Die künftige Telematik-Rahmenarchitektur im Gesundheitswesen

Recht, Technologie, Infrastruktur und Ökonomie

Die Autoren

Gerrit Hornung
Christoph F.-J. Goetz
Andreas J. W. Goldschmidt

Gerrit Hornung, LL.M.
Mitglied der Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Universität Kassel
Vereinsstr. 46
20357 Hamburg
gerrit.hornung@uni-kassel.de
http://www.uni-kassel.de/fb7/oeff_recht/personen/persGH.ghk

Dr. Christoph F.-J. Goetz
Leiter Telemedizin
Kassenärztliche Vereinigung Bayerns (KVB)
Elsenheimer Straße 39
80687 München
Christoph.Goetz@kvb.de
http://www.kvb.de

Univ.-Prof. Dr. Andreas J. W. Goldschmidt
Gf. Institutsleiter
IHCI / Fachbereich IV (Wi-So/WI)
Universität Trier
Wissenschaftspark 29
54296 Trier
goldschmidt@uni-trier.de
http://www.ihci.de

1 Einführung

Der Aufbau einer allgemeinen Telematik-Infrastruktur wird das sich in einem erheblichen Wandel befindliche deutsche Gesundheitswesen [Gold03] strukturell und qualitativ stark verändern und erhebliche volkswirtschaftliche Effekte in diesem sozio-ökonomisch problematischen „Megamarkt“ bewirken. Das Vorhaben ist eines der umfangreichsten IT-Projekte weltweit [Ward02]. Es geht um weit mehr als die technische Realisierung vernetzter Datenströme und die Garantie des Datenschutzes und der Privatsphäre [Goet01]. Zur Umsetzung sind die Entwicklung und Ausgabe elektronischer Gesundheitskarten (eGKs) für die Versicherten und Health Professional Cards (HPCs) für Ärzte, Apotheker und andere Leistungserbringer ebenso erforderlich wie die Bereitstellung entsprechender Lesegeräte. Diese Komponenten sind unter Einhaltung technischer Standards in eine umfassende Rahmenarchitektur einzubetten.

Die eGK soll Baustein eines umfassenden Managements der Patientenbehandlung sein. Gemeinsam mit der HPC und einer verteilten elektronischen Patientenakte könnte eine erhebliche Verbesserung der Patientenversorgung und eine Entlastung der öffentlichen Kassen erreicht werden. Nach § 291a SGB V hat die Einführung der eGK bis zum 2006-01-01 zu erfolgen.

Auch in der EU soll bis Anfang 2006 eine einheitliche Krankenversicherungskarte (reines Sichtdokument) für den administrativ möglichst unproblematischen Arztbesuch in allen Mitgliedstaaten eingeführt

Kernpunkte

Das Gesundheitswesen erlebt gegenwärtig lebhafte Diskussionen um die rechtliche und technische Ausgestaltung der künftigen integrierten Versorgungsstrukturen und deren wirtschaftliche Machbarkeit. Ein wesentlicher Baustein der Telematik-Infrastruktur wird die elektronische Gesundheitskarte (eGK) sein.

- Die rechtlichen Grundlagen der eGK (§ 291a SGB V) sind, von Problemen im Detail abgesehen, hinreichend.
- Der Aufbau einer elektronischen Patientenakte ist technisch machbar, erfordert jedoch die Integration einer Vielzahl heterogener Krankenhausinformations- und Praxissysteme. Zum Schutz der Daten können ein geschlossenes Netz als „first line of defense“, die eGK als „second line of defense“ eingesetzt werden.
- Die Einführung der eGK verspricht eine Verbesserung der medizinischen Versorgung und unmittelbaren wirtschaftlichen Nutzen für die Leistungserbringer. Die geschätzten Anlaufinvestitionen von ca. 1,8 Mrd. Euro dürften sich bereits nach zwei bis drei Jahren amortisieren.

