SOZIALVERBAND VdK RHEINLAND-PFALZ

Juni 2016

Datenschutz und Transparenz

in der gesetzlichen Krankenversicherung

Impressum

Inhalte: Martin Russell Varga

Sozialverband VdK Rheinland-Pfalz e. V., Kaiserstraße 62, 55116 Mainz

E-Mail: rheinland-pfalz@vdk.de
Internet: www.vdk.de/rheinland-pfalz

Die Inhalte wurden sorgfältig erarbeitet. Es kann jedoch keine Gewährleistung für Aktualität, Richtigkeit und Vollständigkeit übernommen werden.

Die in dieser Informationsmappe verwendeten männlichen Bezeichnungen dienen ausschließlich der besseren Lesbarkeit und gelten ausdrücklich für beide Geschlechter. Eine Diskriminierung weiblicher Personen wird damit nicht beabsichtigt.

Inhalt

1. Datenschutz und Transparenz

1.1. Was heißt Datenschutz?

„Datenschutz“ ist seit einigen Jahren in aller Munde. Insbesondere im Zuge einer immer effizienteren elektronischen Datenverarbeitung wird Datenschutz von Nichtregierungsorganisationen und Datenschutzbeauftragten regelmäßig angemahnt. Aber worum geht es dabei eigentlich?
Obgleich der Begriff unterschiedlich verwendet wird, geht es beim Datenschutz im Kern stets um dasselbe, nämlich um das Recht auf Privatsphäre. Diese ist nur gewährleistet, wenn jeder Mensch selbst darüber bestimmen kann, wer welche Informationen über ihn erhält. Das Bundesverfassungsgericht spricht hier vom Grundrecht auf informationelle Selbstbestimmung, welches es auf das allgemeine Persönlichkeitsrecht und damit auch auf die Menschenwürde zurückführt. Rechtlich hat der Datenschutz also einen hohen Stellenwert.
Informationen, die einer Person zugeordnet werden können, heißen im Datenschutzrecht personenbezogene Daten. Personenbezogene Daten können messbare Daten wie die Körpergröße sein, aber auch amtlich festgestellte Qualifikationen, zum Beispiel Schulabschluss und Führerschein, oder nicht messbare, aber auswertbare Informationen wie Ernährungsvorlieben. Auch Daten wie die Krankenversicherungsnummer sind personenbezogene Daten, weil es mit dem Zugriff auf die entsprechenden Datenbanken möglich ist, sie einer bestimmten Person zuzuordnen.
Datenschutz meint zunächst dasselbe wie das informationelle Selbstbestimmungsrecht, nämlich dass im Grundsatz jeder Mensch entscheiden können soll, wer personenbezogene Daten über ihn erlangt. Jedoch wird dieses Selbstbestimmungsrecht durch kollidierende rechtlich geschützte Interessen beschränkt. Diese Einschränkungen müssen ihrerseits bestimmten Mindestanforderungen genügen. Um diese Anforderungen geht es typischerweise beim Datenschutz. Beispielsweise muss der Zugriff auf personenbezogene Daten rechtlich geregelt und im Einzelfall rechtmäßig sein. Die rechtlichen Regelungen dürfen die informationelle Selbstbestimmung nicht zu stark beschneiden, sondern müssen beispielsweise das richtige Maß zwischen den Anforderungen der Verwaltung, die personenbezogene Daten benötigt, und dem Geheimhaltungsinteresse der betroffenen Personen wahren. Was aber das richtige Maß ist, ist Wertungsfrage. Datenschutzrechtliche Fragen sind stets (auch) politische Fragen.

1.2. Warum geht Datenschutz alle an?

Ein Geheimhaltungsinteresse hat im Grundsatz jeder Mensch, auch wenn er oder sie „nichts zu verbergen“ hat. Denn beim Datenschutz geht es nicht nur darum, dass Informationen über Fehlverhalten, womöglich sogar strafbares Verhalten, eines Menschen bekannt werden könnten. Auch wer ganz unbescholten ist, hat Nachteile zu befürchten, wenn Daten in unbefugte Hände gelangen. Denn dieselbe Information kann für unterschiedliche Personen ganz unterschiedliche Bedeutung haben. Wenn jemand beispielsweise von seiner chronischen Erkrankung erzählt, werden Freunde und Bekannte mit Anteilnahme reagieren. Ein potenzieller Arbeitgeber würde sich hingegen fragen, ob der Bewerber wirklich belastbar ist, und vielleicht – mit anderer Begründung – einen anderen Bewerber vorziehen. Ein privates Lebensversicherungsunternehmen wiederum würde ihm eine Berufsunfähigkeitsversicherung vielleicht nur noch zu einem inakzeptablen Preis anbieten.

Beim Datenschutz geht es also nicht nur um „sensible“ Daten, von denen möglichst niemand Kenntnis nehmen sollte. Wer einem anderen eine Information anvertraut, kann unmöglich an alle Konsequenzen denken, die Dritte aus dieser Information ziehen könnten. Gerade wenn es um den Verkehr mit Behörden geht, hat man zudem meist gar keine Wahl – Informationen weiterzugeben gehört dann zur Mitwirkungspflicht im Verwaltungsverfahren und ist vielfach Leistungsvoraussetzung. Ferner kann aus einer Mehrzahl von Daten auf weitere Informationen geschlossen werden, die der Betroffene gar nicht weitergegeben hat. Das heißt: Je mehr personenbezogene Daten in Umlauf sind, desto mehr weitere personenbezogene Daten können daraus gefolgert werden, und desto größer wird die Gefahr negativer Folgen.
Deshalb ist es wichtig, dass Datenweitergabe und Datenzugriff rechtlich geregelt und begrenzt werden. Dafür lassen sich einige Grundsätze formulieren: Vor der Kenntnisnahme Unbefugter müssen Daten geschützt werden. Darüber hinaus sollten nicht mehr Daten erhoben werden, als unbedingt nötig. Ferner sollte jede berechtigte Person nur Zugriff auf die jeweils von ihr benötigten Daten erhalten, auch innerhalb desselben Leistungsträgers. Daten sollten möglichst nur für den Zweck verwendet werden, zu dem sie erhoben worden sind. Zu unterschiedlichen Zwecken erhobene Daten dürfen untereinander nicht verkettet werden, damit kein Persönlichkeitsprofil entstehen kann. Wenn möglich, sollten Daten anonymisiert oder zumindest pseudonymisiert* verarbeitet werden, um die Zuordnung zu einer Person zu erschweren. Viele dieser Grundsätze sind im Bundesdatenschutzgesetz und im geltenden Datenschutzrecht der Krankenversicherung zumindest bereichsweise verwirklicht.

