Die Gesundheitskarte

Teil 2 – Ausgewählte rechtliche, technische und ökonomische Gesichtspunkte

Univ.-Prof. Dr. Andreas J.W. Goldschmidt
Gf. Institutsleiter des Internationalen Health Care Management Instituts der Uni Trier,
http://www.ihci.de
e-mail: goldschmidt@uni-trier.de

Dr. med. Christoph F-J Goetz
Kassenärztliche Vereinigung Bayerns,
Leiter Telemedizin,
e-mail: Christoph.Goetz@kvb.de

Durch die verbindliche Einführung einer elektronischen Patientenkarte, »eGK« – (voraussichtlich) mit Smart Card-Technologie – wird die bisherige Krankenversichertenkarte (mit einfachem Speicherchip) ersetzt. Dieses Vorhaben stellt global betrachtet eines der umfangreichsten IT-Vorhaben dar und wurde in der vergangenen Ausgabe von »mdi« vorgestellt [1]. Im vorliegenden 2. Teil sollen einige rechtliche, technische und (aus Sicht der stationären Versorgung) ökonomische Aspekte genauer betrachtet werden.

Das Regelungssystem des GKV-Modernisierungsgesetzes (GMG) zur elektronischen Gesundheitskarte

Das GMG sieht in § 291a SGB V die Einführung einer elektronischen Gesundheitskarte für die Mitglieder der gesetzlichen Krankenversicherung bis spätestens zum 1.1.2006 vor. Inhalt und Funktionsweise der Karte gliedern sich in einen verpflichtenden und einen freiwilligen Bereich, für die jeweils unterschiedliche Regeln für die Zulässigkeit und Zugriffsbefugnisse gelten (s. bereits [2]). Weitere Bestimmungen widmen sich der Verhinderung des Missbrauchs der auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten und dem Aufbau der erforderlichen technischen und organisatorischen Infrastruktur.

Aufteilung in verpflichtende und freiwillige Teile

Die drei verpflichtenden Teile der elektronischen Gesundheitskarte (§ 291a Abs. 2 SGB V, Abb. 1) 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 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. Der europäische Berechtigungsnachweis muss demgegenüber nach dem Gesetz nicht elektronisch gespeichert werden, sodass im ersten Schritt ein Aufdruck der Daten auf der Kartenrückseite und die Verwendung als Sichtausweis möglich sind.

§ 291a Abs. 3 SGB V enthält sechs Anwendungen, die die elektronische Gesundheitskarte unterstützen muss, die jedoch nicht verpflichtet ausgestaltet sind (Abb. 2). Dies sind die Ablage medizinischer Notfalldaten, der elektronische Arztbrief, die elektronische Patientenakte, die Arzneimitteldokumentation, vom Patienten selbst zur Verfügung gestellte Informationen und Daten über in Anspruch genommene Leistungen. Diese Anwendungen sind nur zulässig, wenn der Versicherte einwilligt. Die Einwilligung ist zu dokumentieren. Ihr hat eine ausführliche Information über die Funktionsweise vorauszugehen, sie ist auf einzelne Anwendungen beschränkbar und kann jederzeit widerrufen werden (§ 291a Abs. 3 Sätze 2-4 SGB V). Nach § 291a Abs. 6 Satz 1 SGB V kann der Versicherte jederzeit die Löschung der Daten verlangen; das gilt auch für die Daten des elektronischen Rezepts.

Das GMG enthält mit Ausnahme der Stammdaten keine Regelung darüber, wo die Daten, die den jeweiligen Anwendungen zugeordnet sind, zu speichern sind. Es ist insoweit offen für eine Speicherung auf der elektronischen Gesundheitskarte, auf einem zentralen Server und in einem dezentral-verteilten System. Aus allgemeinen Datenschutz- und Datensicherheitserwägungen ergibt sich jedoch, dass auf eine zentrale Speicherung zu verzichten ist, weil diese die Attraktivität von Angriffen erhöht und Zweckentfremdungen erleichtert [3], [4].

Zugriffsberechtigungen

§ 291a Abs. 4 und Abs. 5 SGB V enthalten ein ausdifferenziertes System des Zugriffsschutzes, welches die Mitwirkung des Versicherten und die eines Angehörigen einer bestimmten medizinischen Berufsgruppe vorschreibt. § 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 (Abb. 3). Die freiwilligen Anwendungen (außer den Daten über in Anspruch genommene Leistungen) dürfen nur Ärzten, Zahnärzten und Apothekern, die Notfalldaten auch anderen Angehörigen eines Heilberufes zugänglich sein.

Um die Mitwirkung der genannten Berufsgruppen technisch sicherzustellen, ist sowohl für das elektronische Rezept als auch für die freiwilligen Anwendungen der Einsatz eines elektronischen Heilberufsausweises (im Fall des Rezepts auch eines anderen Berufsausweises) erforderlich der »über eine qualifizierte elektronische Signatur verfügen« muss (vgl. § 2 Nr. 3 SigG). Hilfspersonen ohne einen solchen Ausweis müssen gemäß § 291a Abs. 5 Satz 4 SGB V von einem Inhaber eines Heilberufsausweises autorisiert werden.

Gerrit Hornung, LL.M. Mitglied der Projektgruppe verfassungsverträgliche Technikgestaltung, Uni Kassel, e-mail: gerrit.hornung@uni-kassel.de

Der Zugriff auf das elektronische Rezept kann schließlich vom Versicherten auch selbst freigeschaltet werden (§ 291a Abs. 5 Satz 4 SGB V). Damit soll es ihm ermöglicht werden, das Rezept im europäischen und außereuropäischen Ausland auch dann einzulösen, wenn es dort kein System elektronischer Heilberufsausweise gibt oder diese mit der elektronischen Gesundheitskarte nicht interoperabel sind.

