Gesetzliche Rahmenbedingungen der Telemedizin

B. Schütze [1)], T. J. Filler [2)]
1) Johannes Gutenberg-Universität Mainz, Klinik und Poliklinik für Radiologie
2) Universitätsklinikum Münster, Institut für Anatomie / Klinische Anatomie

Der Nutzwert telematischer Anwendungen in der Medizin wurde schon mehrfach beschrieben, z. B. in der Pathologie oder auch bei der Interaktion mit dem Patienten (1,10). In Deutschland werden die größten Erwartungen an die Telemedizin jedoch mit der Interaktion der jeweiligen Partner durch den Aufbau eines verzahnten Gesundheitsnetzwerkes verbunden (4). In diesem haben die vernetzten Partner bei der Patientenbehandlung die Möglichkeit, eine gemeinsame Datenbasis bzgl. der angefallenen Patientendaten zu nutzen. Beim Aufbau dieses Gesundheitsnetzwerkes gilt es natürlich die bestehenden gesetzlichen Bestimmungen zu beachten.

Arztgeheimnis und Datenschutz

Die zentrale Aussage der deutschen Datenschutzgesetze ist im Prinzip identisch: es existiert ein generelles Verbot der Datenerhebung, es sei denn, dass eine andere Rechtsvorschrift die Datenerhebung erlaubt oder sogar anordnet. Dies ist beispielsweise durch das Gesetz zur Modernisierung der Krankenversicherung (GMG) der Fall: nach § 295 Abs. 4 GMG dürfen künftig die „an der vertragsärztlichen Versorgung teilnehmenden Ärzte, ärztlich geleiteten Einrichtungen und medizinischen Versorgungszentren“ nur noch „im Wege elektronischer Datenübertragung oder maschinell verwertbar auf Datenträgern“ abrechnen (5).

Eine der Konsequenzen aus den bestehenden Datenschutzgesetzen ist, dass die bei der Behandlung anfallenden Patientendaten nur digital erfasst und bearbeitet werden dürfen, wenn der Patient nach einer den gesetzlichen Bestimmungen genügenden Aufklärung rechtsverbindlich darin eingewilligt hat. Das Bundesdatenschutzgesetz sieht die Daten im Gesundheitswesen als besonders schützenswert an. Daher ist für die Übermittlung dieser Daten mittels digitaler Methoden ein entsprechender Schutz anzuwenden. Für die Einhaltung der betreffenden Datenschutzgesetze ist dabei die Stelle und die Person verantwortlich, bei der die personenbezogenen Daten erhoben und digital gespeichert bzw. verarbeitet werden (i. d. R. der behandelnde Arzt).

Das Arztgeheimnis findet als eines der ältesten Datenschutzgesetze in der Geschichte in der deutschen Rechtssprechung auch eine entsprechende Berücksichtigung (12). In §9 Abs. 1 der Musterberufsordnung für Ärzte (MBO) wird vorgeschrieben, dass der Arzt über das, was ihm in seiner Eigenschaft als Arzt anvertraut worden ist, zu schweigen hat. §9 Abs. 3 (MBO) fordert den Arzt auf, seine Mitarbeiter zur Verschwiegenheit zu verpflichten. Dieses Satzungsrecht wird durch §203 Abs.1 des Strafgesetzbuches (StGB) bestätigt. Danach wird jeder Arzt, der unbefugt ein fremdes, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbart, das ihm als Arzt anvertraut oder sonst bekannt gegeben worden ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Standesrechtlich kann die Verletzung der ärztlichen Schweigepflicht sogar zum Widerruf der ärztlichen Approbation führen.

