

Jürgen Müller

Regierungsdirektor beim
Bundesbeauftragten für den Datenschutz

Datenschutz und Telematik im Gesundheitswesen am Beispiel Elektronisches Rezept und Elektronische Patientenakte

Vortrag im Rahmen des eHealth-Kongresses
Telematik im Gesundheitswesen am 6. März 2002 in Bonn

Es gibt wenige Bereiche im Leben eines Menschen, und zwar im Leben eines jeden Menschen, die ihn so sehr berühren wie seine eigene Gesundheit. Hierbei handelt es sich im Regelfall Gott sei Dank um kleinere Maläsen, die aber gleichwohl unser Wohlbefinden beeinträchtigen. Manchmal jedoch sind es auch Krankheiten, die über Leben und Tod bestimmen. Deswegen brauchen wir einerseits Hilfe, Zuwendung und Zuspruch bei Krankheit und wollen andererseits gerade hier selbst darüber bestimmen können, wer was unter welchen Umständen über unsere Gesundheit erfährt.

Die Entwicklung der Informationstechnik im Gesundheitsbereich ist somit ein zentrales Anliegen unserer Gesellschaft und bedarf der Unterstützung, Förderung und Bündelung aller Kräfte. Nur so ist der Qualitätsgewinn zu erreichen, den der Einsatz von Informationstechnik verspricht. Ich denke hierbei insbesondere an den schnelleren Zugang zu wichtigen Informationen über medizinische Untersuchungen und Forschungen, die den Ärzten zeitraubende Nachforschungen ersparen. Zeit, die damit den Patienten zugute kommt. Oder es geht schlicht und einfach um die Kommunikation zwischen den behandelnden Ärzten, wenn der Patient von seinem Hausarzt an den Facharzt überwiesen worden ist oder dieser wiederum den Patienten zur Durchführung einer Operation in ein Krankenhaus überweist. Hier lassen sich un-

schwer eine Reihe von Erleichterungen vorstellen, die Zeit ersparen und eine bessere Qualität der Informationen versprechen.

Die Bedeutung des Datenschutzes genießt in diesem Zusammenhang einen hohen Stellenwert. Ich habe es bereits eingangs angesprochen, was diesen Stellenwert charakterisiert: Jeder von uns ist betroffen, der eine mehr, der andere weniger, aber keiner von uns kann abschätzen, ob und wann sich der Grad der Betroffenheit ändert. Zudem handelt es sich um sensible Daten, die für den Einzelnen von derart hoher Bedeutung sind, dass er nun wirklich ganz alleine entscheiden will, mit wem er das Wissen, ja ich sage besser „das Geheimnis“ um diese Daten teilen will. Nicht ohne Grund gehört zu den ältesten Berufsregeln der menschlichen Gesellschaft die Berufspflicht des Arztes, zu helfen und – ich betone – zu schweigen. Der Datenschutz will und muss zu einem Umgang mit personenbezogenen Daten beitragen, der den berechtigten Interessen der Betroffenen auf Selbstbestimmung gerecht wird. Eingriffe in dieses Recht, auch wenn sie im Interesse des Gemeinwohls liegen, sind möglichst gering zu halten. Anders als ich dies gelegentlich in anderen Bereichen feststelle, wollen hier alle Beteiligten, dass der Datenschutz diese Aufgabe wahrnimmt und sie zeigen sich bereit, seinen Rat zu beachten. Denn es gilt eine ganze Reihe von möglichen Problemen oder Gefahren zu erkennen und zu minimieren oder auszuschließen, die sich bei der Anwendung neuer informationstechnischer Verfahren stellen.