§ 291a Abs. 5 Satz 1 SGB V bindet jedes Erheben, Verarbeiten und Nutzen von Daten der freiwilligen Funktionen mittels der elektronischen Gesundheitskarte an das Einverständnis des Versicherten (Abb. 4). Hierzu ist (mit Ausnahme der Notfalldaten, bei denen das im Einzelfall unmöglich sein kann) eine technische Autorisierung durch den Versicherten erforderlich. Bei den verpflichtenden Funktionen besteht dagegen der Schutz nur im Besitz der elektronischen Gesundheitskarte durch den Versicherten. Hierdurch kann er beispielsweise darüber entscheiden, wer die Daten des elektronischen Rezepts ausliest. Soweit eine technische Autorisierung erforderlich ist, kann dies z. B. mittels PIN oder biometrischem Merkmal erfolgen. Beide Verfahren werden nicht im Gesetz, wohl aber in der Begründung angesprochen [5]. Aufgrund des engen Zeitplans der Einführung der elektronischen Gesundheitskarte zum 1.1.2006 dürfte jedoch eine Verwendung biometrischer Verfahren in Anbetracht der – trotz erheblicher Fortschritte – immer noch bestehenden Unsicherheiten über ihre Leistungsfähigkeit (vgl. [6]) zumindest für die erste Kartengeneration unrealistisch sein.

Problematisch ist, dass die gesetzliche Regelung keine Möglichkeit für den Versicherten vorsieht, bestimmte Gesundheitsinformationen im Einzelfall zurückzuhalten. Aufgrund seiner Verfügungsbefugnis über die Daten steht es ihm jedoch zu, auch gegenüber einem Leistungserbringer Informationen nicht zu offenbaren, wenn er dies möchte. Demzufolge ist auf der Ebene der technischen Umsetzung ein Mechanismus abstufbarer Zugriffsrechte zu ermöglichen.

Ein Sonderfall der freiwilligen Anwendungen der elektronischen Gesundheitskarte sind die selbst zur Verfügung gestellten Daten. Hier ist es dem Versicherten möglich, beliebige Informationen zu speichern und nach einer eigenen technischen Autorisierung abzurufen oder Leistungserbringern zur Verfügung zu stellen. Beispiele sind Blutdruck- und Blutzuckerwerte, aber auch Patientenverfügungen und Organspendeausweis. Das Erfordernis der technischen Autorisierung im Einzelfall garantiert, dass ohne den Willen des Karteninhabers kein Zugriff möglich ist. Es wird jedoch dann zum Problem, wenn Daten gerade für den Fall zur Verfügung gestellt werden, in dem eine bewusste Autorisierung nicht mehr möglich ist, beispielsweise bei einer Bewusstlosigkeit. Diese Situation wurde vom Gesetzgeber offensichtlich übersehen, weil nach der aktuellen Rechtslage der – im Regelfall hirntote – Inhaber der elektronischen Gesundheitskarte den Zugriff auf seinen Organspendeausweis freischalten müsste. De lege ferenda wäre eine Teilung des Datenfachs denkbar, sodass bestimmte Informationen ohne PIN-Schutz genau für den Fall zur Verfügung gestellt werden, in dem eine gewillkürte Handlung nicht mehr möglich ist.

Die Versicherten haben nach § 291a Abs. 4 Satz 2 SGB V das Recht, auf alle Daten mit Ausnahme der Stammdaten und des Auslandskrankenscheins »zuzugreifen«. Diese missverständliche Formulierung deutet zunächst auf ein allgemeines technisches Zugriffsrecht, beispielsweise am heimischen PC, hin. Der systematische Zusammenhang mit der Bindung des Zugriffs an einen elektronischen Heilberufsausweis in § 291a Abs. 5 Satz 3 SGB V ergibt jedoch, dass dies vom Gesetz nicht gewollt ist; gemeint ist vielmehr ein besonderes Auskunftsrecht hinsichtlich der Daten. Allerdings kann der Versicherte auf die Daten des elektronischen Rezepts schon deshalb zugreifen, weil er diese auch ohne Mitwirkung eines Heilberufsausweisinhabers selbst freigeben kann.

Ein eigener technischer Lesezugriff des Karteninhabers ist nach dem Gesetz im Übrigen nur für die selbst zur Verfügung gestellten Daten vorgesehen (Abb. 5). Hierzu ist nach § 291a Abs. 5 Satz 3, 2. Halbsatz SGB V eine eigene Signaturkarte des Versicherten erforderlich, die über die Möglichkeit zur Erstellung qualifizierter elektronischer Signaturen verfügen muss. Mit dieser Regelung wird eine separate Signaturkarte des Versicherten vorausgesetzt. Denkbar wäre zwar auch, auf der Gesundheitskarte ein qualifiziertes Signaturverfahren einzurichten und so ein Zugriffsmanagement zu ermöglichen. Der Gesetzeswortlaut spricht jedoch von einer »eigenen« Signaturkarte des Versicherten, die Gesetzesbegründung von Versicherten, die »selbst« über eine solche verfügen [5]. Auch wenn die elektronische Gesundheitskarte (was vom Gesetz nicht gefordert, aber auch nicht ausgeschlossen wird) qualifizierte Signaturen erstellen kann, ist de lege lata also eine weitere Karte zur Verwaltung der selbst zur Verfügung gestellten Daten erforderlich. Sollte es technisch vorzugswürdig sein, auf der Gesundheitskarte selbst ein qualifiziertes Signaturverfahren einzurichten (als »virtuelle« eigene Signaturkarte), so müsste eine Gesetzesänderung erfolgen.

Um eine effektive Datenschutzkontrolle zu ermöglichen, sind schließlich mindestens die letzten 50 Zugriffe auf die elektronische Gesundheitskarte nach § 291a Abs. 6 SGB V zu diesem Zweck zu protokollieren. Eine Verwendung zu anderen Zwecken ist verboten. Die Protokolldaten sind überdies durch geeignete Vorkehrungen gegen zweckfremde Verwendung und sonstigen Missbrauch zu schützen.