Stichworte: Rahmenarchitektur, Gesundheitskarte, elektronische Patientenakte, Geschäftsprozesse, rechtliche Grundlagen, Datenschutz

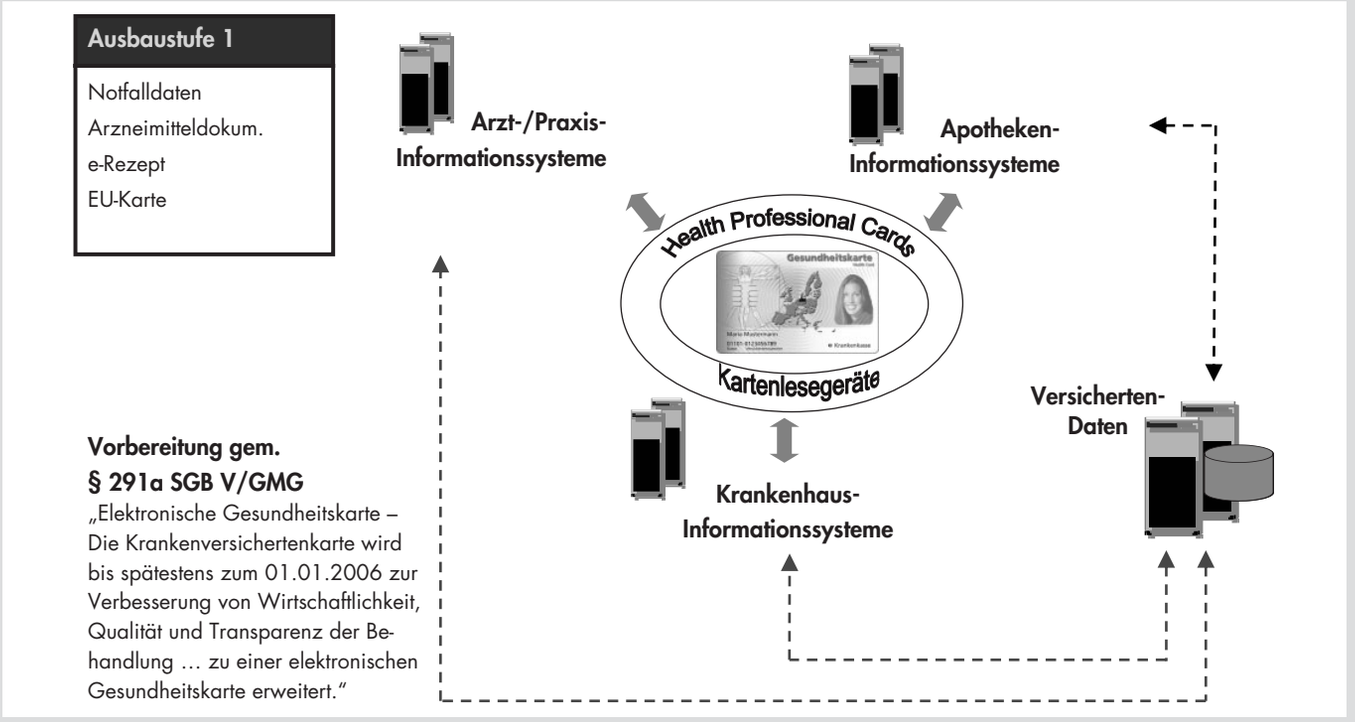

Bild 1 Elemente eines initialen Interaktionsszenarios der elektronischen Gesundheitskarte zum 2006-01-01 (Zeitplan fraglich)

werden. Die eGK in Deutschland soll diese EU-Karte auf der Rückseite enthalten [Mert04], gleichzeitig aber gegenüber der bisherigen Krankenversichertenkarte erweiterte Funktionen auf einem integrierten Chip bieten. Aus produktionstechnischen, ausschreibungsbedingten und anderen Gründen gehen Vertreter der gesetzlichen Krankenkassen und der Kassenärztlichen Vereinigungen davon aus, dass selbst bei einer schrittweisen Einführung, d. h. bei dem vorgesehenen Verzicht auf eine Maximallösung (Bild 1), das Jahr 2006 als Starttermin nicht eingehalten werden kann [PfRe04]. Erste Modellversuche mit der eGK sollen trotzdem laut Planungen des Bundesministeriums für Gesundheit und Soziale Sicherung, BMGS (Projektname „bIT4health", bessere IT für bessere Gesundheit) immer noch 2005 beginnen und bereits im gleichen Jahr abgeschlossen werden.

Die eGK ist für die 72 Mio. Versicherten der Gesetzlichen Krankenkassen vorgesehen. Insgesamt sieht das Projekt die Vernetzung von 80 Mio. Versicherten bei 300 Krankenkassen einschließlich der acht Mio. Privatversicherten mit 130.000 Arztpraxen, 2.200 Krankenhäusern, 20.000 Apotheken, 54.000 Zahnärzten und anderen Heilberufen vor, die pro Jahr 560 Mio. Zugänge von Patienten haben und 740 Mio. Verordnungen ausstellen [Mert04].