Nehmen wir als Beispiel das Rezept, und ich meine jetzt das herkömmliche Papierrezept. Wenn bislang der Patient von seinem behandelnden Arzt zum Abschluss der Behandlung das Rezept ausgehändigt bekommt, so hat nur er und der Arzt Kenntnis vom Inhalt des Rezepts. Ob und wann das Rezept eingelöst wird, liegt in der Hand des Patienten und keiner außer ihm kann später nachvollziehen, wie er mit diesem Rezept umgegangen ist. Anders sieht die Situation bei einem elektronischen Rezept aus. Hier werden Daten gespeichert, ob auf einer Chipkarte oder einem Server, hier weiß der Patient nicht, wer alles auf diese Daten zugreifen kann. Vereinfacht ausgedrückt: Hier fehlt schlicht und einfach die Transparenz für den Patienten, was bei ihm zu einer Verunsicherung führt. Er weiß nicht, wer eventuell „sein Rezept“ einsehen kann, es gegebenenfalls kopieren kann, oder auch den Verlauf des Rezeptes nach-

vollziehen kann, also ob und wann die entsprechende Verordnung in einer Apotheke eingelöst wurde.

Vor dem Hintergrund des allgemeinen Misstrauens gegenüber dem Einsatz neuer Techniken kommt es entscheidend auf die Akzeptanz bei den Menschen an, sowohl bei den sogenannten Betroffenen, aber auch bei denjenigen, die den Einsatz der neuen Techniken propagieren und umsetzen. Es wird entscheidend darauf ankommen, wie man den hilfeschuchenden Patienten durch die informationstechnische Verarbeitung ihrer Gesundheitsdaten besser helfen kann, ohne dabei das Arztgeheimnis generell oder im Einzelfall zu gefährden. Die Bürger müssen sich mit ihren Daten im Netz eines modernen Gesundheitswesens geborgen fühlen, sie dürfen sich nicht als Objekte fühlen, die in diesem Netz gefangen sind. In einer hoch entwickelten Demokratie wie der unserigen wird dies über Erfolg oder Misserfolg des Einsatzes von Informationstechnik im Gesundheitswesen entscheiden.

Über eines müssen wir uns im Klaren sein: Jede unzulässige Verarbeitung von Gesundheitsdaten schädigt nicht nur den jeweils unmittelbar Betroffenen, sondern sie kann auch das notwendige Vertrauen in die generelle Wahrung des Arztgeheimnisses untergraben. Deshalb möchte ich an dieser Stelle drei berufsrechtliche Einschränkungen hervorheben, deren Einhaltung besondere Beachtung zu widmen ist und die – wie auch die folgenden Ausführungen – gleichermaßen für das elektronische Rezept und die elektronische Patientenakte gelten:

1. Daten eines Patienten dürfen nur weitergegeben oder zugänglich gemacht werden, wenn es dem Patienten nicht schadet, sondern nützt, insbesondere also wenn es seine Behandlung fördern kann.
2. Die ärztliche Schweigepflicht gebietet, Daten eines Patienten – auch für seine weitere Behandlung – nur mit seiner Einwilligung weiterzugeben, wobei sich derzeit die Einwilligung z.B. dann konkludent aus dem Verhalten des Patienten ergibt, wenn ein anderer Arzt die Behandlung übernimmt oder daran beteiligt wird und der Patient keinen Einwand gegen die dabei sinnvolle und übliche Datenweitergabe erhebt.
3. Die weiterzugebenden Daten dürfen außer dem Arzt, für den sie bestimmt sind, nur dessen berufsmäßigen Gehilfen, soweit das erforderlich ist, und dem

Patienten selbst bekannt werden, außer wenn darin eine Gefährdung für ihn läge.

Diese berufsrechtlichen Vorgaben gilt es beim Einsatz der Informationstechnik einzuhalten und ihre Umsetzung bedarf einem Bündel von besonderen Maßnahmen. Nach meinem Dafürhalten besteht unter allen, die an dieser Entwicklung beteiligt sind, Einvernehmen über dieses Ziel, so dass die dafür einzusetzende Arbeit eine gute Investition ist.