Regelungen zur Verhinderung von Missbrauch

Das Zugriffssystem des GMG erfordert in einer Vielzahl von Situationen die Mitwirkung des Versicherten: sei es durch die Übergabe der elektronischen Gesundheitskarte, sei es durch eine darüber hinaus erforderliche technische Autorisierung des Zugriffs im Einzelfall. Diese Mitwirkungserfordernisse sind geeignet, die Rolle des Patienten im Rahmen der medizinischen Datenverarbeitung zu stärken; gleichzeitig bergen sie jedoch die Gefahr in sich, dass die Entscheidung über den Zugriff in das Spannungsfeld der allgemeinen sozialen Abhängigkeitsverhältnisse des Karteninhabers gerät. Es muss jedoch verhindert werden, dass das System der elektronischen Gesundheitskarte, zur Verbesserung der Qualität und Effizienz der Gesundheitsversorgung gedacht, von Dritten (beispielsweise potentiellen Arbeitgebern oder Versicherungen) missbraucht wird.

Um diesem Problem der Ausübung sozialen Drucks vorzubeugen, enthält das GMG weitere Schutzvorschriften für die im Zusammenhang mit der elektronischen Gesundheitskarte verwendeten Daten (Abb. 6). § 291a Abs. 8 SGB V verbietet es, 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- 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 50.000 € geahndet.

Wenn der Täter es nicht bei einer Einflussnahme auf den Inhaber der elektronischen Gesundheitskarte belässt, sondern sich selbst Zugriff auf die Daten verschafft, so liegt hierin eine deutliche höhere kriminelle Energie. Der Gesetzgeber ist dieser Wertung gefolgt und hat in § 307a Abs. 1 SGB V eine neue Strafbestimmung eingeführt. Danach wird der Zugriff auf die auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten, der entgegen den Zugriffsbefugnissen des § 291a Abs. 4 Satz 1 SGB V erfolgt, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen Dritten zu schädigen, so kann nach § 307a Abs. 2 SGB V eine Freiheitsstrafe von bis zu drei Jahren verhängt werden.

Das GMG hat schließlich auch das Beschlagnahmeverbot in § 97 StPO ausgeweitet. Dieses dient (bezogen auf das Gesundheitswesen) dem Schutz des Vertrauensverhältnisses zwischen Leistungserbringer und Versichertem. Der Leistungserbringer kann sich im Prozess auf sein Zeugnisverweigerungsrecht berufen. Ließe man nun eine Beschlagnahme und nachfolgende strafrechtliche Verwertung der ärztlichen Dokumentation zu, so würde dieses

Abb. 1: Grundentscheidung und verpflichtende Anwendungen

Abb. 2: Freiwillige Anwendungen

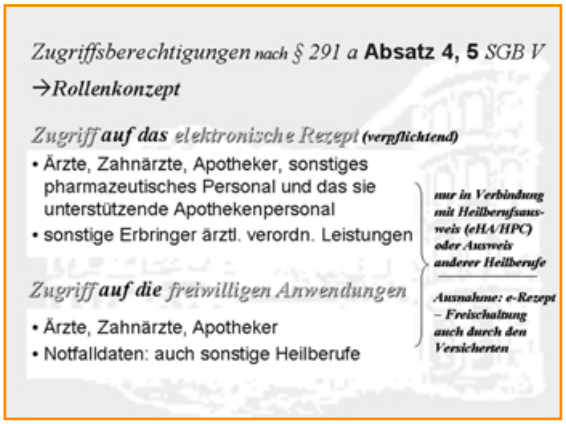

Abb. 3: Zugriffsberechtigungen nach Rollen

Abb. 4: Die Mitwirkung des Versicherten beim Zugriff

Recht ad absurdum geführt. Dies wird durch § 97 StPO verhindert, der jedoch bisher nur einschlägig war, wenn sich die Beweisobjekte im Gewahrsam des Leistungserbringers oder einer Krankenanstalt befanden. Der Einsatz der elektronischen Gesundheitskarte würde unter diesen Bedingungen dazu führen, dass eine Reihe von gespeicherten Daten nicht mehr von der Beschlagnahme ausgenommen wären, weil kein Gewahrsam des Leistungserbringers vorliegt. Das betrifft zum einen die auf der Karte selbst gespeicherten Informationen, weil sich die elektronische Gesundheitskarte im Gewahrsam des Versicherten befindet. Zum anderen werden in der Telematikstruktur externe Dienstleister die Speicherung oder Verarbeitung von Daten übernehmen. Sofern diese nicht selbst zeugnisverweigerungsberechtigt sind, hätte nach alter Rechtslage kein Beschlagnahmeschutz eingegriffen.

Der Gesetzgeber hat diese neuen Gefahren gesehen und den Beschlagnahmeschutz angepasst. Die elektronische Gesundheitskarte unterliegt nach dem neuen § 97 Abs. 2 Satz 1 StPO nie der Beschlagnahme, sofern die Voraussetzungen des Abs. 1 gegeben sind. Gleichzeitig wird der Gewahrsam eines Dienstleisters, der für Ärzte, Zahnärzte, Psychotherapeuten, Apotheker und Hebammen personenbezogene Daten erhebt, verarbeitet oder nutzt, genauso behandelt wie der einer Krankenanstalt.

Arbeitsgemeinschaft für Aufgaben der Datentransparenz

Eine völlig neue Regelung enthalten die §§ 303a bis 303f SGB V, mit denen eine »Arbeitsgemeinschaft für Aufgaben der Datentransparenz« eingerichtet wird. Sie wird nach § 303a Abs. 1 SGB V von den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildet und erhält einen Beirat (§ 303b SGB V), in dem Vertreter aller Beteiligten im Gesundheitswesen vertreten sein werden. Die Aufgaben der Arbeitsgemeinschaft sind die der Vertrauensstelle (§ 303c SGB V) und der Datenaufbereitungsstelle (§ 303d SGB V).