Für den behandelnden Arzt und dem entsprechend tätig werdenden Personenkreis gilt nach § 53 Abs. 2.1 Strafprozessordnung (StPO) ein Zeugnisverweigerungsrecht und ergänzend hierzu ein Beschlagnahmeverbot nach § 97 Abs.1 der StPO, so dass der Arzt über die ihm während einer Patientenbehandlung anvertrauten Daten das Arztgeheimnis wahren kann. Aus diesem Beschlagnahmeverbot ergibt sich zudem aus § 103 Abs.1 StPO ein eingeschränktes Durchsuchungsrecht für Arztpraxen. Das Beschlagnahmeverbot nach § 97 StPO gilt jedoch nur, wenn sich die geschützten Gegenstände bzw. Daten im Gewahrsam des Arztes, d. h. innerhalb der Räumlichkeiten der ärztlichen Tätigkeit, befinden und der Arzt diese Gegenstände (Daten) aufgrund des Vertrauensverhältnisses zwischen Arzt und Patient erlangt hat: der Arzt muss die tatsächliche „Sachherrschaft“ ausüben. Eine Ausnahme von dieser Regel ist im „Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG) vorgesehen: werden medizinische Daten auf der noch einzuführenden elektronischen Gesundheitskarte gespeichert so ist der Zugriff auf diese Daten nach in § 291a Absatz 4 und 5 beschränkt.

Haftungsfragen beim Einsatz der Telemedizin

Bei der Frage nach der ärztlichen Haftung beim Einsatz der Telemedizin muss zwischen dem Organisationsverschulden und der Haftung als Konsiliararzt unterschieden werden.

Die Telemedizin fordert eine gesteigerte Koordination der Zusammenarbeit, wo bisher überwiegend eine Einzelverantwortung vorherrschte. Grundsätzlich lässt sich

Autoren: B. Schütze, T. J. Filler
Titel: Gesetzliche Rahmenbedingungen der Telemedizin
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2005
Seite: 68-71

zur Problematik Organisationsverschulden im Rahmen ärztlicher Behandlung festhalten, dass sich alle ärztlichen Verstöße gegen die zum Schutz des Patienten bestehenden organisatorischen Pflichten als Behandlungsfehler bezeichnen lassen (7, 13). Die Rechtsprechung stellt dementsprechend auch hohe Anforderungen an die Sorgfalt im organisatorischen Bereich: der Zustand der Organisation muss dem Standard des Krankenhauses sowie den typischen Aufgaben entsprechen. Allgemein kann gesagt werden, dass Hochschulkliniken dabei höheren Ansprüchen genügen müssen als kleinere, weniger differenzierte Kliniken (13).

Im Vordergrund der organisatorischen Pflichten stehen die Überwachung des nach geordneten Personals und die Organisation der einzelnen Betriebsabläufe in Diagnostik und Therapie in einer Art und Weise, dass jede denkbare Gefährdung eines Patienten ausgeschlossen ist. Für den telemedizinisch tätigen Arzt bedeutet dies, dass er sich nicht darauf verlassen darf, dass die von ihm eingesetzten Geräte – insbesondere die eingesetzten EDV-Lösungen – fehlerfrei arbeiten, sondern er muss von sich aus eine regelmäßige Sicherheitskontrolle durchführen. Anders ausgedrückt: um ein Organisationsverschulden zu vermeiden muss sich der Arzt aktiv darüber versichern, dass die von ihm eingesetzten Geräte bzw. die eingesetzte EDV ordnungsgemäß, d. h. entsprechend den Herstellervorschriften und dem gegenwärtigen Stand der Technik entsprechend gewartet und diese Wartung dokumentiert wird, und der Arzt so von einer bestimmungsgemäßen Funktion der eingesetzten Gerätschaften ausgehen darf. Unterlässt der Arzt diese Kontrolle bzw. kann diese Kontrolltätigkeit nicht nachweisen und kommt es durch den Einsatz entsprechend fehlerbehafteter Systeme zu Schaden verursachenden Konsequenzen, ist von einer haftungsbegründeten Sorgfaltspflichtverletzung des Arztes regelmäßig auszugehen (13). Für Kommunikations- und Organisationsfehler können aber auch die Hersteller der (EDV-) Systeme entsprechend den Grundsätzen der Produkt- bzw. Herstellerhaftung zur Verantwortung gezogen werden.