1.3. Was heißt Transparenz?

Transparenz ist in gewisser Weise das Gegenstück zum Datenschutz. Wörtlich übersetzt bedeutet der lateinische Begriff „Durchsichtigkeit“. Transparenz meint die öffentliche Zugänglichkeit und Nachvollziehbarkeit von Informationen, entweder für die Allgemeinheit durch öffentliche Bereitstellung oder für Einzelne auf Anfrage. Anders als der Datenschutz ist die Transparenz nicht von vornherein auf personenbezogene Daten beschränkt, sondern umfasst Informationen jeglicher Art, insbesondere über Vorgänge und Zustände, die für die Öffentlichkeit von Interesse sind. Aufgrund dieses unterschiedlichen Bezugspunktes besteht zwischen Transparenz und Datenschutz kein grundsätzlicher Widerspruch. Nur soweit Einzelne oder die Öffentlichkeit gerade von personenbezogenen Daten Dritter Kenntnis nehmen möchten, kann es zu einem Konflikt kommen, in dem die widerstreitenden Interessen abzuwägen sind. So könnte etwa ein Journalist Interesse daran haben, zu erfahren, ob gegen eine Politikerin Ermittlungen wegen Steuerhinterziehung eingeleitet wurden, während die betroffene Politikerin dies geheim halten möchte.
Speziell im Bereich der öffentlichen Verwaltung beschränkt sich Transparenz aber nicht auf Informationen, die für die Allgemeinheit von Interesse sind. Auch Einzelne sollen von Informationen Kenntnis nehmen können, die sie betreffen, insbesondere wenn es um Entscheidungsprozesse und Entscheidungsergebnisse in der Verwal-

* Anonymisieren ist laut Bundesdatenschutzgesetz die Veränderung personenbezogener Daten derart, dass die Einzelangaben nicht mehr oder nur erschwert einer bestimmten Person zugeordnet werden können. Pseudonymisieren ist das Ersetzen eines Namens durch ein Kennzeichen. Wer Namen und Kennzeichen kennt, kann aber die mit dem Kennzeichen verbundenen Daten noch einer Person zuordnen.

tung geht. Solche Informationen können für eine Vielzahl von Personen inhaltsgleich sein, zum Beispiel eine Rechtsbehelfsbelehrung auf einem Bescheid oder eine Broschüre der Krankenkasse. Sie können aber auch höchst individuell sein, etwa wenn es um Akteneinsicht geht, beispielsweise die Einsicht in ein ärztliches Gutachten. Bei Informationen dieser beiden Arten besteht häufig kein Konfliktpotenzial mit dem Datenschutz, denn die maßgeblichen personenbezogenen Daten sind vielfach die Daten desjenigen, der den Informationszugriff begehrt.
Im Gegenteil ist Transparenz sogar ein Leitprinzip des Datenschutzes, nämlich die Transparenz der Datenweitergabe und Datenverwendung: Jeder Mensch soll im Grundsatz wissen, wer Zugriff auf seine Daten hat und wozu sie verwendet werden.

1.4. Was hat Datenschutz mit der Krankenversicherung zu tun?

Gerade in der Sozialverwaltung werden besonders viele personenbezogene Daten erhoben, verarbeitet und genutzt. Sie heißen in diesem Zusammenhang Sozialdaten. Viele dieser Sozialdaten sind zugleich besonders sensibel, geht es doch beispielsweise um Krankheit, Pflegebedürftigkeit, Erwerbsunfähigkeit, Behinderung, um Einkommens- und Vermögensverhältnisse oder darum, mit welchem Menschen eine Lebensgemeinschaft besteht. Deshalb ist der Schutz solcher Daten im Bereich der Sozialverwaltung besonders wichtig.
In der Krankenversicherung sind es insbesondere Informationen über den Gesundheitszustand der Versicherten, die das Thema Datenschutz berühren, daneben aber auch alle anderen Daten, die den Krankenkassen, den behandelnden Ärzten oder dem Medizinischen Dienst der Krankenversicherung (MDK) vorliegen.
Solche Daten sind nicht nur für die Krankenkasse interessant, sondern auch für Dritte, etwa für Arbeitgeber oder Pharmaunternehmen. Deshalb gibt es für den Datenschutz in der Krankenversicherung eine doppelte Herausforderung: Einerseits muss innerhalb des Gesundheitssystems eine klare Trennung der Zugriffsbefugnisse gewährleistet sein, sodass jeweils nur die Stellen Zugriff auf Daten erlangen, die diese Daten benötigen und rechtlich zur Verarbeitung berechtigt sind. Andererseits muss auch gewährleistet sein, dass niemand außerhalb des Gesundheitssystems von den Daten Kenntnis nehmen kann. Ein Beispiel dafür ist die Arbeitsunfähigkeitsbescheinigung: Während das Exemplar, das für die Krankenkasse bestimmt ist, einen Diagnoseschlüssel enthält, ist auf dem Exemplar für den Arbeitgeber nicht vermerkt, an welcher Krankheit der Versicherte leidet.
Transparenz betrifft in der Krankenversicherung beispielsweise die Einsicht in ärztliche Befundberichte und Gutachten, aber auch eine korrekte Beratung zu Versichertenrechten durch die Krankenkasse, etwa beim Thema Krankengeld.

2. Grundlagen des sozialrechtlichen Datenschutzes

Ein insgesamt recht hohes Maß an Datenschutz wird bereits durch die bestehenden Regelungen des Sozialrechts gewährleistet, jedenfalls soweit diese befolgt werden. Im Grundsatz ist zwar auch im Sozialrecht das Bundesdatenschutzgesetz (BDSG) anwendbar. Es wird aber nach § 1 Absatz 3 BDSG weitgehend durch die spezielleren sozialrechtlichen Datenschutzregelungen verdrängt. Wichtige Regelungen finden sich in § 35 Sozialgesetzbuch, Erstes Buch (§ 35 SGB I), im 2. Kapitel des SGB X und im BDSG sowie speziell für die Krankenversicherung im 10. Kapitel des SGB V.

2.1. Das Sozialgeheimnis und seine Konkretisierungen

Zentrale Datenschutzbestimmung im Sozialrecht ist das so genannte Sozialgeheimnis (§ 35 SGB I). Es regelt, dass Daten nicht ohne Rechtsgrundlage erhoben, verarbeitet und genutzt werden dürfen. Die entsprechenden rechtlichen Regelungen des Sozialgesetzbuchs sind abschließend. Generell dürfen die zuständigen Behörden Sozialdaten nur erheben, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Sie müssen so wenig Sozialdaten erheben wie möglich und sie, soweit möglich, anonymisieren (§ 78b SGB X). Näheres regelt § 67a SGB X: Im Grundsatz müssen Daten direkt beim Betroffenen erhoben werden, wobei er darüber zu informieren ist, wozu die Daten benötigt werden. Dieser Grundsatz ist aber von zahlreichen Ausnahmen durchbrochen. So ist eine Erhebung bei anderen Sozialleistungsträgern zulässig, wenn die Erhebung beim Betroffenen zu aufwändig wäre, wenn sie keine überwiegenden schutzwürdigen Interessen des Betroffenen berührt und wenn die jeweilige Stelle zur Übermittlung befugt ist. Werden Daten bei anderen Stellen als Sozialleistungsträgern erhoben, müssen Betroffene in der Regel davon unterrichtet werden. Die verpflichteten Stellen müssen auch dafür Sorge tragen, dass Unbefugte keinen Zugriff auf Sozialdaten erhalten. Zur Einhaltung des Sozialgeheimnisses verpflichtet sind neben Leistungsträgern auch deren Verbände, aber auch beispielsweise die kassenärztlichen Vereinigungen. Soweit nicht die Übermittlung sozialrechtlich zulässig ist, müssen Daten auch auf Verlangen anderer Stellen nicht weitergegeben werden. Auch innerhalb desselben Leistungsträgers dürfen Sozialdaten nur denjenigen zugänglich gemacht werden, die zur Kenntnisnahme befugt sind. Im Detail ist gesetzlich geregelt, zu welchen Zwecken außer zu dem Zweck, zu dem sie erhoben worden sind (§ 69 Abs. Nr. 1 SGB X), Daten übermittelt werden dürfen (§§ 67d – 77 SGB X). Unrichtige Sozialdaten sind zu berichtigen, nicht mehr benötigte Sozialdaten zu löschen. Zu löschen sind auch Daten, die nicht gespeichert werden dürfen (§ 84 SGB X). Unter bestimmten Voraussetzungen kann die Löschung durch eine Sperrung der Daten ersetzt werden. Sie bewirkt, dass die Daten nur unter besonderen Voraussetzungen ohne Einwilligung des Betroffenen übermittelt und genutzt werden dürfen.