Die Datenflüsse sind folgendermaßen geregelt. Die Krankenkassen und die Mitglieder der Kassenärztlichen Bundesvereinigung sind nach § 303e Abs. 2 SGB V verpflichtet, Leistungs- und Abrechnungsdaten an die Vertrauensstelle zu übermitteln. Dies dient den Zwecken nach § 303f Abs. 2 Satz 2 SGB V, nämlich der Wahrnehmung von Steuerungsaufgaben durch die Kollektivvertragspartner, der Verbesserung der Qualität der Versorgung, der Planung von Leistungsressourcen, der Erstellung von Analysen zum Erkennen von Fehlentwicklungen und Ansatzpunkten für Reformen (Längsschnitte, Behandlungsabläufe, Versorgungsgeschehen), der Unterstützung politischer Entscheidungsprozesse zur Weiterentwicklung der gesetzlichen Krankenversicherung und der Analyse und Entwicklung von sektorenübergreifenden Versorgungsformen.

Die Vertrauensstelle pseudonymisiert die empfangenen Daten mittels eines Verfahrens, das im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik zu bestimmen ist. Nach der Pseudonymisierung werden die Daten an die Datenaufbereitungsstelle übermittelt und unmittelbar danach in der Vertrauensstelle gelöscht. Die Datenaufbereitungsstelle bereitet die Daten auf und stellt sie einer Gruppe von Nutzungsberechtigten zur Erfüllung der genannten Zwecke zur Verfügung.

Die Auswahl der Abrechnungs- und Leistungsdaten und die Struktur, die Prüfqualität und das Verfahren der Übermittlung an die Vertrauensstelle werden nach § 303e Abs. 1 SGB V von der Arbeitsgemeinschaft beschlossen. Zum Schutz der Daten sind sowohl die Vertrauens- wie die Datenaufbereitungsstelle von den Trägern der Arbeitsgemeinschaft und ihren Mitgliedern sowie von den nutzungsberechtigten Stellen nach § 303f Abs. 1 zu trennen.

Verpflichtung zum Aufbau von Infrastrukturen

Das GMG enthält einen Auftrag zur Entwicklung einer Informations-, Kommunikations- und Sicherheitsinfrastruktur für den Einsatz von Telematik im Gesundheitswesen (§ 291a Abs. 7 Satz 1 SGB V nennt beispielhaft die elektronische Gesundheitskarte, das elektronische Rezept und die elektronische Patientenakte) und zur Bestimmung von Inhalt und Struktur der Daten der freiwilligen Applikationen der elektronischen Gesundheitskarte (§ 291a Abs. 3 Satz 6 bis 9 SGB V). Verpflichtet sind 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.

Die Vereinbarung bedarf der Genehmigung durch das Bundesministerium für Gesundheit und Soziale Sicherung. Zuvor ist dem Bundesdatenschutzbeauftragten Gelegenheit zur Stellungnahme zu geben. Kommt keine Vereinbarung zustande, wird das Ministerium dazu ermächtigt, nach Anhörung der Beteiligten den Inhalt der Infrastruktur durch eine Rechtsverordnung festzulegen, die der Zustimmung des Bundesrates bedarf. In dieser Regelung liegt – jedenfalls potentiell – eine weitreichende Befugnis zum Eingriff in die Selbstverwaltungsstrukturen des Gesundheitssystems insgesamt.

Funktionsskizze zu einer »Elektronischen Patientenakte« nach GMG

Das GKV-Modernisierungsgesetz (GMG) definiert in § 291a Abs. 3 SGB V eine Reihe von Anwendungen, die neben den obligaten, im Gesetz ausdrücklich genannten Inhalten (§ 291 Abs. 2 mit § 291a Abs. 2 SGB V) durch die

künftige elektronische Gesundheitskarte grundsätzlich unterstützt werden müssen, insbesondere: 1. medizinische Daten ..., 2. ... elektronischer Arztbrief, 3. ... Arzneimitteldokumentation, 4. Daten über Befunde ... für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten, 5. durch selbst ... zur Verfügung gestellte Daten, sowie 6. »Kostenquittungen«. Hier ist also ausdrücklich der Einstieg in eine »elektronische Patientenakte« vorgezeichnet. Diese »ePA« ist dabei für jeden Betroffenen ein Angebot, das dieser freiwillig wahrnehmen kann, während sie für alle Leistungserbringer eine obligate Leistung bedeutet, die diese grundsätzlich anbieten und erbringen müssen.

Integrationsaspekte (Heterogenität und Datensicherheit)

Für die technische Realisierung ergibt sich dabei eine schon bemerkenswerte Heterogenität von unterschiedlichen Ansätzen, in der jeder für sich den Anspruch erhebt, die Lösung der künftigen Gesundheitstelematik zu bieten. Gegenwärtig erarbeitet aus allen diesen bekannten Vorschlägen eine Arbeitsgruppe der in § 291a Abs. 7 SGB V genannten Einrichtungen der Selbstverwaltung ein einheitliches und funktionell konsolidiertes Konzept. Zwar ist noch keine abgerundete Detailstruktur beschlossen, aber wichtige Grundansätze der künftigen elektronischen Patientenakte sind inzwischen absehbar.

Das am weitesten fortgeschrittene Musterkonzept zur elektronischen Patientenakte geht gegenwärtig aus von lokalen Computersystemen der Versorger, elektronischen Gesundheitskarten (»eGKs«) der Betroffenen, Heilberufsausweisen (»HPCs«) der Leistungserbringer und einem heterogen organisierten, aber geschlossenen Netz für das Gesundheitswesen, zu dem nur Angehörige der Heilberufe, Kostenträger oder vergleichbare Stellen mittels ihrer jeweiligen HPCs Zugang erlangen (siehe Abb. 7).

Zunächst bleibt jede Einrichtung im Gesundheitswesen wie bisher verantwortlich für ihre eigene (lokale) Datenhaltung, die sie vollverantwortlich betreibt und gegen jeden fremden Zugriff wirksam schützen muss. Dies beinhaltet auch eine selbständige Nutzerverwaltung, Zugriffsschutz und Virenkontrolle in voller datenschutzrechtlicher Eigenverantwortung. Die hier verarbeiteten und gespeicherten Daten sind dabei »nur« lokal im Schutzbereich der jeweiligen Einrichtung verfügbar. Gleichzeitig ist auch davon auszugehen, dass Gesundheitsinformationen aus vielen solcher lokalen Rechnersysteme nach »Betriebsschluss« der betroffenen Einrichtung für andere/Dritte nicht weiter verfügbar sind. Hier kann also eine 24-Stunden-/365-Tage-Verfügbarkeit für andere/Dritte nicht angenommen werden.

