Der zukünftige Einsatz von Chipkarten im deutschen Gesundheitswesen

Gerrit Hornung

Universität Kassel
gerrit.hornung@uni-kassel.de

Zusammenfassung

Das am 26. September 2003 vom deutschen Bundestag verabschiedete Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GMG)[1] ordnet den Einstieg in eine grundlegende Neuordnung der Prozessabläufe und Datenverarbeitungsvorgänge im Gesundheitswesen an. Wesentliche Bausteine dieser neuen Struktur sind die elektronische Gesundheitskarte und der elektronische Heilberufsausweis. Für diese ergeben sich sowohl aus dem Signatur- wie dem Datenschutzrecht technische Gestaltungsanforderungen, die im Folgenden auf ihre Umsetzbarkeit hin überprüft werden. In signaturrechtlicher Hinsicht fehlen bislang hinreichende Grundlagen für die Zertifikatsstruktur und -verwaltung und für die Langzeitarchivierung elektronischer medizinischer Dokumente. Im Datenschutzbereich gibt es bislang noch keine Entscheidung über den genauen Speicherort der Daten; die bisherigen Zugriffsregelungen sind insoweit unzureichend, als sie keine hinreichende Abstufungsmöglichkeit vorsehen. Im Bereich des Auskunftsrechts über medizinische Daten geht das GMG über die bisherige Rechtsprechung des BGH hinaus. Neben diesen datenschutzrechtlichen Anforderungen führt insbesondere das Problem der Datensicherheit zur Notwendigkeit einer komplexen, hochverfügbaren technischen Infrastruktur, die Entwickler und Systemintegratoren vor neue Herausforderungen stellt.

1 Das Gesundheitssystemmodernisierungsgesetz

1.1 Regelungen zur Gesundheits- und Heilberufskarte

Das GMG sieht in § 291a SGB V die Einführung einer elektronischen Gesundheitskarte bis spätestens zum 1.1.2006 vor. Inhalt und Funktionsweise der Karte gliedern sich in einen verpflichtenden und einen freiwilligen Bereich. Die drei verpflichtenden Teile (§ 291a Abs. 2 SGB V) sind die Speicherung der Versicherungsstammdaten, die Ablage des Berechtigungsnachweises zur Inanspruchnahme von Leistungen in den Mitgliedsstaaten der Europäischen Union sowie die Daten zum Transport des so genannten elektronischen Rezepts. Dieses soll einen medienbruchfreien Transport von der Ausstellung bis zur Abrechnung ermöglichen. Da es verpflichtend eingeführt wird, wird es zum ersten echten Test der neuen Telematik-Infrastruktur werden.

§ 291a Abs. 3 SGB V enthält demgegenüber diejenigen Anwendungen, zu deren Ausführung die Gesundheitskarte zwar in der Lage sein muss, bezüglich derer der Inhaber jedoch entscheiden kann, ob er sie einsetzen möchte. Im Einzelnen sind dies die Ablage medizinischer

[1] BGBl. I, 2190. Beim GMG handelt es sich um ein Artikelgesetz, das eine Vielzahl von bisherigen Gesetzen ändert. Die wesentlichen Änderungen finden sich im 5. Buch des Sozialgesetzbuches (SGB V).

P. Horster (Hrsg.) · D•A•CH Security 2004 · syssec (2004) 226-237.

Notfalldaten, der elektronische Arztbrief, die elektronische Patientenakte, die Arzneimitteldokumentation, vom Patienten selbst zur Verfügung gestellte Informationen und Daten über in Anspruch genommene Leistungen. Hier ist eine Information des Versicherten und eine spezifische, zu dokumentierende Einwilligung erforderlich, die auf einzelne Anwendungen beschränkt und jederzeit widerrufen werden kann (§ 291a Abs. 3 Sätze 2-4 SGB V). § 291a Abs. 6 Satz 1 SGB V normiert ein besonderes Löschungsrecht. Auf Verlangen des Versicherten sind sowohl die Daten des elektronischen Rezepts wie die der freiwilligen Anwendungen nach Abs. 3 Satz 1 zu löschen.

Für den elektronischen Heilberufsausweis regelt das GMG lediglich die Fähigkeit zur Erstellung qualifizierter elektronischer Signaturen und seine Funktion als Zugriffsinstrument auf die auf oder mittels der Gesundheitskarte gespeicherten Daten (s.u.). Es erfolgt keine Anordnung über zu speichernde Daten oder ausgebende Stellen.

1.2 Regelungen zur Zugriffsberechtigung

§ 291a Abs. 4 Satz 1 SGB V beschränkt den Zugriff auf das elektronische Rezept auf Ärzte, Zahnärzte, Apotheker, sonstiges pharmazeutisches Personal und das sie unterstützende Apothekenpersonal und sonstige Erbringer ärztlich verordneter Leistungen. Die Funktionen nach § 291a Abs. 3 SGB V (außer den Daten über in Anspruch genommene Leistungen) sind ausschließlich Ärzten, Zahnärzten und Apothekern, die Notfalldaten auch anderen Angehörigen eines Heilberufes zugänglich. Auch die Versicherten haben nach § 291a Abs. 4 Satz 2 SGB V ein Zugriffsrecht auf alle Daten mit Ausnahme der Stammdaten und des Auslandskrankenscheins. Damit ist jedoch, wie sich aus dem Zusammenspiel mit § 291a Abs. 5 Satz 3 SGB V (Bindung an einen elektronischen Heilberufsausweis) ergibt, mit Ausnahme der selbst zur Verfügung gestellten Daten kein eigener technischer Lesezugriff des Versicherten gemeint.