2.2. Durchsetzung datenschutzrechtlicher Pflichten

Betroffene können gegen missbräuchliche Datenverwendung gerichtlich vorgehen. Je nach Konstellation können sie auf Feststellung oder auf Unterlassung klagen, nötigenfalls auch vorbeugend. Datenschutzverstöße im Verwaltungsverfahren können aber in der Regel nur zusammen mit dem verfahrensabschließenden Verwaltungsakt angegriffen werden, wenn ein solcher zu ergehen hat (§ 56a Sozialgerichtsgesetz – SGG). Anderes kann gelten, wenn die Verfahrensfehler in ihrer Bedeutung über das Interesse an der Gewährung der Sozialleistung hinausreichen, so jedenfalls das Sozialgericht Stade (Urteil vom 23.2.2006, Az. S 6 AL 112/02). Ferner können Betroffene bei vorsätzlichen oder fahrlässigen Verstößen gegen das Sozialgeheimnis Schadensersatz verlangen (§ 82 SGB X). Allerdings sind in der Regel nur materielle Schäden zu ersetzen, immaterielle nur ausnahmsweise, vor allem bei der automatisierten Datenverarbeitung. In bestimmten Fällen – aber nicht immer – können Datenschutzverstöße auch strafrechtliche Konsequenzen nach sich ziehen. Nicht zuletzt damit sie von ihren Rechtsschutzmöglichkeiten sinnvoll Gebrauch machen können, können Betroffene in der Regel Auskunft über zu ihrer Person gespeicherte Sozialdaten, deren Verbreitung und den Zweck der Speicherung verlangen (§ 83 SGB X).

Neben dem Rechtsweg steht Menschen, die von Datenschutzverstößen betroffen sind, auch die Anrufung des Bundesdatenschutzbeauftragten (bei Stellen des Bundes) oder des Landesdatenschutzbeauftragten (bei Stellen des Landes) offen.

2.3. Besonderheiten in der Krankenversicherung

Das spezifisch krankenversicherungsrechtliche Datenschutzrecht kann hier nicht erschöpfend dargestellt werden. Vielmehr werden typische, situationsgebundene Problemkreise für Versicherte und ihre Vertreter herausgegriffen (3. und 4.). Danach werden einige wichtige Gefährdungen des Datenschutzes und der Transparenz in der Krankenversicherung situationsübergreifend vorgestellt (5.).

3. Datenschutz in der Krankenversicherung – Kernfragen

3.1. Zu welchen Zwecken darf die Krankenkasse Sozialdaten erheben?

Zu welchen Zwecken Krankenkassen Daten erheben und speichern dürfen, ist gesetzlich genau und abschließend in § 284 SGB V geregelt. Hier wird nur eine Auswahl dieser Zwecke dargestellt. Zulässig ist die Erhebung und Speicherung unter anderem, soweit die Daten erforderlich sind für:

- die Feststellung des Versicherungsverhältnisses und der Mitgliedschaft, einschließlich der für deren Anbahnung erforderlichen Daten,
- die Ausstellung der elektronischen Gesundheitskarte,
- die Feststellung der Beitragspflicht und der Beiträge,
- die Prüfung der Leistungspflicht und der Erbringung von Leistungen an Versicherte (einschließlich Leistungsbeschränkungen), die Bestimmung des Zuzahlungsstatus und die Durchführung der Verfahren bei Kostenerstattung, Beitragsrückzahlung und der Ermittlung der Belastungsgrenze,
- die Unterstützung der Versicherten bei Behandlungsfehlern,
- die Beteiligung des Medizinischen Dienstes,
- die Abrechnung mit den Leistungserbringern, einschließlich der Prüfung der Rechtmäßigkeit und Plausibilität der Abrechnung,
- die Überwachung der Wirtschaftlichkeit der Leistungserbringung,
- die Abrechnung mit anderen Leistungsträgern,
- zur Gewinnung von Mitgliedern im Regelfall dann, wenn die Daten allgemein zugänglich sind – sobald nicht mehr benötigt, sind die Daten zu löschen.

Einmal erhoben, dürfen die Daten nur zu einem der Zwecke aus dieser Liste genutzt werden. Geregelt ist schließlich auch, wann Daten auf maschinell verwertbaren Datenträgern gespeichert werden dürfen.

3.2. Welche Daten werden auf der Versichertenkarte gespeichert?

Schon seit den 1990er Jahren gibt es die Krankenversichertenkarte. Darauf sind gemäß § 291 SGB V folgende Basisangaben gespeichert – das gilt auch für die neue elektronische Gesundheitskarte:

- die Bezeichnung der ausstellenden Krankenkasse, einschließlich eines Kennzeichens für die Kassenärztliche Vereinigung, in deren Bezirk der Versicherte seinen Wohnsitz hat,
- der Familienname und Vorname des Versicherten,

- das Geburtsdatum des Versicherten,
- das Geschlecht des Versicherten,
- die Anschrift des Versicherten,
- die Krankenversichertennummer* des Versicherten,
- der Versichertenstatus oder für bestimmte Gruppen nicht versicherter Personen der Status der auftragsweisen Betreuung,
- der Zuzahlungsstatus des Versicherten,
- der Tag des Beginns des Versicherungsschutzes,
- bei befristeter Gültigkeit der elektronischen Gesundheitskarte das Datum des Fristablaufs.

Über eine Internetverbindung können Leistungserbringer wie zum Beispiel Ärzte die Aktualität der Daten, die auf der Versichertenkarte gespeichert sind, bei der Krankenkasse prüfen und die Daten aktualisieren. Die Durchführung dieser Prüfung wird auf der Versichertenkarte gespeichert.
Zu den maschinenlesbaren Daten kommt noch ein Foto hinzu, das auf der Versichertenkarte abgedruckt sein muss. Der Versicherte muss auf der Karte unterschreiben.
Die elektronische Gesundheitskarte enthält einen Mikroprozessor. Aufgrund technischer und organisatorischer Probleme wird sie aber bisher zu keinem anderen Zweck genutzt als die frühere Versichertenkarte. In Zukunft soll sie hingegen zu vielen weiteren Anwendungszwecken eingesetzt werden (§ 291a SGB V):
Zunächst soll sie geeignet sein, ärztliche Verordnungen elektronisch und maschinell verwertbar zu übermitteln. Sie soll auch die europäische Krankenversichertenkarte umfassen. Ferner sollen direkt auf der Karte Notfalldaten gespeichert werden können, etwa Medikationen, Allergien, Unverträglichkeiten, Blutgruppe und Kontaktdaten des behandelnden Arztes und von Angehörigen. So wird es künftig leichter, für die Versicherten bereits in der Apotheke Medikationspläne für mehr als ein Medikament zu erstellen. Zukünftige Versionen der elektronischen Gesundheitskarte sollen auch Erklärungen zur Organ- und Gewebespende sowie zum Vorhandensein von Patientenverfügungen und Vorsorgevollmachten enthalten können. Zur Zeit sind die Karten darauf aber noch nicht ausgelegt.
Eine weitere Anwendung wird das elektronische Rezept sein. Es soll entweder direkt auf der Karte oder online gespeichert werden, wobei dann der Zugangsschlüssel auf der Karte hinterlegt wird. Das elektronische Rezept würde in Zukunft zudem die Nutzung von Versandapotheken erleichtern – aus Sicht der Bundesregierung wohl der Hauptgrund für seine Einführung.
Geplant sind auch eine elektronische Patientenakte und ein elektronischer Arztbrief, die jeweils unter Einsatz der Karte genutzt werden können. Hier wird die Karte aber jeweils nur als Zugangsschlüssel dienen. Als verkleinerter Teil der elektronischen Patientenakte sollen ferner auch Daten zur Arzneimitteltherapiesicherheit von Ärzten und Apotheken abgerufen werden können. Des Weiteren soll die Karte auch eine so genannte elektronische Patientenquittung, das heißt eine Aufstellung der in Anspruch genommenen Leistungen und ihrer Kosten, enthalten können.