Aufbau und Inhalt so gespeicherter Patientendaten müssen dabei auf absehbare Zeit »proprietär« bleiben dürfen, damit die vielfältigen Erheber und Nutzer gesundheitsrelevanter Daten mit ihren bewährten Endsystemen weiter arbeiten können. Es ist hingegen genauso absehbar, dass durch die Vernetzung von Funktion und Inhalt mit »externen« Stellen künftig ein erheblicher Druck zur Standardisierung und Vereinheitlichung entstehen wird. Im Rahmen dieser Entwicklung wird es voraussichtlich zu einer weiteren Konsolidierung der heute noch mehr als 180 Praxiscomputersysteme der ambulanten und mehr als 60 Klinik-Informationssysteme der stationären Versorgung und vergleichbarer Systeme kommen. Eine solche Marktbereinigung aber als Vorbedingung für eine Vernetzung anzunehmen, würde jeder Erfahrung bei der Einführung komplexer DV-Systeme widersprechen.

In Fortführung der bereits erkennbaren Entwicklung nutzen die vorgenannten, lokalen Informationssysteme der Einrichtungen im Gesundheitswesen heute schon zunehmend Methoden zum datentechnischen Informationstransfer untereinander. In diesem Kontext ist also absehbar, dass jede Einrichtung neben eigenen Strukturen dann über eine eigene Anbindung an eine telematische Vernetzung der Akteure im Gesundheitswesen verfügen wird. Diese Tendenz birgt die Keimzelle eines künftigen, einheitlichen so genannten »Gesundheitsnetzes«. Das GMG schreibt mit § 291a Abs. 7 SGB V die Schaffung der »erforderlichen Informations-, Kommunikations- und Sicherheitsinfrastruktur« sogar ausdrücklich vor.

Zugriffsberechtigungen nach § 291a **Absatz 4, 5** *SGB V:*
→„Eigener Zugriff" des Versicherten

Verpflichtende Funktionen

- kein Zugriffsrecht durch den Versicherten auf Stammdaten und EU-Berechtigungsnachweis
- e-Rezept: Zugriffsmöglichkeit aufgrund der technischen Möglichkeit der Freigabe ohne Mitwirkung eines Leistungserbringers

Freiwillige Funktionen

- Leserecht, aber Koppelung an Berufsausweis
- Ausnahme: Technischer Lesezugriff auf selbst zur Verfügung gestellte Daten – **separate** Signaturkarte erforderlich

Regelungen zur ***Verhinderung von Missbrauch***

§ 291a Abs. 8 SGB V

- *Ausübung von Druck auf den Versicherten zur Offenbarung an Unberechtigte oder zu anderen Zwecken als denen der Versorgung und Abrechnung* → Ordnungswidrigkeit
- *Zugriff auf die Daten durch Unbefugte* → Straftat

§ 97 Abs. 2 StPO

- *Galt bislang für Gegenstände im Gewahrsam von Ärzten und Krankenhäusern*
- *Ausweitung auf die Gesundheitskarte*
- *Ausweitung auf Dienstleister, die für Ärzte, Zahnärzte, Psychotherapeuten, Apotheker und Hebammen Daten erheben, verarbeiten oder nutzen*

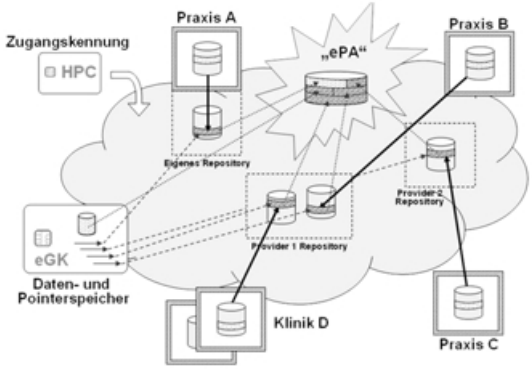

Abb. 5 oben:
Zugriffsmöglichkeiten des Versicherten

Abb. 6 mitte:
Schutz des Versicherten durch Straf- und Ordnungswidrigkeitsbestimmungen

Abb. 7 unten:
Die elektronische Patientenakte (ePA) als Summe eingestellter Informationskopien

Tabelle 1:
Unmittelbarer Nutzen der eGK für die Krankenhäuser

Einheitliche Schnittstellen und Datenformate
(a) machen eine Kommunikation zwischen Krankenhäusern mit unterschiedlicher EDV sowie mit den Praxis-Informationssystemen der Niedergelassenen und anderen Leistungsanbietern überhaupt erst möglich
(b) erleichtern damit die Zusammenarbeit von Krankenhäusern
(c) bewirken eine größere Investitionssicherheit bei der eigenen Informationstechnologie
Standardisierte administrative Versicherteninformationen auf der eGK
(a) werden für alle Krankenkassen und Krankenkassenarten einheitlich sein
(b) sollten fehlerfrei und lückenlos in ein Krankenhausinformationssystem und alle Abteilungssysteme übernommen werden
(c) sorgen damit für »eine« eindeutige Patienten-ID bei allen behandelnden Institutionen
(d) ermöglichen ein besseres Sortieren und Auffinden im Krankenblattarchiv
(e) erleichtern damit die fallbezogene Arbeit für das Medizin-Controlling
(f) helfen fehlerhafte und bruchstückhafte Abrechnungen zu vermeiden
(g) erlauben ein verlässliches Navigieren in Abrechnungsdaten der integrierten Versorgung
(h) erleichtern das hausinterne und -externe Benchmarking
(i) unterstützen die direkte Abrechnung mit den Patienten (GKV-Eigenanteile, Patientenquittung, PKV / Selbstzahler)
Informationen zu Notfalldaten und Verweise (Pointer) zu Behandlungsinformationen
(a) warnen vor Allergien und vermeiden diesbezügliche Arzneimittelkomplikationen
(b) können vor miteinander unverträglichen Arzneimitteln schützen (Interaktionen)
(c) unterstützen die schnelle und verlässliche Auswahl von Blut und Blutersatzstoffen
(d) helfen bei der medizinisch-pflegerischen Dokumentation
(e) erleichtern den elektronischen Kurz-Entlassungsbrief bis hin zum ausführlichen Arztbrief
(f) tragen zu Transparenz und Information der Behandlung für den Patienten bei
(g) sind die Basis für eine verteilte elektronische Patientenakte der Zukunft
Resultierende Vorteile im Allgemeinen (BMGS)
(a) Verbesserung der Qualität der medizinischen Versorgung, u. a. der Arzneimittelsicherheit
(b) Verbesserung patientenorientierter Dienstleistungen
(c) Stärkung der Eigenverantwortung
(d) Mitwirkungsbereitschaft und -initiative der Patienten
(e) Steigerung der Wirtschaftlichkeit und Leistungstransparenz im Gesundheitswesen
(f) Optimierung von Arbeitsprozessen
(g) Bereitstellung von aktuellen Steuerungsinformationen.