§ 291a Abs. 5 Satz 1 SGB V bindet jedes Erheben, Verarbeiten und Nutzen von Daten der *freiwilligen* Funktionen mittels der Gesundheitskarte an das Einverständnis des Versicherten. Satz 2 verlangt hier (mit Ausnahme der Notfalldaten) eine technische Absicherung der Autorisierung des Versicherten im Einzelfall. Dies kann z.B. mittels PIN oder biometrischem Merkmal erfolgen. Beide Verfahren werden nicht im Gesetz, wohl aber in der Begründung angesprochen (BT-Drs. 15/1525, 145). Nach gegenwärtigem Stand der Technik stellt die PIN allerdings das einzige praktikable Verfahren dar. Der Einsatz von Biometrie ist in Anbetracht des engen Zeitrahmens der Einführung der Gesundheitskarte unrealistisch, da es bislang kein Verfahren gibt, das eine der PIN vergleichbare Sicherheit garantiert und für den Einsatz bei allen Krankenversicherten in Deutschland geeignet wäre (s. zur Leistungsfähigkeit biometrischer Verfahren insoweit [TAB02]). Aus diesem Grund kommt der Einsatz von Biometrie lediglich für eine spätere Kartengeneration in Betracht.

Im Umkehrschluss ergibt sich, dass für die verpflichtenden Funktionen des Zugriffs auf die Stammdaten und des elektronischen Rezepts eine technische Autorisierung nicht erforderlich ist. Allerdings ist nach § 291a Abs. 5 Satz 3, 1. Halbsatz SGB V der Zugriff auf die Daten des elektronischen Rezepts und der freiwilligen Funktionen nach Abs. 3 Satz 1 in jedem Einzelfall an den Einsatz eines elektronischen Heilberufsausweises gekoppelt (im Fall des Rezepts auch eines anderen Berufsausweises), der „über eine qualifizierte elektronische Signatur verfügen“[2]

[2] Gemeint ist die Möglichkeit zur Erstellung qualifizierter elektronischer Signaturen. Elektronische Signaturen sind nach § 2 Nr. 1 SigG Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch

muss. Der Zugriff auf die selbst zur Verfügung gestellten Daten ist nach § 291a Abs. 5 Satz 3, 1. Halbsatz SGB V auch mit einer eigenen Signaturkarte des Versicherten möglich, wenn diese über die Möglichkeit zur Erstellung qualifizierter elektronischer Signaturen verfügt. Satz 4 lässt einen Zugriff durch Hilfspersonen, die nicht über einen eigenen elektronischen Heilberufsausweis verfügen, im Umfang ihrer Berechtigung dann zu, wenn sie durch einen Träger eines solchen Ausweises oder eines entsprechenden Berufsausweises autorisiert wurden und der Zugriff und die Autorisierung „nachweisbar elektronisch protokolliert werden".

Der Zugriff auf das elektronische Rezept kann schließlich vom Versicherten auch selbst freigeschaltet werden (§ 291a Abs. 5 Satz 4 SGB V). Damit soll ein Einlösen des Rezepts im Ausland ermöglicht werden. Des Weiteren sind mindestens die letzten 50 Zugriffe auf die Gesundheitskarte nach § 291a Abs. 6 Satz 2 SGB V zu Zwecken der Datenschutzkontrolle zu protokollieren. Satz 3 bestimmt, dass die Protokolldaten nur für diesen Zweck eingesetzt werden dürfen. Sie sind außerdem nach Satz 4 durch geeignete Vorkehrungen gegen zweckfremde Verwendung und sonstigen Missbrauch zu schützen.

1.3 Regelungen zum Aufbau von Infrastrukturen

§ 291a Abs. 7 Satz 1 SGB V verpflichtet die Spitzenverbände der Krankenkassen, die Kassenärztliche Bundesvereinigung, die Kassenzahnärztliche Bundesvereinigung, die Bundesärztekammer, die Bundeszahnärztekammer, die Deutsche Krankenhausgesellschaft sowie die für die Wahrnehmung der wirtschaftlichen Interessen gebildete maßgebliche Spitzenorganisation der Apotheker auf Bundesebene zur Entwicklung einer Informations- Kommunikations- und Sicherheitsinfrastruktur für den Einsatz von Telematik im Gesundheitswesen. Das Gesetz nennt beispielhaft die elektronische Gesundheitskarte, das elektronische Rezept und die elektronische Patientenakte. Die Vereinbarung bedarf nach Satz 2 der Genehmigung durch das Bundesministerium für Gesundheit und Soziale Sicherung. Zuvor ist dem Bundesdatenschutzbeauftragten Gelegenheit zur Stellungnahme zu gegeben. Kommt keine Vereinbarung zustande, wird das Ministerium in § 291a Abs. 7 Satz 4 SGB V dazu ermächtigt, nach Anhörung der Beteiligten den Inhalt der Infrastruktur durch eine Rechtsverordnung, die der Zustimmung des Bundesrates bedarf, festzulegen.

Ebenso wie diese Regelung zur Informations- Kommunikations- und Sicherheitsinfrastruktur wird auch das Verfahren der Bestimmung von Inhalt und Struktur der Daten der freiwilligen Applikationen der elektronischen Gesundheitskarte normiert. In § 291a Abs. 3 Satz 6 bis 9 SGB V finden sich insoweit im Wesentlichen wortgleiche Bestimmungen.

1.4 Regelungen zur Verhinderung von Missbrauch

§ 291a Abs. 8 SGB V enthält weitere Schutzvorschriften für die im Zusammenhang mit der elektronischen Gesundheitskarte verwenden Daten. Danach ist es verboten, vom Versicherten zu verlangen, den Zugriff auf das elektronische Rezept und alle Informationen nach Abs. 3 Satz 1 anderen als berechtigten Personen oder zu anderen Zwecken als denen der Versorgung und Abrechnung zu gestatten. Über eine solche Gestattung darf überdies keine Vereinbarung getroffen werden, und aus der Bewirkung oder Verweigerung des Zugriffs dürfen weder Vor-

mit ihnen verknüpft sind und die zur Authentifizierung dienen. Der Heilberufsausweis „verfügt" deshalb nicht über eine solche Signatur, sondern stellt sie her.

noch Nachteile erwachsen. Verstöße gegen § 291a Abs. 8 SGB V werden nach § 307 Abs. 1 SGB V als Ordnungswidrigkeit mit einem Bußgeld von bis zu 50.0000 € geahndet.