* Die Krankenversichertennummer ist eine individuelle Identifikationsnummer. Sie setzt sich aus einem unveränderlichen Teil, der dem Versicherten zugeordnet ist, und einem veränderlichen Teil, der Angaben zur Kassenzugehörigkeit enthält, zusammen. Sie ist von der Rentenversicherungsnummer zu unterscheiden.

Daten, die im Zusammenhang mit der elektronischen Gesundheitskarte gespeichert werden, sollen nur mit Einwilligung der Versicherten erhoben, verarbeitet und genutzt werden, wobei diese einmalig im Voraus erklärt und auf der Karte selbst abgespeichert werden soll. Werden die Daten erhoben, dürfen nur Ärzte, Zahnärzte und Apotheker sowie deren Angestellte im Rahmen ihrer Aufgaben, ferner Beschäftige in Krankenhäusern und Erbringer ärztlich verordneter Leistungen und Psychotherapeuten die Daten einsehen. Der unbefugte Zugriff wird strafrechtlich verfolgt. Die Patienten selbst sollen auf alle Daten zugreifen können. Sie sollen auch ohne Einsatz der Karte gespeicherte Daten zu Organspende, Patientenverfügung und Vorsorgevollmacht löschen können. Andere Daten sollen auf ihr Verlangen gelöscht werden, sofern keine rechtlichen oder sonstigen Einwände dagegen sprechen.

3.3. Darf die Krankenkasse Fotos Versicherter dauerhaft speichern?

Ja, die Krankenkasse darf Fotos unbegrenzt speichern – jedenfalls nach Auffassung des Sozialgerichts Mainz in seiner Entscheidung vom 1. Dezember 2015. Das Gericht beruft sich darauf, die Abwägung zwischen dem Grundrecht auf informationelle Selbstbestimmung und den Erfordernissen der Massenverwaltung gehe zulasten der Versicherten aus. Es liege in deren eigenem Interesse, schnellstmöglich eine neue Versichertenkarte zu erhalten. Davon könnten auch die Krankenkassen ausgehen, solange der Versicherte nicht ausdrücklich die Löschung des Fotos verlangt habe. Der Kläger in dem Verfahren und Teile der juristischen Literatur[*] sehen das anders. Es fehle bereits die Rechtsgrundlage für die Speicherung des Fotos. Sie sei zudem nicht zwingend erforderlich, denn sonst wäre es auch nicht möglich, die Fotos auf die Aufforderung des Versicherten hin zu löschen. Bei Verlust der Karte oder nach Ablauf der Gültigkeit könne ein neues Bild angefordert werden. Wer das nicht wolle, könne freiwillig in die Speicherung des Bildes einwilligen. Zudem sei Folgendes zu berücksichtigen: Wenn schon die Gültigkeit der Karte begrenzt sei – was im Übrigen unnötigen Verwaltungsaufwand erzeuge – dann sei es auch sinnvoll, ein jeweils aktuelles Foto anzufordern, weil das Bild sonst mit der Zeit für die Identifizierung des Karteninhabers nutzlos werde. Zudem wird das Lichtbild ohnehin von der Krankenkasse nicht auf Echtheit geprüft, sodass Missbrauch möglich bleibt, obwohl dessen Vermeidung ein Grund für die Einführung des Fotos war.
Es bleibt abzuwarten, wie die höchstrichterliche Rechtsprechung entscheiden wird und ob der Gesetzgeber nachbessert.

3.4. Bleibt nachvollziehbar, welche Leistungen Versicherte erhalten haben?

Welche Leistungen Versicherte erhalten haben, wird dann von der Krankenkasse versichertenbezogen aufgezeichnet, wenn der Erhalt dieser Leistungen Voraussetzung für den Erhalt anderer Leistungen in der Zukunft sein könnte (§ 292 SGB V). Der Versicherte soll dadurch von der Aufbewahrung von Nachweisen entlastet werden. Das betrifft beispielsweise zukünftige Leistungen bei Krankenhausbehandlung, Gesundheitsvorsorge und Rehabilitation sowie Kostenerstattungs- und Zuschussansprüche. Bei Arbeitsunfähigkeit sind die Diagnosen aufzuzeichnen. Alle Daten dieser Art – ausgenommen ärztliche Abrechnungsdaten, für die Sonderregeln gelten – müssen spätestens 10 Jahre nach Ende des Geschäftsjahres der Leistungsgewährung gelöscht werden. Das gilt auch bei Kassenwechsel; dazu muss die alte Kasse

[*] Ziebarth, WzS 02/16, S. 51 f.

der neuen auf Verlangen die laufenden Fristen mitteilen (§ 304 Abs. 1 Satz 1 Nr. 1 SGB V).
Ein „Patientenprofil“ mit einer Übersicht aller jemals in Anspruch genommener Leistungen darf die Krankenkasse nicht anlegen (§ 305 Abs. 1 Satz 4 SGB V). Ihr liegen aber, getrennt nach ärztlichen und nichtärztlichen Leistungserbringern, Abrechnungsdaten vor, aus denen sie nach § 305 SGB V auf Antrag des Versicherten eine Übersicht der in den letzten 18 Monaten in Anspruch genommenen Leistungen erstellen darf und muss.
Davon unabhängig sind neben Diagnosen und Arztbriefen auch Daten über erbrachte Leistungen in den jeweiligen Patientenakten der Leistungserbringer, insbesondere der Ärzte, enthalten, die in § 630f Abs. 2 Bürgerliches Gesetzbuch (BGB) geregelt sind. Schon heute werden Patientenakten oft elektronisch geführt. Zukünftig sollen sie einheitlich elektronisch geführt werden können, wobei die elektronische Gesundheitskarte als Zugangsschlüssel dienen soll. Ob sich daraus eine Verbesserung oder eine Verschlechterung beim Datenschutz ergibt, wird unterschiedlich beurteilt. Unabhängig von der Form der Akte haben Patienten nach § 630g BGB ein Einsichtsrecht. Sie können auch gegen Auslagenersatz Kopien der Dokumente verlangen.