Aus organisationsrechtlichen Gesichtspunkten sind auch die weiter oben besprochenen Themen Datenschutz und Schweigepflicht/-recht zu berücksichtigen. Hier sollte der Arzt sich vor dem Einsatz der (EDV-) Systeme von der Existenz der (schriftlichen) Erklärung der Systemhersteller überzeugen, dass durch den Einsatz der Systeme die geltenden gesetzlichen Bestimmungen beachtet werden. An dieser Stelle sei nur noch einmal auf die Problematik der Wartung der Systeme durch den Hersteller hingewiesen, bei der die Wartungsarbeiter der Herstellerfirma häufig Einblick in die Daten von behandelten Patienten erhalten, was selbstverständlich schon eine Verletzung der ärztlichen Schweigepflicht wie auch der entsprechenden Datenschutzgesetze bedeutet (5, 7).

Bei den in Deutschland eingesetzten Bereichen der Telemedizin sind der bzw. die telemedizinisch tätigen Ärzte Konsiliarärzte, da sie nicht selbst die Behandlung übernehmen. Nur wenn der Telemediziner die Therapie festlegt und als der steuernde Experte erscheint, ist er Mitbehandler und nicht Konsiliarius (11).

Zivilrechtlich ist der Konsiliararzt für eigene und fremde Fehler haftbar (9, 11). Bei eigenem Fehlverhalten (z.B. Fehldiagnose, fehlerhafte Anweisung, usw.) haftet der telemedizinisch tätige Arzt, wenn sein Fehler ein schuldhafter Sorgfaltspflichtverstoß und kausal für den Schaden war. Der primär behandelnde Arzt handelt jedoch nach seiner eigenen ärztlichen Entscheidung, wodurch der behandelnde Arzt zusammen mit dem Konsiliarius gemeinsam gesamtschuldnerisch haftet (11).

Der Konsiliarius haftet nicht für von ihm gegebene Ratschläge, wenn der Primärbehandler ihm unrichtige Daten vorgelegt hat – ausgenommen, der Konsiliararzt konnte erkennen, dass die vorgelegten Daten fehlerhaft oder unvollständig sind, z. B. Laborwerte, die mit dem Leben des Patienten nicht vereinbar wären. Hier haftet der Konsiliararzt nur im Rahmen seiner eigenen Pflichtverletzung; er hätte erkennen müssen, dass die Daten falsch bzw. unvollständig sind.

Der Konsiliararzt haftet für fremdes Verschulden, wenn er eine eigene vertragliche Beziehung zum Patienten hat und daher für ein Verschulden seiner Erfüllungsgehilfen einstehen muss. Z. B. haftet ein Laborarzt dafür, wenn die MTA das Blut zweier Patientinnen verwechselt und daher dem Patienten falsche Laborwerte zugeordnet werden. Der Primärbehandler ist jedoch kein Erfüllungsgehilfe des Konsiliarius.

Unterlassene Hilfeleistung?

Bei der strafrechtlichen Betrachtung der Telemedizin muss auch noch der § 323c StGB („unterlassene Hilfeleistung“) Beachtung finden. So stellt sich, wenn in einem telemedizinischen Verbund aus irgendwelchen Gründen eine Dienstleistung nicht erbracht werden kann, die Frage, ob ein anderer telemedizinischer Spezialist, der zwar das technische Equipment hat, jedoch mit dem Primärbehandler in keinem vertraglichen Beziehung steht, die Dienstleistung bei einem Notfall erbringen muss? In der Literatur wird dies bejaht, da „die Hilfspflicht auch einen Abwesenden, insbesondere einen um Hilfe Angerufenen“ treffen kann (11).