Während § 291a Abs. 8 SGB V damit Einflussnahmen auf den Versicherten als Ordnungswidrigkeit normiert, ist ein Zugriff auf die auf oder mittels der Gesundheitskarte gespeicherten Daten, der entgegen den Zugriffsbefugnissen des § 291a Abs. 4 Satz 1 SGB V erfolgt, nach § 307a Abs. 1 SGB V eine Straftat. Sie ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bedroht. Bei einem Handeln gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht kann nach Abs. 2 eine Freiheitsstrafe von bis zu drei Jahren verhängt werden.

Nach dem Gesetz (§ 291a Abs. 2 Satz 2 und Abs. 3 Satz 5 SGB V) findet außerdem die Transparenzregel des § 6c BDSG in den Fällen der § 291a Abs. 1 und Abs. 2 SGB V Anwendung. Schließlich wird der Beschlagnahmeschutz in § 97 Abs. 2 StPO ausgeweitet. Dieser erstreckt sich nunmehr auch auf die Gesundheitskarte selbst, sowie auf Dienstleister, die für Ärzte, Zahnärzte, Psychotherapeuten, Apotheker und Hebammen personenbezogene Daten erheben, verarbeiten oder nutzen.

1.5 Telematik-Expertise der Wirtschaft

Von Seiten der deutschen Industrie wurde parallel zum Gesetzgebungsprozess eine Expertise zur Einführung einer Telematik-Architektur im Gesundheitswesen verfasst [BVV+03]. Sie geht von nahezu identischen Voraussetzungen für die Umsetzung aus, insbesondere von einem verpflichtenden elektronischen Rezept und freiwilligen weiteren Funktionen, dem PIN-Schutz der Karte und dem Zugriff mittels eines elektronischen Heilberufsausweises. Die Daten sollen wahlweise auf der Karte oder auf Servern abgelegt werden. Die Expertise befasst sich auch näher mit den Heilberufsausweisen, die von denselben Institutionen wie bisher ausgegeben werden sollen.

Die Hauptziele des Gesamtvorhabens „Telematik im Gesundheitswesen“ liegen in der effektiveren Behandlung und Kostenreduzierung. Auf der Seite des Staates und der Krankenkassen sind die Pläne vor allem finanziell motiviert. Man erhofft sich mittelfristig Einsparungen von bis zu 1 Mrd. € pro Jahr.[3] Die Anlaufinvestitionen sollen sich bereits innerhalb von ein bis zwei Jahren amortisieren. Der Zeitraum wäre damit vergleichbar mit dem bei der Einführung der Krankenversicherungskarte [Bize02, 36].

2 Umsetzbarkeit signaturrechtlicher Normen

Die höchsten signaturrechtlichen Anforderungen im System der Gesundheitskarte bestehen an den elektronischen *Heilberufsausweis* (Health Professional Card) Die im Gesetz vorgesehene Eignung für qualifizierte Signaturen ist erforderlich, weil nach § 126a BGB nur so die signierten Dokumente die bisherigen Verfahren ersetzen können, wenn für diese die Schriftform vorgeschrieben ist. Hieran knüpfen sich allerdings Folgeprobleme: die Zertifikatsstruktur der Heilberufsausweise muss eine Interoperabilität gewährleisten, die bei den bisher verfügbaren Systemen nicht gegeben ist. Ungeklärt ist auch die Frage, wer den Heilberufsausweis ausstellen und die Zertifikate anbieten soll. Für die Mehrzahl der Leistungserbringer kommen hier die jeweiligen Kammern in Betracht, die auch für die bisherigen Papiere verantwortlich sind.

[3] So die Begründung des Gesetzesentwurfs, BT-Drs. 15/1525, 173. Zur Motivation s. a. [BVV+03, 5, 14ff.; Diet03, 267ff.].

Die Kammern könnten sich entweder auf die Ausstellung der nach § 5 Abs. 2 Satz 2 SigG erforderlichen Nachweise über die Berufszugehörigkeit beschränken oder die Ausweise selbst ausgeben und dabei evt. zusätzlich auch als – ggf. virtuelle – Zertifizierungsdiensteanbieter die Zertifikate verwalten. Für nicht kammergebundene Berufe wie Hebammen und Krankengymnasten ist allerdings auf jeden Fall eine alternative Organisation erforderlich. Die Berufsbescheinigungen können nach § 7 SigG entweder in das Hauptzertifikat oder in ein gesondertes Attribut-Zertifikat aufgenommen werden.

Die Einführung von Telematik im Gesundheitswesen stellt in diesem Zusammenhang insbesondere die *Langzeitarchivierung elektronischer Dokumente* vor immense Herausforderungen. Die Telematik-Expertise beschränkt sich hier auf den allgemeinen Verweis auf bereits verfügbare Archivierungsverfahren [BVV+03, 55, 59f.]. Demgegenüber muss aber betont werden, dass bislang keine Erfahrungen mit der Archivierung über einen Zeitraum von mindestens zehn Jahren (Regelfall nach § 10 Abs. 3 der Musterberufsordnung für Ärzte), in Einzelfällen bis zu 30 Jahren (Röntgenbehandlungen), bestehen. Die archivierten Daten und die verwendeten Signaturen müssen nach § 17 SigV immer wieder neu signiert werden. Für ein Verfahren, das dies datenschutz- und signaturgesetzkonform und für große Archive performant ermöglicht, wurde bisher erst ein Prototyp in dem Forschungsprojekt ArchiSig entwickelt [BrPo03]. Um diesen Ansatz fortzuführen und zu einem verlässlichen Archivierungssystem zu entwickeln, sind noch große Anstrengungen erforderlich.