Meine Damen und Herren, die aus Sicht des Datenschutzes entscheidende Frage ist die der Freiwilligkeit. Der Patient ist Herr seiner Daten und das muss auch so bleiben. Das bedeutet, dass ihm bei Freiwilligkeit der Teilnahme an einem Projekt das Recht der vollständigen Einsichtnahme, der notwendigen Ergänzung oder der Löschung von Daten eingeräumt werden muss, soweit nicht gesetzliche Vorschriften dies ausschließen. Wir reden hier über den von allen Seiten gewünschten „aufgeklärten“ Patienten. Ihn gilt es ernst zu nehmen. Wenn wir dies tun, so muss er auch das Recht haben zu entscheiden, welche seiner medizinischen Daten aufgenommen werden und wem er die Daten im Einzelfall zugänglich machen will. Ich bin fest davon überzeugt, dass man bei einer strikten und konsequenten Beibehaltung des Grundsatzes der Freiwilligkeit die Akzeptanz innerhalb der Bevölkerung gewinnen wird. Und man wird m.E. ein Ziel erreichen, um das es ja allen geht: Es werden die Vorteile für alle Beteiligte die zugegebenermaßen auch nicht auszuschließenden Nachteile überwiegen. Die Patienten, die aufgrund ihrer Erkrankungen am häufigsten einen Arzt konsultieren müssen, seien es nun die chronisch Kranken oder Behinderter, werden den größten Nutzen haben. Sie werden den Prozentanteil der Bevölkerung, der vielleicht so gut wie nie krank ist oder der sich einfach aus prinzipiellen Erwägungen, ja fast möchte ich ideologischen Erwägungen sagen, jedem Fortschritt in den Weg stellt, in den zu vernachlässigenden Hintergrund drängen. Oder, warum sollte man dies von vorneherein ausschließen, vielleicht ergibt sich eine Sogwirkung auch für diesen Personenkreis, wenn er sieht, dass er an diesem Verfahren teilnehmen kann, es aber nicht muss.

Wenn ich an dieser Stelle den Begriff „Verfahren“ benutze, dann ist es nur ein kleiner Schritt zum Thema Datensicherheit und damit zum technologischen Datenschutz.

Die Risiken für Datenschutz und Datensicherheit liegen im Wesentlichen auf dem Transportweg, auf dem die Daten übertragen werden. Dabei sind diese technischen Bedingungen den beteiligten Ärzten oftmals nicht bekannt, geschweige denn, dass sie von ihnen beeinflusst werden können. Deshalb ist es nicht auszuschließen, dass die übertragenen Daten unterwegs verfälscht oder von unbefugten Dritten angesehen werden können. Diese Risiken mögen gering sein, sie dürfen aber nicht völlig vernachlässigt werden. Und weil auch in diesem Bereich Maßnahmen zum absoluten Schutz kaum möglich sind, muss das Augenmerk auch auf die Reduzierung des möglichen Schadens gerichtet werden. Der Schaden einer Verfälschung lässt sich durch das Hinzufügen einer digitalen Signatur des jeweiligen Absenders der Daten wirksam begrenzen. Denn dadurch kann der Empfänger jede Verfälschung mit extrem hoher Sicherheit bemerken und bei Bedarf eine erneute Übertragung der Daten anfordern. Zugleich wird damit die Verantwortung für die Richtigkeit der jeweiligen Daten deutlich gemacht. Der rechtliche Rahmen für solche Verfahren ist mit dem Signaturgesetz und der Signaturverordnung vorhanden, so dass einer regelmäßigen Anwendung derartiger Verfahren nichts im Wege stehen dürfte.

Die unbefugte Kenntnisnahme schädigt das Interesse des Patienten an der Geheimhaltung seiner Gesundheitsdaten. Dieser Schaden lässt sich vermeiden, indem nur solche Daten übertragen werden, die nicht erkennen lassen, um wessen Gesundheitsdaten es sich handelt. Dies lässt sich dadurch erreichen, dass die Daten – auf den Patienten bezogen – anonym übertragen werden. Darüber hinaus müssen die Daten verschlüsselt übertragen werden.