2 Das Regelungssystem des GKV-Modernisierungsgesetzes (GMG)

Das GMG enthält nur für einen Baustein der Telematik-Infrastruktur, die eGK, detaillierte Regelungen. § 291a SGB V sieht die Einführung der Karte für die Mitglieder der gesetzlichen Krankenversicherung bis spätestens zum 2006-01-01 vor.

2.1.1 Aufteilung der eGK in verpflichtende und freiwillige Teile

Inhalt und Funktionsweise der eGK gliedern sich in einen verpflichtenden und einen freiwilligen Bereich (Bild 2), für die jeweils unterschiedliche Regeln für Zulässigkeit und Zugriffsbefugnisse gelten [Horn04, 226ff.; Weic04, 391ff.]. Die drei verpflichtenden Teile (§ 291a Abs. 2 SGB V) sind die Speicherung der Versicherungsstammdaten, des Berechtigungsnachweises zur Inanspruchnahme von Leistungen in den EU-Staaten sowie der Daten zum Transport des elektronischen Rezepts. Letzteres soll eine medienbruchfreie Verarbeitung 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 sechs Anwendungen, die die eGK unterstützen muss, die jedoch für den Versicherten freiwillig sind: Ablage medizinischer Notfalldaten, elektronischer Arztbrief, elektronische Patientenakte, Daten zur Prüfung der Arzneimitteltherapiesicherheit, vom Patienten selbst zur Verfügung gestellte Informationen und Daten über in Anspruch genommene Leistungen („Patientenquittung"). Diese Anwendungen sind nur zulässig, wenn der Versicherte einwilligt [dazu Weic04, 398f.]. Die Einwilligung ist zu dokumentieren. Ihr hat eine ausführliche Information über die Funktionsweise vorauszugehen, sie ist auf einzelne Anwendungen beschränkbar und jederzeit widerruflich (§ 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 der jeweiligen Anwendungen zu speichern sind. Es ist insoweit offen für eine Speicherung auf der eGK, auf einem zentralen Server oder in einem dezentral verteilten System. Aus allgemeinen Datenschutz- und Datensicherheitserwägungen ist jedoch auf eine zentrale Speicherung zu verzichten, weil diese die Attraktivität von Angriffen erhöht und Zweckentfremdungen erleichtert [KDSB01; BWB+02].

Obligat	Fakultativ
▪ Versichertendaten ▪ E-Rezept ▪ EU-KV-Karte	▪ Arzneimitteldokumentation ▪ E-Arztbrief ▪ Kostenquittung ▪ Notfallinformationen ▪ E-Patientenakte ▪ allg. Patientendaten

Bild 2 Inhaltsfestlegung gemäß § 291a SGB V

2.1.2 Zugriffsberechtigungen

§ 291a Abs. 4 und 5 SGB V enthalten ein ausdifferenziertes System des Zugriffsschutzes, das die Mitwirkung des Versicherten und die eines Angehörigen einer bestimmten medizinischen Berufsgruppe vorschreibt [Horn04 227f.]. § 291a Abs. 4 Satz 1 SGB V beschränkt den Zugriff auf das elektronische Rezept auf Ärzte, Zahnärzte, Apotheker, Apothekerassistenten, Pharmazieingenieure und Apothekenassistenten und Personen, die bei den Genannten oder in einem Krankenhaus als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind. Auch sonstige Erbringer ärztlich verordneter Leistungen werden auf die Rezepte zugreifen können. Die Zugriffsberechtigung bei den freiwilligen Anwendungen war zunächst erheblich enger, wurde mittlerweile aber auf das genannte Apothekenpersonal und Psychotherapeuten ausgeweitet.

Um die Mitwirkung der Berufsgruppen technisch sicherzustellen, ist für das elektronische Rezept und die freiwilligen Anwendungen der Einsatz einer HPC erforderlich, die „über eine qualifizierte elektronische Signatur verfügen" muss. Das bezieht sich auf qualifizierte Signaturen nach § 2 Nr. 3 SigG [dazu Roßn04]. Im Fall des Rezepts genügt auch ein anderer Berufsausweis. Hilfspersonen ohne einen solchen Ausweis müssen gemäß § 291a Abs. 5 Satz 4 SGB V von einem Inhaber einer HPC autorisiert werden.

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, dieses im europäischen und außereuropäischen Ausland auch dann einzulösen, wenn es dort kein HPC-System gibt oder dieses mit der eGK nicht interoperabel ist.