Für die elektronische *Gesundheitskarte* gibt es demgegenüber keine Anforderungen des Signaturrechts. Sie muss zwar nach § 291 Abs. 2a Satz 3 SGB V technisch geeignet sein, Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen. Für den Einsatz der Gesundheitskarte innerhalb des Gesundheitswesens bestehen jedoch keine weiteren Anforderungen, weshalb es sich noch nicht einmal um fortgeschrittene Verfahren nach § 2 Nr. 2 SigG handeln muss. Nach letzten Plänen soll allerdings auch die Gesundheitskarte eine Mikroprozessorkarte mit einem zertifizierten Betriebssystem sein. Sollte die Karte neben den gesetzlichen Funktionen noch über hinreichend Speicher- und Verarbeitungskapazitäten verfügen, könnte damit optional die Möglichkeit zur Verwendung qualifizierter Signaturverfahren gegeben werden. Die elektronische Gesundheitskarte könnte damit parallel oder alternativ zu anderen Trägermedien (Digitaler Personalausweis, elektronischer Dienstausweis) zu einem Verbreitungsweg für elektronische Signaturverfahren werden. Die Einrichtung eines solchen Verbreitungswegs ist insbesondere deshalb von großer Wichtigkeit, weil nach den Plänen der Bundesregierung am 1.1.2006 das System der „Jobkarte“ eingeführt werden soll [BReg03, 9]. Hierbei handelt es sich – entgegen dem Wortlaut – nicht um ein Karten-, sondern um ein Anwendungsprojekt, das jedoch bei ca. 40 Mio. Beschäftigten in Deutschland den Besitz einer Signaturkarte voraussetzen wird, die zur Erstellung qualifizierter Signaturen in der Lage ist.

Schließlich kann nach § 291a Abs. 5 Satz 3, 1. Halbsatz SGB V auch eine *eigene Signaturkarte des Versicherten*, die über ein qualifiziertes Zertifikat verfügt, für den Zugriff auf selbst zur Verfügung gestellte Daten auf der Gesundheitskarte zum Einsatz kommen. Dies stellt jedoch keine weitere Anforderung an die eigene Karte, sondern an die Verwaltung von Zugriffsrechten auf der Gesundheitskarte dar.

3 Datenschutzrechtliche Herausforderungen

Patienten sind unter Datenschutzgesichtspunkten in einer *widersprüchlichen Situation*: die Preisgabe von Gesundheitsinformationen bedingt die Speicherung, Verarbeitung und Nutzung

von sensiblen Daten, gleichzeitig ist dem behandelnden Arzt eine optimale Versorgung jedoch nur dann möglich, wenn er über alle relevanten Informationen verfügt. Das geltende Recht löst diesen Widerspruch so, dass der Versicherte frei darüber bestimmen kann, welche Daten er offenbart, ihm im Fall der Preisgabe aber Schutzmechanismen gegen eine nicht autorisierte Verwendung zur Verfügung stehen. Dies sind insbesondere die Schweigepflicht der Informationsempfänger (diese ergibt sich aus § 203 StGB, der standesrechtlichen Norm des § 9 der Musterberufsordnung für Ärzte und dem Behandlungsvertrag, [Bäum98, 400; KlMe01, 27ff]), das Zeugnisverweigerungsrecht des Arztes, anderer Beteiligter im Gesundheitswesen und deren Hilfspersonen in einem Prozess gegen den Versicherten (§§ 53 Abs. 1 Nr. 3, 53a StPO), sowie der Beschlagnahmeschutz für Mitteilungen, Aufzeichnungen und Befunde gegenüber Strafverfolgungsbehörden (§ 97 Abs. 1 StPO). Dieses Schutzsystem muss auch im Konzept der elektronischen Gesundheitskarte Bestand haben.

3.1 Abgelegte Daten und Speicherort

Angaben über die Gesundheit sind *besondere Arten personenbezogener Daten* (§ 3 Abs. 9 BDSG). Erfasst sind alle auf oder mittels der Gesundheitskarte erhobenen, verarbeiteten oder genutzten Daten mit Ausnahme von Stammdaten, elektronischem Auslandskrankenschein und Angaben, die wie ein Organspendeausweis keinen Bezug zur Gesundheit haben. Auch das elektronische Rezept ist betroffen, da aus einer Verschreibung unmittelbare Rückschlüsse auf die Gesundheit gezogen werden können. Daten nach § 3 Abs. 9 BDSG unterliegen Verarbeitungsbeschränkungen, die jedoch für Zwecke der medizinischen Versorgung weitgehend aufgehoben sind (§ 28 Abs. 7 BDSG).

Für die Daten, die im System der Gesundheitskarte anfallen, gibt es *mehrere denkbare Aufbewahrungsorte*, nämlich eine Speicherung auf der Karte selbst, auf zentralen Servern oder innerhalb einer verteilten Datenhaltung, das heißt in dezentral-vernetzten Serverstrukturen [BWB+02, 14ff.; Herm00, 9ff.]. Das GMG legt sich hier nur bezüglich der Stammdaten fest, die auf die Karte aufgebracht werden sollen. Für die übrigen Daten schlägt die Telematik-Expertise eine Wahlmöglichkeit des Versicherten zwischen einer Speicherung auf der Karte und einer Serverlösung vor [BVV+03, 13, 36]. Da hierfür eine zweigleisige Infrastruktur erforderlich wäre, ist dies jedoch unrealistisch. Für die elektronische Patientenakte, in weiten Bereichen auch für den Arztbrief, wird überdies aufgrund der Menge der zu speichernden Daten die Kartenvariante ausscheiden und eine andere Speicherform zu wählen sein. Unter Verhältnismäßigkeitsgesichtspunkten ist hier allerdings *auf die zentrale Servervariante zu verzichten*. Zentrale Datensammlungen erhöhen die Attraktivität von internen und externen Angriffen und erleichtern Profilbildungen und Zweckentfremdungen [KonD01; BWB+02, 16].