Wenn ich mich jetzt zuletzt mit Fragen der Erstellung und Übertragung der Datensätze befasst habe, so drängt sich natürlich auch die Frage auf, wer diese Daten in welchem Zusammenhang nutzen darf. Dazu halte ich es für unerlässlich, dass die Berechtigung zur Teilnahme an dieser Art von Datenverkehr durch einen Ausweis in Form einer Chipkarte nachzuweisen ist. Diese Chipkarte muss ihren Inhaber identifizieren, die Art seiner berufsspezifischen Zugriffsberechtigung angeben, eine digitale Signaturfunktion enthalten und das Verschlüsseln und Entschlüsseln digitaler Nachrichten unterstützen. Ich spreche also von der sogenannten Health Professional Card, die als Zugriffsberechtigung nach dem heutigen Planungsstand zwingend er-

forderlich ist. Sie leistet einen unverzichtbaren Beitrag zur Wahrung des Arztgeheimnisses.

An dieser Stelle möchte ich ein weiteres zentrales Thema ansprechen, nämlich den Schutz vor einer Beschlagnahme. Die entsprechenden Vorschriften in der Strafprozessordnung führen dazu, dass die Patientendaten dem besonderen Schutz vor staatlichen Zugriffen nur dann unterliegen, wenn sich diese Daten im Gewahrsam des „zur Verweigerung des Zeugnisses Berechtigten“ befinden, also, um es vereinfacht auszudrücken: Der Beschlagnahmeschutz gilt nur dann, wenn der Arzt die Daten in seinem Gewahrsam hat. Was passiert aber mit den Daten, die auf der Chipkarte übertragen sind und die sich nicht mehr beim Arzt befinden? Was ist mit den Daten auf einem elektronischen Rezept? Hier muss der gleiche Schutz gelten, als ob sich die Daten noch beim Arzt befänden, denn eine Aufweichung des Arztgeheimnisses und der damit verbundenen, gesetzlich angeordneten Schutzmechanismen muss verhindert werden. Auch solche Fragen, meine Damen und Herren, müssen einer Lösung zugeführt werden, die vor allem aus Sicht des Patienten transparent ist und die ihm immer wieder den Eindruck vermittelt, dass er Herr seiner Daten ist und bleibt.

Lassen Sie mich nun nach diesen Ausführungen, die sich gleichermaßen auf das elektronische Rezept und auf die elektronische Patientenakte bezogen, auf einige konkrete Punkte zum elektronischen Rezept eingehen.

Für diesen elektronischen Datentransport zu der Apotheke, die der Patient aufsucht, werden vor allem zwei verschiedene Verfahren diskutiert:

Bei dem einen wird das Rezept in den Speicher einer Chipkarte geschrieben und bei dem anderen werden die Rezeptdaten auf einen Server geschrieben, von dem sie aus jeder Apotheke abrufbar sind, sobald sie vom Patienten dort vorgelegt werden.

Beide Verfahren lassen sich datenschutzrechtlich so ausgestalten, dass sie den größtmöglichen Schutz vor Missbrauchsmöglichkeiten bieten. Aus diesem Grunde haben sich die Datenschützer auch bislang nicht für ein bestimmtes Verfahren ausgesprochen, sondern stets betont, dass die konkrete Ausgestaltung im Einzelnen

entscheidend ist. So sind zahlreiche Fragen zu klären, angefangen damit, wer Einblick in die Daten hat, ob der Apotheker nur die Daten einsehen kann, die für die Ausgabe des Medikamentes erforderlich sind, ob diese Daten nach Ausgabe des Medikamentes automatisch gelöscht werden oder nicht doch Kopien zurück bleiben, die sogar dazu führen können, dass der Patient das Medikament in einer anderen Apotheke nochmals erhalten kann. Wie und wann kann der Patient selbst die Daten lesen oder eventuell auch löschen, und zwar unabhängig vom Arzt oder Apotheker? Muss bzw. darf der behandelnde Arzt erfahren, ob und wann der Patient das Rezept eingelöst hat oder soll nicht auch über diese Frage der Patient selbst entscheiden dürfen.