3.5. An wen dürfen Ärzte zu welchem Zweck welche Daten übermitteln?

Zusammenfassend lässt sich sagen, dass Leistungserbringer solche Daten an die Krankenkassen und Kassenärztlichen Vereinigungen übermitteln dürfen und müssen, die im Zusammenhang mit den erbrachten Leistungen stehen und die die Krankenkassen beziehungsweise Kassenärztlichen Vereinigungen zur Erfüllung ihrer Aufgaben benötigen, wie es § 294 SGB V als Einweisungsvorschrift zusammenfasst.
Im Zusammenhang mit der Abrechnung ärztlicher Leistungen sind nach § 295 SGB V an Sozialdaten zu übermitteln:

- in dem Exemplar der Arbeitsunfähigkeitsbescheinigung, das für die Krankenkasse bestimmt ist, die (verschlüsselte) Diagnose
- in den Abrechnungsunterlagen für vertragsärztliche Leistungen die Arztnummer sowie die Leistungen, bei Ärzten mit (verschlüsselter) Diagnose, bei Zahnärzten mit Zahnbezug und Befunden
- auf Überweisungen die Arztnummer sowie die Basisangaben, die auf der Krankenversichertenkarte gespeichert sind (Liste in Abschnitt 3.2.).

Zusätzliche Spezialregelungen gelten für besondere Versorgungsformen wie die hausarztzentrierte und die integrierte Versorgung (§ 295a SGB V).
Die Kassenärztlichen Vereinigungen übermitteln quartalsweise für jeden Versicherten einen Großteil der entsprechenden Angaben, jedoch pseudonymisiert durch die Krankenversichertennummer (§ 296 SGB V). Zudem können sie bei arztbezogenen Wirtschaftlichkeitsprüfungen an die zuständigen Prüfstellen neben anonymisierten (§ 297 SGB V) sowie durch die Krankenversichertennummer pseudonymisierten (§ 298 SGB V) Daten auch versichertenbezogene Daten über Leistungen übermitteln.
Hat der behandelnde Arzt den Verdacht, dass eine Berufskrankheit oder eine Arbeitsunfallfolge vorliegt, muss er dies der Krankenkasse mitteilen (§ 294a SGB V). Gleiches gilt, wenn der Arzt davon ausgeht, dass die Krankheit auf einer medizinisch nicht indizierten kosmetischen Operation, einer Tätowierung oder einem Piercing beruht, weil in diesem Fall die Krankenkasse eine Kostenbeteiligung verlangen und Krankengeld ganz oder teilweise versagen kann (§ 52 II SGB V). In letztgenanntem Fall muss der Arzt den Versicherten über den Grund der Meldung und über die

übermittelten Daten informieren. Ob Ohrringe wie andere Piercings zu behandeln sind, ist übrigens rechtlich umstritten. Den Krankenkassen ist jedenfalls ein Ermessensspielraum eingeräumt, ob sie den Versicherten an den Kosten beteiligen beziehungsweise das Krankengeld kürzen. Bei Folgeproblemen durchstochener Ohrläppchen etwa dürften sie vielfach keine Eigenbeteiligung verlangen. Gerade dieser Spielraum der Krankenkassen ist jedoch, weil er zu einer Ungleichbehandlung von Versicherten nach Risikogruppen (Besserstellung rentabler Versicherter) sowie anhand von sozialen Normvorstellungen („sozialübliche“ versus „anormale“ Piercings) führen kann, verfassungsrechtlich und politisch problematisch.
Zu Zwecken der Qualitätssicherung dürfen Ärzte auch personenbezogene Daten der Versicherten erheben, verarbeiten und nutzen. Die Daten sollen aber in der Regel pseudonymisiert werden; ferner müssen Patienten über die Datenerhebung informiert werden (§ 299 SGB V). Die Daten können an die Kassenärztlichen Vereinigungen oder an unabhängige Auswertungsstellen übermittelt werden.

3.6. Welche Daten dürfen Krankenhäuser übermitteln?

Einige der Regeln für Ärzte sind auch auf Krankenhäuser anwendbar. Ferner müssen Krankenhäuser der Krankenkasse gemäß § 301 Abs. 1 SGB V elektronisch oder maschinenlesbar (unter anderem) folgende Daten übermitteln:

- die Basisdaten auf der Krankenversichertenkarte (Liste in Abschnitt 3.2.)
- das krankenhausinterne Kennzeichen des Versicherten
- das Institutionskennzeichen des Krankenhauses und der Krankenkasse
- Tag, Uhrzeit und Grund der Aufnahme, Einweisungsdiagnose, Aufnahmediagnose, bei einer Änderung der Aufnahmediagnose die nachfolgenden Diagnosen, die voraussichtliche Dauer der Krankenhausbehandlung,
- bei ärztlicher Verordnung von Krankenhausbehandlung die Arztnummer des einweisenden Arztes, bei Notfallaufnahme die veranlassende Stelle,
- die Bezeichnung der aufnehmenden Fachabteilung, bei Verlegung die der weiterbehandelnden Fachabteilungen,
- Datum und Art der im jeweiligen Krankenhaus durchgeführten Operationen und sonstigen Prozeduren,
- Tag, Uhrzeit und Grund der Entlassung oder der Verlegung, bei Entlassung oder Verlegung die für die Krankenhausbehandlung maßgebliche Hauptdiagnose und die Nebendiagnosen,
- Angaben über die im jeweiligen Krankenhaus durchgeführten Leistungen zur medizinischen Rehabilitation und ergänzende Leistungen sowie Aussagen zur Arbeitsfähigkeit und Vorschläge für die Art der weiteren Behandlung mit Angabe geeigneter Einrichtungen,
- die berechneten Entgelte.

Diagnosen sind zu verschlüsseln. Für Vorsorge- und Rehabilitationseinrichtungen gelten im Wesentlichen ähnliche Regelungen wie für Krankenhäuser (§ 301 Abs. 4 SGB V).

3.7. Welche Daten darf der Medizinische Dienst erheben?

Der Medizinische Dienst der Krankenversicherung hat insbesondere die Aufgabe, auf Verlangen der Krankenkasse Gutachten über Leistungsvoraussetzungen und Arbeitsunfähigkeit zu erstellen. Das geschieht in gesetzlich näher bestimmten Fällen

sowie immer dann, wenn nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf aus Sicht der Krankenkasse eine solche Begutachtung erforderlich ist (§ 275 SGB V). Im Wesentlichen dient die Tätigkeit des Medizinischen Dienstes also dazu, „unnötige“ Leistungen und Krankschreibungen zu vermeiden. Vielen Menschen ist der Medizinische Dienst auch aus dem Bereich der gesetzlichen Pflegeversicherung bekannt, in dem er gleichfalls Begutachtungsaufgaben (zur Einstufung in eine Pflegestufe) wahrnimmt. Für dieses Tätigkeitsfeld des Medizinischen Dienstes gelten nach § 276 VI SGB V zusätzliche Regelungen im SGB XI, die hier unberücksichtigt bleiben.
Im Übrigen gilt § 276 SGB V. In der gesetzlichen Krankenversicherung darf der Medizinische Dienst Sozialdaten nur erheben und speichern, soweit es für seine gutachtlichen Stellungnahmen und seine anderen Aufgaben erforderlich ist. Wenn der Medizinische Dienst von der Krankenkasse mit einer Begutachtung beauftragt wurde, müssen Leistungserbringer, wenn sie dazu aufgefordert werden, Sozialdaten an den Medizinischen Dienst übermitteln. Soweit der Medizinische Dienst seinerseits einen Gutachter beauftragt, dürfen die in diesem Rahmen erforderlichen Daten zwischen dem Medizinischen Dienst und dem Gutachter ausgetauscht werden.
Wenn der Medizinische Dienst Notwendigkeit und Dauer der stationären Behandlung eines Versicherten zu prüfen hat, darf er zwischen 8 und 18 Uhr die Räume der jeweiligen Einrichtung, beispielsweise des Krankenhauses, betreten, Unterlagen einsehen und den Versicherten untersuchen. Geht es um die Überprüfung der Arbeitsunfähigkeit und kann der Versicherte aus gesundheitlichen Gründen den MDK nicht aufsuchen oder verweigert dies, soll er in seiner Wohnung untersucht werden. Sofern er die Zustimmung verweigert, können – sofern die Untersuchung in der Wohnung nicht ausnahmsweise unzumutbar oder unverhältnismäßig ist (§§ 276 Abs. 5 SGB V, 65 SGB I) – Leistungen versagt werden.
Die Daten, die der Medizinische Dienst erhebt, dürfen nur für Zwecke der Begutachtung verwendet werden sowie für andere Zwecke, soweit das Sozialgesetzbuch dies erlaubt. Die Daten, die zur Identifikation des Versicherten dienen, muss der Medizinische Dienst getrennt von den medizinischen Sozialdaten speichern. Nur der Datenschutzbeauftragte des Medizinischen Dienstes darf über den Schlüssel für die Zusammenführung der Daten verfügen und muss jede Zusammenführung protokollieren. Nach fünf Jahren sind Sozialdaten zu löschen.
Daneben darf der Medizinische Dienst (wie die Krankenkassen und Kassenärztlichen Vereinigungen) mit Erlaubnis der zuständigen Aufsichtsbehörde Datenbestände für Forschungsvorhaben auswerten und auch über die gesetzlichen Fristen hinaus speichern, wobei Sozialdaten zu anonymisieren sind. Er darf darüber hinaus auch im Auftrag der Krankenkasse Datensätze der Krankenkasse auswerten, wobei die Daten schon vor Übermittlung an den Medizinischen Dienst zu anonymisieren sind.

