftung des Arztes und des Spitals. Reihe Forum Gesundheitsrecht. Zürich: Schulthess; 2003. S. 181-232.

32 SGAM. Positionspapier E-Health. PrimaryCare. 2006;6(37):643-44.