Teleradiologie

Einen Sonderfall in der Telemedizin nimmt die Teleradiologie ein, die als erste telemedizinische Anwendung in der Röntgenverordnung (RöV) rechtlich verbindliche Bestimmungen für ihren Einsatz hat, d. h. ein anderer teleradiologischer Einsatz als der Festgeschriebene erfolgt widerrechtlich (3, 8). Die Voraussetzungen für den Einsatz der Teleradiologie in einem bestimmten Versorgungsgebiet sind

- eine geringe Versorgungsdichte mit Radiologen in dem jeweiligen Gebiet,
- ein krankheitsbedingter Ausfall des Fachkundigen,
- die Notfallversorgung von Nicht-Akutkrankenhäusern und
- weniger als 5 teleradiologische Untersuchungen je Tag.

Sind alle diese Bedingungen erfüllt, gibt es grundlegende Anforderungen an das Management zum Betreiben einer teleradiologischen Einrichtung:

- die Übertragungszeit der Bilddaten beträgt maximal 5 bis 10 Minuten
- es erfolgt eine sofortige Befundung
- die Befundungsgrundlage sind alle

Bilder einer Untersuchung – im Bereich der Nicht-Notfall-Diagnostik einschließlich aller Voruntersuchungen
- alle notwendigen klinischen Informationen liegen dem Befundenden vor
- der teleradiologisch tätige Arzt befindet sich in einer Entfernung vom Untersuchungsort, die in maximal 15 Minuten zurückgelegt werden kann.

Auch im Bereich des Einsatzes der „Humanressourcen" gibt die RöV jetzt klare Vorgaben. Damit Teleradiologie betrieben werden kann, muss das eingesetzte Team mindestens folgende Kenntnisse aufweisen:

- der teleradiologisch tätige Arzt hat die volle Fachkunde,
- der Arzt vor Ort besitzt Kenntnisse im Strahlenschutz, d. h. er hat wenigstens einen 24-Stunden-Kurs oder einen Grund- und Spezialkurs absolviert; weiterhin wird er wahrscheinlich vier Wochen praktische Erfahrung im radiologischen Einsatz nachweisen müssen und
- die technische Durchführung vor Ort darf nur von einer MTRA bzw. MTA durchgeführt werden.

Arzthelferinnen, die auch im „normalen" Einsatz in der Radiologie nur unter Aufsicht arbeiten dürfen, sind damit vom Einsatz in der Teleradiologie ausgeschlossen. Dies bedeutet für den Betreiber der Einrichtung, eine entsprechende Redundanz im Personalstamm haben zu müssen. Damit die Mustergenehmigung zum Betreiben einer teleradiologischen Einrichtung erteilt werden kann, sind weitere organisatorische Anforderungen zu erfüllen:

- es existiert ein Kooperationsvertrag zwischen dem Betreiber der Röntgeneinrichtung und dem teleradiologisch tätigen Arzt, der die Verantwortlichkeiten und Weisungsbefugnisse regelt,
- es existieren am Ort der Untersuchungen entsprechende (schriftliche) Arbeitsanweisungen, die auch dem teleradiologisch tätigen Arzt bekannt sind,
- die Datenleitung und die Befundungsmonitore sind entsprechend den geltenden Bestimmungen von der Ordnungsbehörde abgenommen und
- es erfolgt eine monatliche Qualitätssicherung von Befundungsmonitoren und Bildübertragung durch „Dummy"-Aufnahmen

Damit ist die Radiologie die erste medizinische Disziplin, die ihre telemedizinische Anwendung explizit unter Einhaltung von verbindlichen Regeln erlaubt.

E-Mail-Einsatz in der Telemedizin

Für die Übermittlung medizinischer Daten, z. B. Befunde und Bilddaten mittels E-Mail resultiert aus den rechtlichen Rahmenbedingungen die Forderung, dass die Daten mit sicheren kryptographischen Methoden verschlüsselt werden müssen, sobald öffentliche Übertragungsmedien benutzt werden.