Doch auch hier ist auf absehbare Zeit von einer dezentralen, heterogen aufgebauten, finanzierten und organisierten Struktur auszugehen.

Schutzmaßnahmen (»first and second line of defense«)

Während das geplante Gesundheitsnetz funktionell auf die bewährte Technologie des Internets in neuester Ausprägung (IP v6) aufbauen soll, ist bei dem gegenwärtigen Ansatz wesentlich, dass es als eigenständiges, geschlossenes Netz konzipiert und betrieben werden soll. Dies dient als erste Schutzmaßnahme (»first line of defense«) für alle angeschlossenen Nutzer und transportierten Daten. Dabei ist natürlich nicht ausgeschlossen, sondern eher absehbar, dass dieses funktionell einheitliche Gesundheitsnetz verschiedene Dienstleister mit unterschiedlichen Server-Strukturen nach einer zentral administrierten Policy umfassen wird. Es scheint dabei auch Konsens zu geben über die Notwendigkeit eines sehr sicherheitsbewussten bzw. »konservativen« Vorgehens unter Ausschluss aller »Experimentierwiesen«. Nicht ausgeschlossen sind dabei aber Möglichkeiten für entsprechend abgesicherte Gateways zu »externen« Informationsinhalten oder Kommunikationsstrukturen außerhalb des Gesundheitswesens. Ebenfalls absehbar ist, dass Migrationskonzepte laufend eine Integration neuer Anforderungen, Konzepte und Funktionen ermöglichen müssen.

Es wird geplant, dass in diesem Gesundheitsnetz neben der reinen Transportfunktion auch professionell betriebene Speicherstellen im Sinne von »data repositories« angeboten werden können. Jede Einrichtung des Gesundheitswesens kann also über die eigene Datenhaltung hinaus eine oder mehrere (ggf. kommerziell organisierte) »externe« Speicherstellen unterhalten oder mit der Bereithaltung personenbezogener Gesundheitsdaten beauftragen. Diese heterogen organisierten, dezentralen Speicherstellen setzen die 24-Stunden-/365-Tage-Verfügbarkeit dort eingelagerter Datenbestände konkret um.

Diese Datenbestände in dezentralen Speicherstellen sind zwar nach der Reform des § 92 Abs. 2 Satz 2 StPO ebenfalls vom strafrechtlichen Beschlagnahmeschutz erfasst. Nichtsdestotrotz sind sie besonderen datenschutzrechtlichen Gefährdungen ausgesetzt. Deshalb muss jede Möglichkeit einer fremden Einsichtnahme oder Nutzung nachweisbar technisch ausgeschlossen werden.

Die Rolle der eGK hierbei

Hierfür bietet die Gesundheitskarte den entscheidenden Mechanismus. Werden in Absprache mit und auf Veranlassung der Betroffenen eigene Gesundheitsdaten im Gesundheitsnetz für andere Leistungserbringer selbst zur Verfügung gestellt, so geschieht dies immer mittels eines durch die eGK des Betroffenen verschlüsselten Extrakts und Kopie eigener Lokaldaten der jeweiligen Leistungserbringer. In vernetzten Speicherstellen hinterlegte Gesundheitsdaten sind somit immer moderiert (durch den Einsteller), strukturiert (nach Regeln des Gesundheitsnetzes) und redundant (mit den Ursprungsdaten).

In einem Gesundheitsnetz abgelegte Gesundheitsdaten sind mit einem Hybridverfahren verschlüsselt, unter Nutzung eines einmaligen, symmetrischen Session- oder Objektschlüssels zur Verschlüsselung der Nutzdaten. Dieser symmetrische Schüssel ist wiederum mit dem öffentlichen Schlüssel des Betroffenen verschlüsselt und den Nutzdaten beigefügt. So kann nur der Betroffene mit seinem privaten Schlüssel seiner Gesundheitskarte den symmetrischen Session- oder Objektschlüssel wieder herstellen und zur Nutzung anderer bereitstellen. Wie in der Praxis üblich, darf/kann der private, asymmetrische Schlüs-

sel die Gesundheitskarte nie verlassen. Die Karte wendet diesen Schlüssel lediglich auf übergebene Kryptogramme an und gibt das entschlüsselte Ergebnis zurück. Somit dient die Gesundheitskarte als wichtigste Schutzmaßname des Betroffenen (»second line of defense«) in dem hoch sensiblen Konstrukt der vernetzten Bereitstellung und Nutzung von Gesundheitsdaten.

Über diese Schlüsselfunktion hinaus soll die eGK natürlich auch Querverweise (Pointer) auf diese im Gesundheitsnetz hinterlegten, verschlüsselten Kopien vereinbarter und relevanter Gesundheitsdaten enthalten. Diese Pointer der Gesundheitskarte weisen dabei auf alle im Gesundheitsnetz hinterlegten Informationen, auch oder gerade wenn diese in Data Repositories unterschiedlicher Anbieter hinterlegt sind. Die eGK wird mit dieser Verzeichnisfunktion zusammen mit der Schlüsselfunktion zu einem entscheidenden Dreh- und Angelpunkt im Gesundheitssystem.