Eine Speicherung auf der Karte verschafft demgegenüber dem Versicherten die ausschließliche physische Obhut über seine Daten und ist deshalb die am wenigsten eingriffsintensive Lösung. Sofern der Speicherplatz auf der Karte ausreicht, ist deshalb diese Variante zu verwenden. Sie birgt zwar Risiken bei Verlust oder Beschädigung der Gesundheitskarte. Dies bedeutet jedoch keinen vollständigen Datenverlust, weil schon zu Abrechnungszwecken und zur Beweisführung in einem möglichen Arzthaftungsprozess weiterhin eine Dokumentation beim Leistungserbringer erfolgen wird [BVV+03, 49; Bize02, 37]. Die insoweit bestehenden Dokumentationspflichten werden durch das GMG nicht verändert. Eine ausschließliche Ablage wichtiger Gesundheitsdaten auf der Gesundheitskarte wäre auch nicht praktikabel. Für den Fall des Verlusts der Karte wären die Daten unwiederbringlich verloren; der Zugang zu ihnen würde außerdem in das Belieben des Versicherten gestellt – dieser ist jedoch der wahrschein-

lichste Prozessgegner des Arztes im Haftungsfall. Eine totale Datenhoheit des Versicherten mittels der Chipkarte ist also nicht möglich. Für den behandelnden Arzt bedeutet dies gleichzeitig, dass er wie bisher über ein paralleles Dokumentationssystem verfügen muss.

3.2 Zugriffsberechtigungen

Der Versicherten ist auch innerhalb des Gesundheitswesens befugt, darüber zu entscheiden, wem gegenüber er welche Informationen offenbart; die ärztliche Schweigepflicht gilt auch zwischen Ärzten [BGH91; UlHe99, 202]. Hieraus ergibt sich unmittelbar das Erfordernis eines *abstufbaren Zugriffsschutzes* im System der Gesundheitskarte. Dieser ist im GMG bislang *nicht hinreichend umgesetzt*. Schon die Speicherung der Versicherungsstammdaten ohne jeden Zugriffsschutz ist problematisch, weil diese um eine Angabe zum Zuzahlungsstatus erweitert werden. Aus einer Zuzahlungsbefreiung, die bei Erreichen der Zuzahlungsobergrenze von 2% des Bruttoeinkommens (bzw. 1% für chronisch Kranke) erteilt wird, kann jedoch auf eine schwerwiegende oder chronische Erkrankung des Versicherten geschlossen werden.

Das Auslesen des elektronischen Rezepts ohne technische Autorisierung des Karteninhabers, aber unter Einsatz eines elektronischen Heilberufsausweises ist demgegenüber datenschutzrechtlich hinnehmbar, weil es dem bisherigen Verfahren einer Sicherung der Daten durch Besitz des Versicherten entspricht. Wie bisher kann der Versicherte durch Vorlage (des Papierrezepts oder der Gesundheitskarte) darüber entscheiden, wer Zugriff auf das Rezept hat. Der Schutz wird sogar leicht erhöht, weil im Unterschied zum papierbasierten Verfahren im Fall des Verlusts die Rezeptdaten nicht mehr unmittelbar visuell wahrnehmbar sind.

Für die freiwilligen Applikationen ist mit Ausnahme der Notfalldaten eine technische Autorisierung durch den Versicherten erforderlich. Nach dem Gesetz gibt es aber keine Möglichkeit, diese auf einzelne Datenfelder zu begrenzen (auch wenn dies nicht ausgeschlossen ist). Als Sicherung ist vielmehr vorgesehen, dass der Leistungserbringer auf die Daten nur zugreifen darf, „soweit es zur Versorgung der Versicherten erforderlich ist“ (§ 291a Abs. 3 Satz 1 SGB V). Hierin liegt ein *grundsätzlicher Systemwechsel des Informationsflusses im Gesundheitswesen*, weil die Erforderlichkeit nicht durch den Patienten definiert wird, sondern ein objektives Merkmal ist, das nur vom Arzt bestimmt werden kann. Überdies vermag letzterer im Regelfall die Erforderlichkeit eines Datenzugriffs ohne eben diesen Zugriff nicht zu erkennen. Im Ergebnis kann der Versicherte damit nur den Zugriff insgesamt verweigern oder einen Vollzugriff des Leistungserbringers gestatten. Dies kollidiert jedoch mit dem verfassungsrechtlich garantierten Selbstbestimmungsrecht des Patienten, der sensible Informationen (wie Geschlechtskrankheiten) zurückhalten können muss. Es widerspricht außerdem der grundsätzlichen Konzeption des Arzt-Patient-Verhältnisses, das eben nicht paternalistisch einseitige Entscheidungsbefugnisse des Arztes beinhaltet. Um die grundsätzliche Informationshoheit des Patienten auch im System der Gesundheitskarte zu erhalten, muss zumindest die Möglichkeit für diesen geschaffen werden, bestimmte, selbst als sensibel definierte Datenbestände in einen gesonderten Bereich auf der Karte ablegen zu können.

Demgegenüber findet sich im GMG auch eine Regelung, die einen *zu hohen Schutz von Daten* beinhaltet. Das Datenfach für eigene Daten soll ebenfalls PIN-gesichert sein. Dies ist im Regelfall sinnvoll: stellt der Versicherte selbst Daten zur Verfügung, so muss er auch über deren Freigabe im Einzelfall entscheiden können. In einigen Situationen wird der Versicherte aber Daten gerade für Konstellationen zur Verfügung stellen, in denen ihm eine Autorisierung nicht möglich ist. Dies wird sogar in der Gesetzesbegründung angesprochen, die die Anwen-

dungsfälle Patientenverfügung und Organspendeausweis erwähnt (BT-Drs. 15/1525, 145 und die Begründung des ersten Entwurfs, BT-Drs. 15/1170, 123). In der Folge wurde ganz offensichtlich übersehen, dass nach dem Gesetz der – im Regelfall hirntote – Karteninhaber noch mittels einer PIN den Zugriff auf seinen Organspendeausweis freischalten müsste. Dies muss im Wege der Gesetzesänderung korrigiert werden. Dabei ist allerdings zu beachten, dass andere Daten durchaus zu schützen sind. Damit bietet sich eine Zweiteilung des Datenfachs in einen PIN-gesicherten und einen ohne Autorisierung des Versicherten, jedoch nur mit Hilfe eines elektronischen Heilberufsausweises zugänglichen, Teil an.