Dabei ergibt sich, dass die Verschlüsselung der medizinischen Nutzdaten durch eine schnelle symmetrische Verschlüsselung erfolgen sollte. Zur Nutzung von Public-Key-Verfahren kann nach Ansicht der Autoren nicht geraten werden, da nach deutschem Recht der private Schlüssel beschlagnahmt werden und damit das Schweigerecht / die Schweigepflicht des Arztes nicht länger aufrecht gehalten werden kann (17). Diese rechtlichen Bedenken werden sich nach den bisherigen Erkenntnissen mit der bundesweiten Einführung des elektronischen Arztausweises (Health Professional Card, HPC) ändern, so dass dieser Arztausweis und die dazu gehörende Public Key Infrastructure (PKI) zur sicheren Datenverschlüsselung genutzt werden können (2, 18).

Gleiches gilt für die Einführung der elektronischen Gesundheitskarte entsprechend dem §291 Absatz 2a (Kapitel 10) des GMG, die allen Krankenversicherten ab dem 01. Januar 2006 zur Verfügung stehen soll (2, 3). Die Gesundheitskarte soll als Mikroprozessorkarte ausgestaltet werden, welche die Authentifizierung (elektronische Identitätsprüfung) sowie die Nutzung von Verschlüsselung und elektronischer Signatur ermöglicht, wenngleich es dem jeweiligen Bürger überlassen bleibt, ob er die Funktionalität der digitalen Signatur auf seine eigenen Kosten frei schalten lässt.

Für andere Bereiche der Telemedizin wie z. B. der Bestellung von medizinischem Material mittels des Internets eignen sich Public-Key-Verfahren schon heute sehr gut, wenn auch der Aufwand für die Implementierung einer eigenen PKI nicht unterschätzt werden sollte (19).

Datenfernabfrage aus medizinischen Informationssystemen

Um die Sicherheitsanforderungen der Datenübertragung bei der Abfrage von medizinischen Informationssystemen zu erfüllen, müssen kryptographische Methoden zum Einsatz kommen, welche die Sicherheit der Datenintegrität und der Vertraulichkeit der übertragenen Daten gewährleisten sowie eine digitale „Quittierung" der übermittelten Daten ermöglichen. Hierzu zählt

- die Integritätssicherung
- der Schutz der Vertraulichkeit durch Verschlüsselung der übertragenen Daten
- die Quittierung des Empfangs
- die Erkennung wieder eingespielter manipulierter Nachrichten.

Die vorgenannten Maßnahmen sichern nicht die eingesetzten Rechner bzw. die Datenbank mit den medizinischen Nutzdaten vor unbefugten Manipulationen. Hier ist die einzige Möglichkeit zur Verhinderung von Manipulationen der Einsatz eines Content-Security-Systems (6) wobei dieser Einsatz von Methoden zur Absicherung des internen Netzwerkes (Security Policies, Anti-Viren-Systemen, Desktop-Firewalls) begleitet werden muss.

Diese Prinzipien werden auch bei dem Projekt „akteonline" der Gesakon GmbH erfüllt. Die „akteonline" ist als eine über das Internet erreichbare elektronische Gesundheitsakte konzipiert, wobei die erste Stufe dieses Projektes in Zusammenarbeit mit dem Institut für Medizinische Informatik und Biomathematik des Universitätsklinikum Münster entwickelt wurde (15, 16). Bei diesem Projekt werden die elektronisch hinterlegten Patientendaten durch mehrere Sicherheitsmechanismen geschützt:

- die Übertragung der Daten erfolgt durch eine 128-Bit- Verschlüsselung,
- die Patientendaten werden verschlüsselt abgelegt,
- es erfolgt eine direkte Zugriffskontrolle, d. h. der Patient hat die volle Kontrolle darüber, wer außer ihm selbst auf seine gesamte Akte oder von ihm festgelegte einzelne Bestandteile der Akte zugreifen kann.