3.8. Dürfen Krankenkassen Daten des Medizinischen Dienstes einsehen?

Nein. Das Sozialgesetzbuch V bestimmte bereits in der bisherigen Fassung des § 276 Abs. 1 Satz 1 und 6 SGB V, dass Leistungserbringer wie zum Beispiel Ärzte Sozialdaten unmittelbar an den MDK übermitteln sollen, wenn dieser von der Krankenkasse mit einem Gutachten beauftragt wurde. In der Praxis wurde diese Vorgabe aber regelmäßig nicht eingehalten. Vielmehr schickten Ärzte die Unterlagen in einem Umschlag an die Krankenkasse, die sie dann an den Medizinischen Dienst weiterleitete. Zwar waren die Umschläge regelmäßig verschlossen und trugen die Aufschrift

„Ärztliche Unterlagen nur vom MDK zu öffnen“. Aber tatsächlich wurden die Umschläge häufig von Krankenkassenmitarbeitern geöffnet. Selbst dann, wenn die Umschläge verschlossen beim MDK ankamen, sandte er die Unterlagen oft offen wieder an die Krankenkasse zurück. Die Bundesdatenschutzbeauftragte sowie die Linksfraktion im Deutschen Bundestag haben diese Praxis gerügt. Der durch das Krankenhausstrukturgesetz geänderte § 276 SGB V stellt jetzt klar, dass eine direkte Übermittlung an den Medizinischen Dienst auch dann geboten ist, wenn die Unterlagen von der Krankenkasse für den Medizinischen Dienst angefordert wurden. Das Umschlagverfahren ist damit abgeschafft.
Sofern Versicherte selbst Unterlagen übersenden, die der MDK angefordert hat, sollten sie die Unterlagen gleichfalls direkt verschicken und nicht über die Krankenkasse. Notfalls sollten die Unterlagen zumindest in einem verschlossenen Zweitumschlag mit dem oben erwähnten Vermerk verschickt werden.

4. Transparenz in der Krankenversicherung – Kernfragen

4.1. Welche Auskünfte können Versicherte von der Krankenkasse verlangen?

Von der Krankenkasse können Versicherte zunächst nach § 305 SGB V die schon erwähnte Leistungsübersicht verlangen, und zwar für einen Zeitraum von mindestens 18 Monaten vor Antragstellung. Den Leistungserbringern darf die Krankenkasse nicht mitteilen, dass der Versicherte diese Übersicht verlangt hat. Die Krankenkasse darf den Leistungsüberblick nur auf Anforderung und zu dem Anforderungszweck erstellen. Sie darf hingegen nicht eine Gesamtaufstellung der vom Versicherten in Anspruch genommenen Leistungen vorhalten („Patientenprofil“). Eine solche Gesamtaufstellung „auf Vorrat“ benötigt die Krankenkasse auch nicht, weil sie ohnehin die Abrechnungsdaten der ärztlichen und nichtärztlichen Leistungserbringer aus unterschiedlichen Quellen erhält und in der Übersicht zwischen ärztlichen und ärztlich verordneten Leistungen unterscheiden muss.
Darüber hinaus haben Versicherte auch in der Krankenversicherung den bereits erwähnten allgemeinen Anspruch auf Auskunft über zu ihrer Person gespeicherte Sozialdaten, deren Verbreitung und den Zweck der Speicherung (§ 83 SGB X).
Hinzu kommt das allgemeine Akteneinsichtsrecht im Verwaltungsverfahren (§ 25 SGB X), das auch in der Krankenversicherung und auch gegenüber dem Medizinischen Dienst Anwendung findet (§ 276 Abs. 3 SGB V).
Ferner hat die Krankenkasse auch (wie andere Sozialbehörden) Auskunfts-, Beratungs- und Belehrungspflichten gegenüber ihren Versicherten. Speziell für Krankenkassen gilt außerdem, dass sie Versicherte auf Verlangen über zugelassene Leistungserbringer, verordnungsfähige Leistungen und deren Bezugsquellen zu informieren haben (§ 305 Abs. 3 SGB V). Zu diesem Zweck bieten die Krankenkassen auf ihren Online-Portalen in der Regel Recherche-Instrumente an, mit denen sich solche Informationen ermitteln lassen. Bei der Verletzung individueller Belehrungs-, Beratungs- und Auskunftspflichten kann unter weiteren Voraussetzungen der Versicherte so zu stellen sein, wie er bei ordnungsgemäßem Verhalten der Krankenkasse stünde. Auch eine Haftung der Krankenkasse kann in Betracht kommen.[*] Allerdings müs-

[*] In Frage kommen je nach Konstellation: Sozialrechtlicher Herstellungsanspruch, Amtshaftungsanspruch, Wiedereinsetzung in den vorigen Stand, längere Fristen.

sen die Krankenkassen nicht in jedem Fall so beraten, dass der Versicherte eine optimale Gestaltung wählen kann. Blindes Vertrauen in die Beratung ist deshalb nicht gerechtfertigt. Bestimmte Praxen bei Krankenkassen – etwa Formen des „Herausdrängens“ aus dem Krankengeldbezug ohne adäquate Belehrung – bewegen sich in einem rechtlichen Graubereich.