Das im GMG geregelte Verbot, vom Versicherten Zugriff auf die Daten der Karte zu verlangen, dient der Absicherung der gesetzlichen Zugriffsberechtigungen und soll über die Bußgeldandrohung davon abschrecken, durch die Ausübung *sozialen Drucks* sensible Informationen vom Versicherten zu erlangen. Grundsätzlich besteht dieses Risiko bereits gegenwärtig. Auch ohne weitgehende elektronische Datenverarbeitung im Gesundheitswesen kann auf Versicherte (bspw. von Seiten eines potentiellen Arbeitgebers) Druck ausgeübt werden, Behandlungsergebnisse zu offenbaren, sich untersuchen zu lassen oder Leistungserbringer von ihrer Schweigepflicht zu entbinden. Die Probleme werden aber durch die leichtere Verfügbarkeit der Daten verschärft. So bietet die elektronische Gesundheitskarte, konsequent angewendet, die Möglichkeit der Erstellung einer elektronischen Patientenakte mit allen oder allen wesentlichen Informationen über die gesamte Krankengeschichte des Versicherten. Eine derartige Datensammlung besteht im momentanen System nicht und kann auch unter sozialem Druck kaum durch den Versicherten zusammengeführt werden. Existiert dagegen eine elektronische Patientenakte, so kann er bei einem beliebigen Arzt eine Art „Gesundheitsauszug“ über seine Krankengeschichte und den aktuellen Gesundheitszustand erhalten. Für diesen relativ einfachen Vorgang ist das Risiko psychischen oder materiellen sozialen Drucks erheblich größer. Vor diesem Hintergrund ist die Regelung des GMG unbedingt erforderlich; ihre Wirksamkeit sollte überdies nach einiger Zeit evaluiert werden.

3.3 Serverlösung als Auftragsdatenverarbeitung?

Es ist absehbar, dass im System der Gesundheitskarte Gesundheitsdaten in großem Umfang durch externe Dienstleister verwaltet werden. Im GMG finden sich hierzu keine Regelungen. Das Teledienstedatenschutzrecht ist zwar für manche Anwendungen der Telematik im Gesundheitswesen anwendbar. Es schützt jedoch nur die personenbezogenen Daten der Leistungserbringer, da diese es sind, die den Teledienst nutzen [Herm00, 161]. Die Verantwortung für Patientendaten bestimmt sich damit nach dem allgemeinen Datenschutzrecht.

Hier kommt es vor allem auf die Einordnung der Einbeziehung des Dritten entweder als Datenverarbeitung im Auftrag (§ 11 BDSG) oder Funktionsübertragung an. Im letzteren Fall liegt in dem Datentransfer eine Übermittlung an einen Dritten (§ 3 Abs. 4 Nr. 3 BDSG) mit der Folge, dass die entsprechenden Zulässigkeitsvoraussetzungen einzuhalten sind.

Um eine Datenverarbeitung im Auftrag kann es sich etwa handeln, wenn eine Arztpraxis ein externes Archiv mit der Datenspeicherung beauftragt [Herm00, 181ff.]. Auch für eine einrichtungsübergreifende zentrale Datenhaltung (wie etwa für die elektronische Patientenakte) ist vorgeschlagen worden, hierin eine Datenverarbeitung im Auftrag zu sehen [BWB+02, 7f., 15, 17]. Der Tatbestand des § 11 BDSG ist hier jedoch nicht einschlägig. Für eine Datenverarbeitung im Auftrag ist ein deutliches Über-Unterordnungsverhältnis erforderlich, in dem der Auftragnehmer weisungsgebunden in vollständiger Abhängigkeit hinsichtlich des Umgangs mit

den Daten tätig wird [Hoer03; Walz03]. Das Gesetz erlegt dem Auftraggeber fortwährende Kontrollpflichten auf und verschafft ihm Zutritts- und Weisungsbefugnisse. Dies ist in einem System, in dem ein Dienstleister für eine Vielzahl von Leistungserbringern Daten speichert, praktisch undurchführbar. Die Organisation und der Betrieb eines zentralen Datenverarbeitungssystems im Gesundheitswesen bedingen vielmehr einen Umfang und Komplexitätsgrad, der nicht mehr als Hilfsfunktion betrachtet werden kann. Hier handelt es sich um eine eigene Aufgabe des Dienstleisters. Genau dies ist das Kriterium für eine Funktionsübertragung.

Damit ist für die Einbeziehung externer Dienstleister die Einwilligung des Betroffenen oder eine gesetzliche Ermächtigungsgrundlage erforderlich. Da letztere jedoch nicht existiert, bleibt es allein bei der Einwilligung. Für die freiwilligen Anwendungen der Gesundheitskarte ist dieses Problem allerdings insoweit entschärft, als ohnehin eine solche erforderlich ist. Die Einwilligung muss sich hier aber ausdrücklich auch auf die Datenverwendung durch externe Dritte beziehen, so eine solche erfolgt.

3.4 Unterrichtungspflichten und Auskunftsrecht

Das GMG ordnet für die Gesundheitskarte die Anwendung von § 6c BDSG an. Der Tatbestand dieser Norm ist an sich nicht erfüllt, wenn das Medium lediglich zur Datenspeicherung oder zum Datentransport genutzt wird. Erforderlich ist vielmehr eine automatisierte Verarbeitung auf dem Medium selbst (näher [Horn04]). Durch die Verweisung im GMG gelten die in § 6c BDSG normierten Unterrichtungspflichten jedoch unabhängig von der konkreten technischen Ausgestaltung der elektronischen Gesundheitskarte. Nach Abs. 1 muss über die Identität und Anschrift der jeweiligen Stelle, die Funktionsweise des Mediums, die Ausübbarkeit von Betroffenenrechten und die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichtet werden. Bei der Gesundheitskarte ist insbesondere die Funktionsweise von entscheidender Bedeutung, da diese weitreichende Implikationen für das Recht auf informationelle Selbstbestimmung der Versicherten hat. Die Unterrichtung hat hier in „allgemein verständlicher Form“ zu erfolgen.