Hier ist der – aus der Sicht eines Datenschützers – ideale Zustand erreicht: der Patient bestimmt selbst, wer seine Daten einsehen darf (Siehe auch: „Die elektronische Gesundheitsakte in internationaler Kooperation: Aufruf zur Zusammenarbeit“, Seite 33.

Literatur

1. Brenner G. Spezielle Anwendungen in der Gesundheitstelematik. Z. ärztl. Fortbild. Qual.sich.(ZaeFQ) 2001; 95: 646 – 651
2. Bundesministerium für Gesundheit und Soziales [Online]. 2003 [zitiert 2003 November 25]; Verfügbar unter: http://www.bmgs.bund.de/deu/gra/themen/gesundheit/geskarte/index_2011.cfm
3. Filler TJ, Schütze B, Geisbe T, Grönemeyer DHW. Röntgenverordnung: Wesentliche Neuerungen vorgesehen. Deutsches Ärzteblatt 2002; 99/49: A3309-3310
4. Geisthoff UW, Federspil PA, Sittel C, Plinkert PK. Telemedizin: Interaktionen zwischen Klinik und Praxis. HNO 2002; 50:812 – 821
5. Krüger-Brand H. Aus für EDV-Muffel. Deutsches Ärzteblatt 2003; 40: A-2541 / B-2117 / C-1993
6. Pommering K. Klinischer Datenschutz und Internet. Zentralbl Gynakol 2000; 122: 291 - 294
7. Quade G, Flimmers R, Müller J, Molitor E. Datenschutz: Fernwartung medizinischer EDV-Systeme. Deutsches Ärzteblatt 2002; 23: B1360 - B1363
8. Schütze B, Kroll M, Geisbe T, Grönemeyer DHW, Filler TJ. Anforderungen der Röntgenverordnung an die Radiologie. Deutsches Ärzteblatt 2003; 28/29:A1915
9. Stellpflug MH. Internationales Haftungsrecht. Z. ärztl. Fortbild. Qual.sich.(ZaeFQ) 2001; 95: 615 – 618
10. Terpe HJ, Müller W, Liese A, Vogel CU, Broer KH. Schnellschnitttelepathologie im klinischen Alltag eines Brustzentrums. Pathologe 2003; 24: 150-153
11. Ulsenheimer K, Erlinger R. Die Haftung als Konsiliararzt. Z. ärztl. Fortbild. Qual.sich.(ZaeFQ) 2001; 95: 609 – 615
12. Vetter R. Datenschutzrechtliche Aspekte der Telemedizin. Z. ärztl. Fortbild. Qual.sich.(ZaeFQ) 2001; 95: 662 – 666
13. Wienke A. Organisationsverschulden bei vernetzten Strukturen. Z. ärztl. Fortbild. Qual.sich.(ZaeFQ) 2001; 95: 629 – 632
14. Das Teleradiologie-Projekt Rhein-Neckar-Dreieck [Online]. 2004 [zitiert 2004 Februar 09]; Verfügbar unter: http://www.teleradiologie-rnd.de/
15. Akte Online [Online]. 2004 [zitiert 2004 Februar 09]; Verfügbar unter: http://www.akteonline.de
16. Akte Online [Online]. 2004 [zitiert 2004 Februar 09]; Verfügbar unter: http://akteonline.uni-muenster.de/perl/webseiten/webseiten.pl?idp=2&idk=6
17. Schütze B, Geisbe T, Grönemeyer DHW, Filler TJ (2002) Sicherer elektronischer Datenaustausch durch electronic Mail. In: Steyer G, Löhr KP, Tolxdorff T (Hrsg.). Telemed 2002 - Tagungsband zur 7. Fortbildungsveranstaltung und Arbeitstagung, ; ISBN 3-9808-6530-4; S 203-212
18. Goetz C (2001) Sichere e-mail zwischen Ärzten. Z. ärztl. Fortbild. Qual.sich.(ZaeFQ) 95: 652 – 656

19. Brandner R, van der Haak M, Hartmann M, Haux R, Schmücker P (2002) Electronic Signature for Medical