4.2. Wie weit reicht das Akteneinsichtsrecht?

Das Akteneinsichtsrecht nach § 25 SGB X ist begrenzt. So bezieht sich das Einsichtsrecht vor Ergehen einer Verwaltungsentscheidung in der Sache nicht auf Entscheidungsentwürfe und Vorbereitungsarbeiten. Bei berechtigten Interessen anderer Personen können Teile des Akteninhalts geheim gehalten werden. Ferner muss Akteneinsicht nur gestattet werden, soweit dies zur Geltendmachung oder Verteidigung rechtlicher Interessen notwendig ist. Die Akten können im Original eingesehen werden. Die Akten können den Berechtigten außerdem in Kopie (elektronisch oder in Papierform) überlassen werden. Ob es zulässig ist, wenn die Behörde (z. B. die Krankenkasse) Einsichtsberechtigte auf die Einsicht vor Ort verweist, statt auf Verlangen eine Kopie der ganzen Akte anzufertigen, ist fraglich. Das Bundessozialgericht lässt dies offen (30.11.1994, Az.: 11 RAr 89/94), fordert aber, dass die zu kopierenden Teile der Akte genau bezeichnet werden, wenn nicht eine Kopie der ganzen Akte verlangt wird. Dazu wird in der Regel die Einsichtnahme vor Ort nötig werden. In der Akte „suchen“ muss die Behörde nicht. Auf Überlassung der Akten im Original besteht im Verwaltungsverfahren auch für Prozessbevollmächtigte kein Anspruch (im Widerspruchs- und Klageverfahren gelten hingegen die §§ 120 Abs. 2 Satz 2, 84a SGG). Allerdings darf einzelnen Prozessbevollmächtigten, wenn die Behörde in vergleichbaren Fällen stets die Akten überlässt, nicht willkürlich die Überlassung verweigert werden.
Die Krankenkasse kann unter Umständen einen Arzt damit beauftragen, den Inhalt der Akten zu vermitteln. Das soll insbesondere dann geschehen, wenn die Akteneinsicht der Gesundheit des Einsicht Verlangenden Schaden zufügen würde.
Wie bereits erwähnt, kann das Akteneinsichtsrecht nur ausnahmsweise isoliert (das heißt nicht zusammen mit einem Angriff gegen den abschließenden Verwaltungsakt) gerichtlich durchgesetzt werden. Ein solcher Ausnahmefall kann beispielsweise vorliegen, wenn das Interesse an Akteneinsicht nicht nur der Durchsetzung eines Sozialleistungsanspruchs dient, sondern weitergehende Bedeutung mit Blick auf das informationelle Selbstbestimmungsrecht hat, oder wenn sonst effektiver Rechtsschutz verhindert würde, so das Sozialgericht Stade in seiner bereits erwähnten Entscheidung und das Hessische Landessozialgericht (7.11.2014, Az.: L 6 AS 722/14 B ER).

4.3. Welche Auskünfte können Versicherte von Ärzten verlangen?

Bereits erwähnt wurde der Anspruch auf Einsicht in die Patientenakte (Abschnitt 3.4.). Weil in die Patientenakte auch Arztbriefe aufzunehmen sind (§ 630f Abs. 2 Satz 2 BGB), können Patienten auch Kopien der Arztbriefe verlangen.
Für viele Patienten sind Arztbriefe zunächst unverständlich. Jedoch können Fachbegriffe beispielsweise in Online-Enzyklopädien nachgeschlagen werden. Einige Krankenkassen bieten (nicht nur für Mitglieder zugänglich) ein Suchwerkzeug für Diagnoseschlüssel an. Bei Angabe des Diagnoseschlüssels wird die dazugehörige Diagnose ausgeworfen und kurz erläutert. Schließlich gibt es noch das von der Stiftung Warentest geprüfte Angebot „Was hab ich?“ (https://washabich.de). Im Rahmen dieses

Projekts übersetzen Ärzte und Medizinstudenten ab dem 8. Semester kostenlos Arztbriefe in eine für Laien verständliche Sprache.
Neben dem Anspruch auf Einsicht in die Patientenakte gibt es noch den Anspruch auf die Patientenquittung (§ 305 Abs. 2 SGB V): Ärzte haben Versicherte schriftlich in verständlicher Form über die zu Lasten der Krankenkassen erbrachten Leistungen und deren vorläufige Kosten zu unterrichten. Das muss entweder direkt im Anschluss an die Behandlung geschehen oder mindestens quartalsweise, und zwar spätestens vier Wochen nach Ablauf des Quartals, in dem die Leistungen in Anspruch genommen worden sind. Für die Quittung ist eine Aufwandspauschale von 1 Euro zuzüglich Versand zu zahlen. Krankenhäuser müssen spätestens vier Wochen nach Behandlungsabschluss entsprechend informieren.
Bei Konflikten mit Ärzten finden Patienten Unterstützung bei der Unabhängigen Patientenberatung (UPD), wenngleich diese bislang vom VdK mitgetragene Institution vom Bundesgesundheitsministerium nun an ein krankenkassennahes Privatunternehmen vergeben wurde, was der VdK und seine Partner scharf kritisieren.

5. Gefährdungen des Datenschutzes in der Krankenversicherung

5.1. Übermäßige Datenerhebung und Datenspeicherung

Gefährdet ist der Datenschutz zunächst immer dann, wenn Daten im Übermaß erhoben und gespeichert werden. Denn allein das Vorhandensein von Daten verschafft Zugriffsmöglichkeiten. Wichtige Datenspeicherstellen sind die Krankenkassen, die Kassenärztlichen Vereinigungen und die Leistungserbringer selbst. Jede neu eingeführte Datenspeicherungsberechtigung einer dieser Stellen, die nicht der Einwilligung des Versicherten bedarf, muss deshalb kritisch hinterfragt werden. Bei der Einführung der neuen elektronischen Gesundheitskarte soll diesem Grundsatz durch einen Zustimmungsvorbehalt entsprochen werden. Ferner sollen die erwähnten Löschungsfristen und Datentrennungsgebote eine übermäßige Anhäufung von Daten über eine Person vermeiden.

5.2. Mangelnde Sicherung von Daten gegen unbefugten Zugriff

Wie in anderen Bereichen geht auch im Gesundheitswesen eine Hauptgefahr für personenbezogene Daten von schlechter Sicherung aus. Gründe dafür können Fahrlässigkeit im Einzelfall, aber auch Gleichgültigkeit oder mangelndes Problembewusstsein sein. Letztgenannte Variante stellt das größere Problem dar, weil sie zu einer allgemein laxen Praxis im Umgang mit sensiblen Daten führt. Das betrifft Ärzte und Krankenkassen gleichermaßen.
Mit dem Umschlagverfahren bei der Weiterleitung von Daten an den Medizinischen Dienst wurde bereits ein wichtiges Problemfeld angesprochen (Abschnitt 3.8.). Hinsichtlich der Einführung der elektronischen Gesundheitskarte besteht Streit, ob diese insgesamt eher Verbesserungen oder Verschlechterungen beim Datenschutz mit sich bringen wird. Eine noch intensivere Diskussion um datenschutzrechtliche Standards der elektronischen Gesundheitskarte ist zu erwarten, wenn mehr Details der technischen Umsetzung bekannt sind. Dazu fehlt zur Zeit noch die Infrastruktur. Doch umstritten ist schon jetzt beispielsweise, ob die elektronische Gesundheitskarte nach dem Stand der Technik von morgen ausreichende Sicherungen gegen unbefugten Zugriff gewährleisten kann. Insbesondere die geplante Speicherung von Pati-

entendaten auf Servern könnte problematisch sein. Denn wer die technischen Sicherungen überwindet, kann möglicherweise auf einen Schlag nicht nur einzelne Daten, sondern die Datensätze von tausenden oder Millionen Patienten einsehen.
Allerdings werden auch die heutigen papiergebundenen und elektronischen Datenverarbeitungsverfahren von Datenschützern heftig kritisiert. Gerade Papierunterlagen sind oft ohne jede Sicherung für jedermann zugänglich. Teils liegen sie beispielsweise in Arztpraxen offen auf Schreibtischen herum, sodass auch andere Patienten oder nichtmedizinisches Personal die Daten einsehen können. Auf Monitoren werden Patientendaten teils für jedermann offen einsehbar angezeigt, auch wenn kein medizinisches Personal im Raum ist. Die elektronische Gesundheitskarte könnte bei diesen Problemen Abhilfe schaffen. Ob sie aber insgesamt zu einer größeren Datensicherheit beiträgt, bleibt abzuwarten. Vor allem die Qualität der technischen Umsetzung und die Begrenzung von Zugriffsbefugnissen werden dafür entscheidend sein.
Gewiss von Vorteil für Patienten können die direkt auf der Karte gespeicherten Notfalldaten sein. Sie könnten dazu beitragen, Behandlungsfehler zu reduzieren. Dazu müssten die Daten aber im Ernstfall auch tatsächlich eingesehen werden.