§ 6c Abs. 2 BDSG enthält neben dieser Pflicht die Anforderung an die kartenausgebende Stelle, technische Geräte für das Auskunftsrecht unentgeltlich zur Verfügung zu stellen. Die Krankenversicherungen müssen damit (in angemessenem Umfang) für eine entsprechende Infrastruktur sorgen, und zwar unabhängig davon, dass sie selbst verglichen mit den Leistungserbringern die elektronische Gesundheitskarte nur sehr eingeschränkt zur Datenverwendung nutzen werden.

Bezüglich des Auskunftsrechts stellt sich ein weiteres Problem. Der Betroffene hat das Recht, auf das elektronische Rezept und die Daten der freiwilligen Anwendungen zuzugreifen (auch wenn er hierzu außer bei den selbst bereitgestellten Daten die Freischaltung mittels eines elektronischen Heilberufsausweises benötigt). Auch bislang besteht zwar ein Auskunftsrecht des Betroffenen aus dem Behandlungsvertrag. Im Bereich psychiatrischer Behandlung schränkt der BGH dieses jedoch ein, wenn ein schützenswertes Interesse des Patienten selbst, eines Arztes oder Dritten entgegensteht (so genanntes „therapeutisches Privileg“, [BGH85; MeSc99, 74]). Auch über subjektive Notizen des Arztes muss keine Auskunft erteilt werden. Beide Einschränkungen finden sich im nicht GMG und können auch nicht in den Wortlaut interpretiert werden. Das kann dazu führen, dass Leistungserbringer in diesen Bereichen (etwa bei einem Arztbrief mit therapeutischen Angaben) *keine vollständigen Angaben* auf der Gesundheitskarte machen, weil diese dem Versicherten vollständig zugänglich zu machen sind.

4 Gewährleistung von Datensicherheit

Eine der größten Herausforderungen der Telematikstruktur wird die *Datensicherheit* sein. Es ist unabdingbar, dass diese die Authentizität (Urheberschaft), Integrität (Echtheit, Korrektheit und Vollständigkeit), Verfügbarkeit und Revisionsfähigkeit (Nachvollzug der Verarbeitung) von Daten sowie die Nicht-Abstreitbarkeit von Datenübermittlungen sicher und dauerhaft gewährleistet [Bäum98, 402; BWB+02, 11ff.; MeSc99, 74]. Nur dann sind Behandlungserfolg und Rechtssicherheit für alle Beteiligten erreichbar.

Die Vertraulichkeit der Daten ist zunächst durch die Verwendung starker kryptographischer Verfahren bei der Datenspeicherung und -übermittlung sicherzustellen. Zur Gewährleistung von Authentizität und Integrität der verwendeten Daten sind insbesondere elektronische Signaturverfahren zu verwenden [BVV+03, 54f.; BWB+02, 21]. Diese gewährleisten die Zuordnung von Daten zur ausstellenden Instanz, wie auch eine Überprüfbarkeit hinsichtlich nachträglicher Veränderungen. Die im Gesundheitssystem wichtige Sicherstellung der Nichtabstreitbarkeit von Datenübermittlungen kann sowohl in zentralen wie in verteilten Systemen über die Protokollierung der Vorgänge erreicht werden. Darüber hinaus sind für den Fall des Systemsausfalls geeignete Rückfallsysteme vorzuhalten. Dasselbe gilt aber auch, falls ein Beteiligter seine Chipkarte nicht verfügbar oder vergessen hat und wenn diese nicht funktionstüchtig ist. Auch die lokale Infrastruktur, insbesondere die Kartenlesegeräte, können defekt sein. In diesen Fällen sind alternative Verfahren bereitzustellen. Das bedeutet etwa für das elektronische Rezept, dass das papierbasierte Verfahren nicht völlig eingestellt werden kann. Für den Fall des zufälligen Kartenverlusts oder Diebstahls ist es daneben wichtig, eine unmittelbare Sperrmöglichkeit einzurichten.

Im System der Gesundheitskarte kann der Schutz der Daten durch Pseudonymisierungsverfahren sichergestellt werden. Mittels eines dreistufigen Sicherheitskonzepts für das Directory ist es hier möglich, unter der Verwendung von Pseudonymen Daten über Geschäftsvorfälle und Dokumentationen zu erzeugen, auf die mittels Pointern auf der Gesundheitskarte verwiesen wird, aus denen aber nicht umgekehrt auf die Identität des Versicherten zurückgeschlossen werden kann (näher [BVV+03, 27ff.]). In dieselbe Richtung geht die Forderung der Telematik-Expertise, im Gesamtsystem keinen „roten Knopf“ einzurichten, das heißt keine Möglichkeit, unabhängig von einer Patienteneinwilligung unbeschränkt auf die Daten zuzugreifen [BVV+03, 7, 52]. Die Missbrauchsgefahren einer solchen Zugriffsmöglichkeit wären zu groß.

Da an der Telematikstruktur eine Vielzahl von Teilnehmern beteiligt sind, ist zur Herstellung organisatorischer Sicherheit die Bereitstellung ausdifferenzierter Rollenkonzepte erforderlich. Diese müssen danach auf der technischen Ebene in ausdifferenzierten Zugriffsbefugnissen abgebildet werden. Dies ist kartenseitig durch unterschiedliche Karten oder entsprechende Attributzertifikate möglich [BVV+03, 42ff.]. Die Applikationen in der Peripherie sind dann nur denjenigen Teilnehmern zugänglich, die über ein entsprechendes Attribut verfügen.

Ganz allgemein dürfen die Sicherheitsanforderungen an die Gesundheitskarte nicht zu gering sein. Es könnte zwar argumentiert werden, da auf die Daten überwiegend ohnehin nur unter Verwendung eines (hochsicheren und mit qualifizierten Signaturverfahren ausgerüsteten) elektronischen Heilberufsausweises zugegriffen werden könne, müsse die elektronische Gesundheitskarte lediglich geringeren Standards genügen. Es wäre dann jedoch möglich, diese nicht sichere Gesundheitskarte bei jedem Arztbesuch, aber auch bei Verlust durch einen be-

liebigen Heilberufsausweis auszuspähen. Dies ist angesichts der hohen Sensibilität der Daten nicht akzeptabel.