§ 291a Abs. 5 Satz 1 SGB V bindet jedes Erheben, Verarbeiten und Nutzen von Daten der freiwilligen Funktionen an das Einverständnis des Versicherten. 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 eGK durch den Versicherten. 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 [SCB03, 145]. Aufgrund des engen Zeitplans der Einführung der eGK zum 2006-01-01 dürfte jedoch eine Verwendung biometrischer Verfahren in Anbetracht der – trotz erheblicher Fortschritte – immer noch bestehenden Unsicherheiten über ihre Leistungsfähigkeit [näher TAB02] zumindest für die erste Kartengeneration unrealistisch sein.

Problematisch ist, dass die gesetzliche Regelung keine ausdrückliche Vorgabe macht, wie der Versicherte bestimmte Gesundheitsinformationen im Einzelfall zurückhalten kann. Aufgrund seiner Verfügungsbefugnis über die Daten steht es ihm jedoch zu, auch gegenüber einem Leistungserbringer Informationen nicht zu offenbaren, wenn er dies möchte [Fues99, 173; DNG03, 240; Horn04, 232]. Demzufolge ist auf der Ebene der technischen Umsetzung ein Verfahren abstufbarer Zugriffsrechte zu ermöglichen.

Ein Sonderfall der freiwilligen Anwendungen der eGK sind die selbst zur Verfügung gestellten Daten. Hier kann der Versicherte beliebige Informationen (z. B. Blutdruck- und Blutzuckerwerte, Patientenverfügungen, Organspendeausweis) speichern und abrufen oder Leistungserbringern zur Verfügung zu stellen. Das Erfordernis der technischen Autorisierung im Einzelfall garantiert, dass ohne den Willen des Karteninhabers kein Zugriff möglich ist. Es wird jedoch zum Problem, wenn Daten gerade für den Fall zur Verfügung gestellt werden, in dem keine Autorisierung möglich ist, z. B. bei einer Bewusstlosigkeit. Dies wurde vom Gesetzgeber offensichtlich übersehen, weil nach der aktuellen Rechtslage der – im Regelfall hirntote – Inhaber der eGK den Zugriff auf den 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. Ein Schutz der Daten könnte dadurch eingerichtet werden, dass zum Zugriff eine HPC erforderlich wäre.

Die Versicherten haben nach § 291a Abs. 4 Satz 2 SGB V das Recht, auf alle Daten mit Ausnahme der Stammdaten und des Auslandskrankenscheins „zuzugreifen". Trotz dieser missverständlichen Formulierung ergibt der systematische Zusammenhang mit der Bindung des Zugriffs an eine HPC in § 291a Abs. 5 Satz 3 SGB V, dass damit kein eigenes technisches Zugriffsrecht, sondern vielmehr ein besonderes Auskunftsrecht für die Daten gemeint ist. Allerdings kann der Versicherte auf das Rezept schon deshalb zugreifen, weil er dieses auch ohne Mitwirkung eines HPC-Inhabers selbst freigeben kann.

Ein eigener technischer Lesezugriff des Karteninhabers ist nach dem Gesetz nur für die selbst zur Verfügung gestellten Daten vorgesehen. Hierzu ist nach § 291a Abs. 5 Satz 3, 2. Halbsatz SGB V eine eigene separate qualifizierte Signaturkarte des Versicherten erforderlich. Denkbar wäre zwar auch, auf der eGK 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 [SCB03, 145]. Auch wenn die eGK (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 Daten erforderlich. Hintergrund dieser Regelung war die Absicht des Gesetzgebers, dem Karteninhaber auch mit anderen, eigenen Signaturkarten den Zugriff zu ermöglichen. Schon technisch stehen hier gravierende Fragen der Interoperabilität heutiger Karten einer schnellen Lösung entgegen, sodass davon auszugehen ist, dass eine solche technische Lösung auf sich warten lassen wird.

Um eine effektive Datenschutzkontrolle zu ermöglichen, sind schließlich mindestens die letzten 50 Zugriffe auf die eGK nach § 291a Abs. 6 SGB V zu protokollieren. Eine Verwendung zu anderen Zwecken ist verboten, und die Daten sind technisch gegen Missbrauch zu schützen.