Das GMG wie auch funktionelle Überlegungen lassen auch die Speicherung originärer Nutzdaten auf der Gesundheitskarte als sinnvoll erscheinen, sofern sich diese in Datenvolumen und absehbarem Nutzen einer Offline-Nutzung erschließen (z. B. bei Notfalldaten oder der Arzneimitteldokumentation). Konkret sollte also die Gesundheitskarte auch originäre Gesundheitsdaten der Betroffenen enthalten können und nicht nur Querverweise auf »externe« Speicherstellen.

Szenarien (»Use-Cases«)

Ausgehend von diesen Überlegungen bezeichnet der Begriff »Elektronische Patientenakte« immer ein dynamisches Konstrukt aller direkt lokal (auf der Gesundheitskarte) und indirekt peripher (im Gesundheitsnetz) verfügbaren gesundheitsrelevanten Daten eines Betroffenen. Viele Nutzungsszenarien dieser neuen Technologie werden erst im Laufe der Zeit ihre Funktionalität beweisen oder Änderungsbedarf offenbaren können. Trotzdem können konkrete Use-Cases heute schon den Umgang mit dieser Infrastruktur zeigen, wie z. B.:

Der Betroffene kann, ggf. auch zeitversetzt, beliebigen Heilberufsangehörigen seines Vertrauens die Querverweise auf vernetzt verfügbare, dezentrale Speicherstellen (im Gesundheitsnetz) übermitteln, mittels derer diese unter Nutzung ihrer Heilberufausweise eine (noch verschlüsselte) Kopie der Nutzdaten einholen können. Nach Übergabe des asymmetrisch verschlüsselten Sitzungs- oder Objektschlüssels an die Gesundheitskarte des Betroffenen kann diese unter Nutzung des privaten Schlüssels des Betroffenen dann wieder den nutzbaren symmetrischen Schlüssel für das bezeichnete Objekt errechnen. Wenn dieser Schlüssel dann dem Leistungserbringer übergeben wird, so kann dieser die zuvor »abgeholten« Nutzdaten entschlüsseln und lokal nutzen. Der Besitz des (nun unverschlüsselten) Objektschlüssels durch den Leistungserbringer stellt somit keine eigenständige Bedrohung dar, sofern über entsprechende Policy-Vereinbarungen (oder noch zu definierende Rechtskonstrukte) die Preisgabe dieses Schlüssels den gleichen Regeln unterworfen wird wie die Weitergabe originärer Gesundheitsdaten.

Bei Verlust der Gesundheitskarte sind natürlich alle auf ihr gespeicherten Nutzdaten und alle durch sie bezeichneten Pointerdaten verloren, da sie (wegen Verlust des Querverweises und des privaten Schlüssel des Betroffenen) nicht mehr verfügbar/entschlüsselbar sind. Gegen einen solchen Verlust kann Vorsorge betrieben werden, indem die Pointerobjekte einer Gesundheitskarte einer Treuhänderstelle übergeben werden. Für die Sicherung originärer Nutzdaten oder auch der Pointerdaten kann ein (ärztlicher oder sonst vom Beschlagnahmeverbot geschützter) Leistungserbringer des Vertrauens beauftragt werden. Mittels gesicherter Pointerinformation können nach Verlust der Gesundheitskarte unter Nutzung einer neuen Gesundheitskarte entsprechend neu verschlüsselte Kopien angefordert und die Löschung obsoleter Datenbestände veranlasst werden. Dies sichert die Wiederherstellung nutzbarer und verfügbarer Gesundheitsdaten auf Basis einer neu ausgestellten Gesundheitskarte.

Tabelle 2:
Geschätzte Kosten der eGK in einem Beispiel-Krankenhaus mit 500 Betten und ca. 1.200 Voll- und Teilzeitbeschäftigten

300 bis max. 1.200 Health Professional- und Mitarbeiterkarten. Massenproduktion zw. 10 und 20 € pro Stück (Doppelkarte, größter Chip).
Sicherstellung des sog. »life-cycle-Managements«. Inhalte und Berechtigungen ständig überprüfen und auf dem Laufenden halten.
Lesegeräte (Dual-Slot) – siehe aber »alternatives« Mono-Slot-Verfahren in Österreich – für administrative und medizin.-pflegerische EDV-Arbeitsplätze, ca. 200 €.
Schnittstellenmanagement, Trustcenter-/PKI-Management
in einigen Fällen ein zugehöriger stationärer Drucker
Summe/Platz investiv je nach Ausstattung und Stückzahl zw. 300 und 500 €.
Plus laufende Kosten (neue Karten produzieren lassen, alte Karten entsorgen, kontinuierliche Kartenverwaltung, PKI-Dienste, Schnittstellenpflege etc.).

Kosten-Nutzen-Gesichtspunkte

Unmittelbarer Nutzen der eGK für Krankenhäuser

Die eGK bietet enorme Vorteile für die Administration und Behandlung, vor allem auf Grund (a) der Notwendigkeit einheitlicher Schnittstellen und Datenformate für Krankenhausinformationssysteme (KIS), (b) standardisier-

ter administrativer Versicherteninformationen und (c) der Informationen zu Notfall- sowie der Verweise (Pointer) zu Behandlungsinformationen auf dem integrierten Chip (siehe Tabelle 1).

Was bedeutet die Einführung der eGK finanziell für Krankenhäuser und IT?

Einheitliche Schnittstellen und entsprechende Modularität der Krankenhausinformations- und Abteilungssysteme sind seitens der Hersteller zunächst zu entwickeln und zu implementieren. Die Kosten dafür dürften letztendlich von den Krankenhäusern getragen werden müssen. Daher stellt sich für diese die Frage der Refinanzierung und des break even.