5 Ausblick

Bereits die bislang im GMG normierten Anforderungen bedingen einen komplexen Aufbau der zukünftigen Telematikstruktur im deutschen Gesundheitswesen. Das geltende Recht geht (inklusive der eigenen qualifizierten Karte des Versicherten) vom Einsatz dreier verschiedener Chipkarten, interoperabler Signaturverfahren unterschiedlicher Sicherheitsstufen und einer hochverfügbaren Serverarchitektur zur Datenspeicherung und -übermittlung aus. Die dargelegten datenschutzrechtlichen Anforderungen verkomplizieren den Aufbau weiter. Insbesondere die Erfordernisse der Datensicherheit und der im Einzelfall abstufbaren Zugriffsrechte führen zu Herausforderungen an die eingesetzte Technik (sichere Verschlüsselungsprozesse, Anonymisierungs- und Pseudonymisierungsverfahren, Verwaltung von Zugriffsbefugnissen) und zu kostenintensiven Investitionen. Neue Aufgaben stellen sich daneben für Entwickler von elektronischen Archivierungsverfahren. Ob unter diesen Bedingungen der geplante Starttermin des Systems verwirklicht werden kann, bleibt abzuwarten.

Mit einem Verweis auf Kosten und Aufwand können indes nicht grundlegende Regeln des Arzt-Patient-Verhältnisses und der Patientenautonomie ausgehebelt werden. Zur Beachtung signatur- und datenschutzrechtlicher Regelungen gibt es keine Alternative. Dies gilt umso mehr, als die freiwilligen Komponenten der Telematikstruktur auf die Akzeptanz durch die Versicherten angewiesen sind. Diese ist jedoch ohne einen effektiven Schutz persönlicher Daten nicht zu erwarten. Aus diesem Grund liegt die Sicherung des Rechts auf informationelle Selbstbestimmung der Versicherten im Interesse aller Beteiligten im Gesundheitswesen.

Literatur

[Bäum98] H. Bäumler: Medizinische Dokumentation und Datenschutzrecht, Medizinrecht 1998, 400-405.

[BGH85] Bundesgerichtshof: Urteil vom Urteil vom 02.10.1984 – VI ZR 311/82, Neue Juristische Wochenschrift 1985, 674-676.

[BGH91] Bundesgerichtshof: Urteil vom Urteil vom 10.07.1991 – VIII ZR 296/90, Neue Juristische Wochenschrift 1991, 2955-2958.

[Bize02] J. Bizer: Datenspeicherung in zentralen und peripheren Netzen versus Smart-Cards – wozu digitale Signaturen in der öffentlichen Verwaltung? In: F.von Zezschwitz, K.P. Möller (Hrsg.): Verwaltung im Zeitalter des Internet. Vernetzte Verwaltung und Datenschutz, Nomos, Baden-Baden 2002, 19-70.

[BReg03] Bundesregierung: Informationsgesellschaft Deutschland 2006, abrufbar unter www.bmbf.de/pub/aktionsprogramm_informationsgesellschaft_2006.pdf, 2003.

[BrPo03] R. Brandner, U. Pordesch: Konzept zur signaturgesetzkonformen Erneuerung qualifizierter Signaturen, Datenschutz und Datensicherheit 2003, 354-359.

[BVV+03] BITKOM / VDAP / VHitG / ZVEI: Einführung einer Telematik-Architektur im deutschen Gesundheitswesen. Expertise, abrufbar unter http://www.ztg-nrw.de/down/262/telematik_expertise.pdf, 2003.

[BWB+02] M. Bultmann, R. Wellbrock, H. Biermann, J. Engels, W. Ernestus, U. Höhn, R. Wehrmann, A. Schurig: Datenschutz und Telemedizin. Anforderungen an Medizinnetze. Stand 10/02, http://www.bfd.bund.de/technik/telemed.pdf

[Diet03] G. Dietzel: Politische Verantwortung bei der Entwicklung von Gesundheitstelematik und -informationssystemen, Bundesgesundheitsblatt 2003, 267-271.

[Herm00] A.E. Hermeler: Rechtliche Rahmenbedingungen der Telemedizin. Dargestellt am Beispiel der Elektronischen Patientenakte sowie des Outsourcing von Patientendaten, Beck, München, 2000.

[Hoer03] T. Hoeren: Verantwortliche Stellen. In: A. Roßnagel (Hrsg.): Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung, Beck, München, 2003, 526-545.

[Horn04] G. Hornung: Datenschutz für Chipkarten. Die Anwendung des § 6c BDSG auf Biometrie- und Signaturkarten, Datenschutz und Datensicherheit 2004, i.E.

[KlMe01] I. Klöcker, J. Meister: Datenschutz im Krankenhaus (begründet von T. Barta), 2. Auflage, Dt. Krankenhaus-Verl.-Ges., Düsseldorf, 2001.

[KonD01] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Entschliessung der 62. Konferenz zu Datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte), abrufbar unter www.datenschutz-berlin.de/doc/de/konf/65/top07.htm, 2001.

[MeSc99] H.-J. Menzel, U. Schläger: Der Patient im Gesundheitsnetz, Datenschutz und Datensicherheit 1999, 70-75.

[TAB02] Büro für Technikfolgenabschätzung beim Deutschen Bundestag, Biometrische Identifikationssysteme – Sachstandsbericht, BT-Drs. 14/10005, 2002.

[UlHe99] K. Ulsenheimer, N. Heinemann: Rechtliche Aspekte der Telemedizin – Grenzen der Telemedizin? Medizinrecht 1999, 197-203.

[Walz03] S. Walz: Kommentierung zu § 11 BDSG. In: S. Simitis (Hrsg.): Kommentar zum Bundesdatenschutzgesetz, 5. Auflage, Nomos, Baden-Baden, 2003, 748-768.