2.1.3 Regelungen zur Verhinderung von Missbrauch

Das GMG normiert in einer Vielzahl von Situationen (Übergabe der eGK, technische Autorisierung des Zugriffs) Mitwirkungserfordernisse des Versicherten. Diese sind geeignet, die Rolle des Patienten im Rahmen der medizinischen Datenverarbeitung zu stärken; gleichzeitig bergen sie jedoch die Gefahr, dass die Entscheidung über den Zugriff in das Spannungsfeld der allgemeinen sozialen Abhängigkeitsverhältnisse des Karteninhabers gerät. Es muss verhindert werden, dass das System der eGK, zur Verbesserung der Qualität und Effizienz der Gesundheitsversorgung gedacht, von Dritten (z. B. potenziellen Arbeitgebern oder Versicherungen) missbraucht wird.

Zur Vorzubeugung enthält das GMG Schutzvorschriften. § 291a Abs. 8 Satz 1 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 oder über eine solche Gestattung eine Vereinbarung zu treffen. Nach § 291a Abs. 8 Satz 2 SGB V dürfen aus der Bewirkung oder Verweigerung des Zugriffs weder Vor- noch Nachteile erwachsen. Verstöße gegen § 291a Abs. 8 Satz 1 (nicht jedoch Satz 2) SGB V werden nach § 307 Abs. 1 SGB V als Ordnungswidrigkeit mit einem Bußgeld von bis zu 50.000 € geahndet.

Wenn der Täter sich selbst entgegen den Befugnissen in § 291a Abs. 4 Satz 1 SGB V Zugriff verschafft, so handelt es sich gemäß § 307a SGB V um eine Straftat, die mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft wird. Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen Dritten zu schädigen, so kann Freiheitsstrafe bis zu drei Jahre verhängt werden.

Das GMG hat schließlich auch das Beschlagnahmeverbot in § 97 StPO ausgeweitet. Dieses dient dem Schutz des Vertrauensverhältnisses zwischen Leistungserbringer und Versicherten. Der Leistungserbringer kann sich im Prozess auf sein Zeugnisverweigerungsrecht berufen (§ 53 Abs. 1 Nr. 3 StPO). Ließe man nun eine Beschlagnahme der ärztlichen Dokumentation zu, so würde dieses Recht ad absurdum geführt [Beul02, Rn. 248; MeGo04, Rn. 1]. Dies wird durch § 97 StPO verhindert, der jedoch bisher nur einschlägig war, wenn sich die Beweisobjekte im Gewahrsam des Leistungserbringers oder einer Krankenanstalt befanden. Das trifft jedoch weder auf die eGK noch auf Daten zu, die in der künftigen Telematikstruktur durch externe Dienstleister gespeichert oder verarbeitet werden. Der Gesetzgeber hat deshalb den Beschlagnahmeschutz angepasst. Die eGK unterliegt nach dem neuen § 97 Abs. 2 Satz 1 StPO nie der Beschlagnahme. 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.

2.1.4 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 (Bild 3). Sie wird nach § 303a Abs. 1 SGB V von den Spitzenverbänden der Krankenkassen und der Kassenärztliche 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 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 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 Sektoren übergreifenden Versorgungsformen.

Die Vertrauensstelle pseudonymisiert die empfangenen Daten mittels eines Verfahrens, das im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu bestimmen ist. Danach werden die Daten an die Datenaufbereitungsstelle übermittelt, die sie aufbereitet und einer Gruppe von Nutzungsberechtigten zur Verfügung stellt.

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 SGB V zu trennen.

2.1.5 Aufbau von Infrastrukturen

Das GMG enthält Aufträge zur Entwicklung einer Informations-, Kommunikations- und Sicherheitsinfrastruktur für den Einsatz von Telematik im Gesundheitswesen (§ 291a Abs. 7 Satz 1 SGB V) und zur Bestimmung von Inhalt und Struktur der Daten der freiwilligen Applikationen der eGK (§ 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 BMGS. Zuvor ist dem Bundesdatenschutzbeauftragten Gelegenheit zur Stellungnahme zu gegeben. Kommt keine Vereinbarung zustande, wird das Ministerium dazu ermächtigt, nach Anhörung der Beteiligten den Inhalt der Infrastruktur