Auch bei der elektronischen Patientenakte stellt sich die Frage, ob die Daten auf einem zentralen Server oder besser dezentral gespeichert werden sollen. Da auch nach Einführung einer elektronischen Patientenakte medizinische Daten bei den einzelnen Behandlern gespeichert werden, führt eine zentrale Speicherung zu einer zusätzlichen Speicherung der Daten. So etwas löst bei Datenschützern immer ein gewisses Unbehagen aus. Ein zentrales datenschutzrechtliches Anliegen ist auch hier die Freiwilligkeit der Teilnahme. Kein Patient darf gezwungen werden, an einem solchen Projekt teilnehmen zu müssen. Diese Freiwilligkeit muss auch dauerhaft gewährleistet sein. So darf z.B. das immer wieder propagierte Ziel der „Vermeidung von Doppeluntersuchungen“ nicht dazu führen, dass sich ein faktischer Zwang zur Einwilligung der Führung und des Zugriffs auf die elektronische Patientenakte durch den Zweitbehandler ergibt, wenn dieser behauptet, die Vorabinformationen für seine Behandlung zu benötigen. Abgesehen davon kann es durchaus im Interesse des Patienten liegen, eine unbeeinflusste Zweitmeinung einzuholen.

Ferner ist zu klären, ob und wie es dem Patienten ermöglicht werden kann, lediglich einzelne Segmente seiner Daten für die jeweils behandelnden Ärzte freizugeben. Würde eine partielle Freigabe der Daten fehlen, könnte sich wiederum ein faktischer Zwang für den Patienten ergeben, seine Daten insgesamt zu offenbaren. Regelungen sind auch erforderlich für die Datennutzung, da Zugriff auf die elektronische Patientenakte viele haben wollen, aber nicht alle haben können. Auch bedarf es, da die elektronische Patientenakte nicht „ewig“ verfügbar sein soll, Vorgaben für die Löschung der Daten. Schließlich muss die Frage gelöst werden, wie der Patient seine

Auskunfts- und Einsichtsrechte wahrnehmen kann. Der Patient muss ohne großen Aufwand und Kosten diese Rechte geltend machen können. Schließlich ist er Herr seiner Daten. Das dies so bleiben muss, hat erfreulicherweise auch der Beauftragte der Bundesregierung für die Belange der Behinderten, Karl Hermann Haack, Ende letzten Jahres festgestellt, als er zu einem Workshop zum Projekt der elektronischen Patientenakte einlud.

Sie sehen, meine Damen und Herren, es bleiben eine Reihe von Fragestellungen, die einer datenschutzgerechten Lösung zugeführt werden müssen. Alle Probleme, die ich in der Kürze der zur Verfügung stehenden Zeit zum Teil nur habe anreißen können, erscheinen sowohl aus rechtlicher als auch technischer Sicht lösbar. Der Datenschutz, um dies auch nochmals zu verdeutlichen, tritt hier nicht als Verhinderer auf – wie übrigens auch sonst nicht – , sondern als Wahrer des Schutzes von personenbezogenen Daten der Patienten. Dadurch erfüllt er letztlich eine ganz wichtige Funktion, denn alle neuen Projekte müssen sich daran messen lassen, dass die Patienten sich auf diese Systeme auch verlassen können müssen, um ihnen ihre „Geheimnisse“ anzuvertrauen. Dazu gehört zwingend ein hohes Maß an Transparenz der Strukturen, sowohl der Datenverarbeitung selbst als auch deren Schutzmaßnahmen. Ohne diese Transparenz wird die notwendige Akzeptanz der Patienten nicht erreicht werden können. Diese Akzeptanz sowohl bei Patienten als auch in der Politik zu erreichen, ist das Ziel aller Beteiligten, und da schließe ich den Datenschutzbeauftragten ausdrücklich mit ein. Zur Unterstützung und Beratung stehe ich wie schon in der Vergangenheit gerne bereit. Ich bin sicher, dass das Aktionsforum Telematik im Gesundheitswesen, dem eine ganz entscheidende Bedeutung bei der Einführung von Verfahren zur Verbesserung der Kommunikation im Gesundheitswesen zukommt, auch zukünftig mit den Datenschutzbeauftragten eng und vertrauensvoll zusammen arbeiten wird. Im Interesse des Datenschutzes der Patienten wünsche ich eine erfolgreiche Fortsetzung der bisherigen Aktivitäten. Der Datenschutzbeauftragte ist bereit, hierzu seinen Beitrag zu leisten.