5.3. Ökonomisierung des Gesundheitssystems

Mehr noch als fehlendes Bewusstsein dürfte sich zukünftig der Ökonomisierungsdruck im Gesundheitssystem negativ auf den Datenschutz auswirken. Denn während mangelndem Problembewusstsein durch Aufklärung und Sensibilisierung begegnet werden kann, hat es der Datenschutz schwer, wenn ihm handfeste ökonomische Interessen entgegen stehen. Der Problemkreis kann hier nur aufgerissen werden:
Gefahren drohen zunächst durch den vom Gesetzgeber künstlich erzeugten, marktförmigen Wettbewerb der Krankenkassen untereinander. Trotz des Risikostrukturausgleichs haben Krankenkassen immer noch wirtschaftliche Anreize, gesunde und wohlhabende Versicherte an sich zu binden und krankheitsgefährdete oder ärmere Versicherte in andere Krankenkassen abzudrängen. Es entsteht damit ein ökonomischer Anreiz, Daten missbräuchlich zu verwenden oder in unzulässiger Weise zusammenzuführen, damit die Krankenkasse ein Patientenprofil erstellen kann. Auf Grundlage eines solchen Profils könnten Krankenkassen beispielsweise gezielt bei „teuren“ Versicherten Leistungen besonders zurückhaltend gewähren, um Kosten zu sparen und diese Versicherten langfristig zu „vergraulen“. Vergleichbare rechtswidrige Praxen sind in der Vergangenheit bereits bekannt geworden (Bundestagsdrucksache 18/7784). So hatte eine Krankenkasse bei „teuren“, zugleich einkommensschwachen Mitgliedern ausstehende Zusatzbeiträge verschärft eingetrieben und hatte ihren Mitarbeitern finanzielle Anreize für die Anwerbung von Neumitgliedern nur gewährt, wenn diese Neumitglieder einkommensstark waren.
In den Kontext der Ökonomisierung gehört auch das neue Modell von Boni für gesundheitsbewusstes Verhalten (§ 65a SGB V). Was wie ein harmloser neuer Ansatz der Gesundheitsprävention wirken mag, bricht mit dem Prinzip, dass in der Sozialversicherung Beiträge und Leistungen risikounabhängig gestaltet werden. Durch den Einzug der Wettbewerbslogik der privaten Versicherungswirtschaft in die gesetzliche Krankenversicherung gerät dieses Prinzip unter Druck. Das bleibt für den Datenschutz nicht ohne Auswirkungen. Denn spätestens dann, wenn Bonussysteme nicht mehr nur an die Teilnahme an Präventionsmaßnahmen, sondern an eine gesunde Lebensweise anknüpfen, müssten die Krankenkassen Zugang zu umfassenden Daten über die Gestaltung des Privatlebens Versicherter erhalten.

Auch in der Kooperation von Krankenkassen und Leistungserbringern mit privaten Drittanbietern liegt Gefahrenpotenzial. Bereits jetzt arbeiten beispielsweise viele Ärzte – mit Einwilligung der Patienten – mit Abrechnungsgesellschaften zusammen, wenn es um privat abgerechnete Leistungen geht. Wenn der Trend zum Public-Private-Partnership anhält, könnten in Zukunft Krankenkassen und Leistungserbringern weitergehende Rechte eingeräumt werden, Daten durch Dritte verarbeiten zu lassen, die nur noch einer gelockerten Kontrolle durch öffentliche Stellen unterliegen.

5.4. Freiwillige Preisgabe oder Gefährdung von Daten

Die vielleicht größte Gefahr für personenbezogene Daten geht aber von den Krankenversicherten selbst aus. Sicherungssysteme und strenge Rechtspflichten für Krankenkassen und Ärzte nützen nichts, wenn Patienten selbst ohne jede Sicherung Daten sammeln oder sie öffentlich zugänglich machen.
So liegt es im Eigeninteresse der Versicherten, dafür zu sorgen, dass Unterlagen unmittelbar und sicher an die Stelle übermittelt werden, für die sie bestimmt sind. Privates sollte nur an Personen weitergegeben werden, die sich als berechtigt legitimieren können. Insbesondere bei unerwarteten E-Mails, die auf Internetseiten verlinken (Phishing) und bei Telefonanrufen Unbekannter sollten keine sensiblen Daten eingegeben beziehungsweise genannt werden – das gilt nicht nur im Gesundheitsbereich. Es liegt aber auch im Interesse Krankenversicherter, Daten nicht unnötig zu erheben. Vor diesem Hintergrund ist der Trend zur permanenten Selbstüberwachung, etwa mittels der zur Zeit beliebten Fitnessarmbänder („Activity Tracker“), kritisch zu sehen. Denn in der kapitalistischen Leistungsgesellschaft wird Selbstoptimierung zunehmend als Obliegenheit von Individuen wahrgenommen, die sich die beispielsweise von Arbeitgebern gestellten Leistungsanforderungen zu eigen machen, statt sich dagegen zu solidarisieren. Diese Selbstoptimierung führt nicht zu verschärfter Ausbeutung von Arbeitskraft und gesellschaftlichem Konformitätsdruck, sondern erfordert auch eine Datengrundlage, die neue Begehrlichkeiten wecken kann – von Krankenkassen, Arbeitgebern und von den großen Onlinedienstanbietern, deren Geschäftsmodell schon heute auf der Vermarktung von Daten beruht.
Dazu gehören etwa personalisierte Werbemodelle von Anbietern sozialer Netzwerke. Je mehr Daten verfügbar gemacht werden, desto leichter wird es für diese Unternehmen, ein Persönlichkeitsprofil zu erstellen. Soweit die Daten öffentlich einsehbar sind, gilt das aber nicht nur für den Anbieter des jeweiligen Dienstes, sondern jedermann kann mit wenig Aufwand ein Persönlichkeitsprofil erstellen. Arbeitgeber, Versicherungsunternehmen und staatliche Geheimdienste können sich dies schon jetzt zunutze machen. Würde das erwähnte Modell des Bonus für gesundheitsbewusstes Verhalten ausgeweitet, könnten sich öffentliche Profile in sozialen Netzwerken auch zur Datenfundgrube für Krankenkassen und Gesundheitsunternehmen entwickeln.

5.5. Ausblick

Das Thema „Datenschutz in der gesetzlichen Krankenversicherung“ ist also mit den detaillierten Regelungen des Sozialgesetzbuches nicht abgeschlossen. Denn die gesundheitspolitischen Entwicklungen der Zukunft sind kaum absehbar. Deshalb gilt es Datenschutz und Transparenz für Versicherte auch in Zukunft gegen neue Gefährdungen zu verteidigen und, wo möglich, auszubauen. Für Datenschutz und Patientenrechte setzt sich auch der VdK im Rahmen seiner sozialpolitischen Arbeit ein.