Der Aufwand dafür könnte etwa mit den Umstellungskosten zur Jahrtausendwende vergleichbar sein (Y2K-Problem), was im Durchschnitt etwa 0,5–1,5% eines Krankenhaus-Jahresbudgets bezogen auf 3 Jahre entspräche. Dies hieße summarisch in Deutschland im Mittel etwa 500 Mio. Euro (ggf. bis schätzungsweise 1 Mrd. Euro) für den stationären Bereich bzw. etwa die Hälfte der insgesamt erwarteten Gesamtkosten von mind. 1 Mrd. Euro (ggf. bis schätzungsweise 2 Mrd. Euro) [7]. Die Kostenseite beinhaltet neben den Software-Updates und -Upgrades für die jeweiligen Anwendungssysteme die Anschaffung von neuer Hardware. Hinzu kommen die Inanspruchnahme von Trustcenter-Dienstleistungen für die Verschlüsselung (public keys) sowie alle anderen laufenden Kosten nach der Primärinvestition. Bei einem 500-Betten-Haus und etwa 1.200 Voll- und Teilzeitbeschäftigen sind je nach Gestaltung des Geschäftsprozesses schätzungsweise zwischen 300 und maximal 1.000 Health Professional- und Mitarbeiter-Karten erforderlich, die in der künftigen Massenproduktion zwischen 10 und 20 Euro pro Stück kosten dürften. Hinzu kommt die Sicherstellung des sog. »life-cycle-Managements« der Karten, deren Inhalte und Berechtigungen ständig überprüft und auf dem Laufenden gehalten werden müssen. Für einen Großteil der administrativen und medizinisch-pflegerischen EDV-Arbeitsplätze ist voraussichtlich ein Dual-Slot-Lesegerät erforderlich sowie in einigen Fällen ein zugehöriger stationärer Drucker, was je nach Ausstattung und Stückzahl zwischen 300 und 500 Euro kosten dürfte (Tabelle 2). Viele Krankenhäuser, die bislang noch auf eine weitergehende Unterstützung der medizinischen Dokumentation verzichtet haben, werden dies nachholen müssen.

Weiterführende regelmäßige Informationen finden sich auf den Webseiten http://www.bIT4health.de und http://www.dimdi.de

Fazit

Mit dem GMG steht für die elektronische Gesundheitskarte ein normativer Rahmen fest, der, von Ausnahmen im Detail abgesehen (wie den vollständigen PIN-Schutz des Datenfachs für selbst zur Verfügung gestellte Daten), für den ersten Schritt der Entwicklung der technischen Infrastruktur hinreichend ist. Er bedarf jedoch der technischen Ausfüllung sowohl im Bereich der Zugriffsorganisation für die auf oder mit Hilfe der Gesundheitskarte gespeicherten Daten, als auch im Bereich der technischen Zusammenarbeit der Vielzahl von Beteiligten an der Telematik-Infrastruktur.

Wie bereits im ersten Teil [1] geschildert, stellt die sinnvolle informationstechnologische Vernetzung eine besondere Herausforderung für die integrierte Versorgung dar. Die integrierte Versorgung, unterstützt durch die elektronische Gesundheitskarte, sollte letztendlich zu den dringend notwendigen Einsparungen im Gesundheitswesen führen und die Qualität der medizinisch-pflegerischen Behandlung verbessern helfen.

Es ist absehbar, dass die vorgenannten Konzepte und Überlegungen an verschiedenen Stellen noch Unschärfen aufweisen und Unwägbarkeiten zu Problemen führen könnten. Trotzdem verbinden sich in der Beurteilung der für die künftige Entwicklung Zuständigen hier alle wesentlichen Überlegungen und Funktionen, damit das kommende Konstrukt der elektronischen Patientenakte mit bester Aussicht auf Erfolg und Akzeptanz durch Leistungserbringer, Gesetzgeber, Datenschutz und Betroffene ein funktionierendes Gesamtes werden kann, welches die nächste Dekade des deutschen Gesundheitswesens mit Modellcharakter für europäische Entwicklungen prägen wird.

Literatur

[1] Goldschmidt, A: Die Gesundheitskarte. bIT4health – bessere IT für bessere Gesundheit. Forum der Medizin_Dokumentation und Medizin_Informatik (mdi), Heft 1 (Jahrgang 6) März 2004 (ISSN 1438-0900): 22-26
[2] Hornung, G: Der zukünftige Einsatz von Chipkarten im deutschen Gesundheitswesen. In: Horster, P (Hrsg.), D-A-CH Security 2004, 226.
[3] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Entschließung der 62. Konferenz zu Datenschutzrechtlichen Anforderungen an den »Arzneimittelpass« (Medikamentenchipkarte), abrufbar unter http://www.datenschutz-berlin.de/doc/de/konf/65/top07.htm, 2001.
[4] Bultmann, M; Wellbrock, R; Biermann, H; Engels, J; Ernestus, W; Höhn, U; Wehrmann, R; Schurig, A: Datenschutz und Telemedizin. Anforderungen an Medizinnetze. Stand 10/02, abrufbar unter http://www.bfd.bund.de/technik/telemed.pdf.
[5] Gesetzesentwurf der Fraktionen SPD, CDU/CSU und BÜNDNIS 90/DIE GRÜNEN: Entwurf eines Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG), BT-Drs. 15/1525, 145, 2003.
[6] Büro für Technikfolgenabschätzung beim Deutschen Bundestag, Biometrische Identifikationssysteme – Sachstandsbericht, BT-Drs. 14/10005, 2002.
[7] Pfeiffer D.; Rebscher H.: Die Krankenkassen befürchten wegen der bevorstehenden Einführung der elektronischen Patientenkarte ein neues Chaos im Gesundheitswesen; sie erwarten Probleme durch den engen Zeitplan. Interview von Doris Pfeiffer (VdAK-Vorsitzende) mit der »Hannoverschen Allgemeinen Zeitung« und Aussage von Herbert Rebscher (DAK-Vorstand). In: Financial Times Deutschland (AP), 21.02.2004