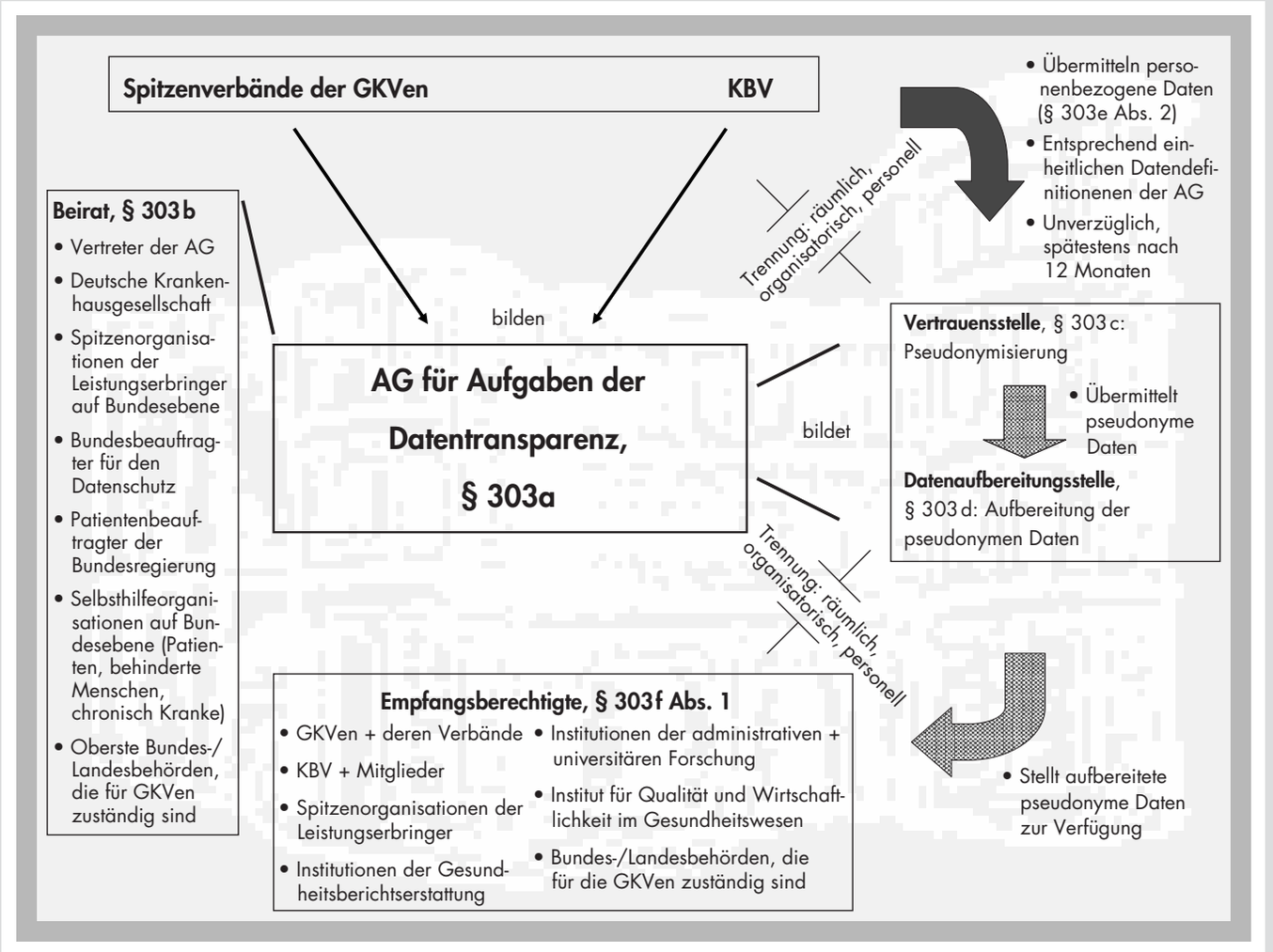

Bild 3 Arbeitsgemeinschaft für Aufgaben der Datentransparenz

durch eine Rechtsverordnung, die der Zustimmung des Bundesrates bedarf, festzulegen. In dieser Regelung liegt – jedenfalls potenziell – eine weit reichende Befugnis zum Eingriff in die Selbstverwaltungsstrukturen des Gesundheitssystems insgesamt.

Inzwischen hat sich das vom GMG vorgegebene Einstimmigkeitsprinzip für Entscheidungen der Leistungserbringer und Kostenträger als zu schwerfällig erweisen. Deshalb hat die Selbstverwaltung eine neue Einrichtung („gematik", Gesellschaft für Telematikanwendungen der Gesundheitskarte gGmbH) gegründet, in der Entscheidungen nach dem Mehrheitsprinzip getroffen werden können [Rabb05, 96]. Hierzu notwendige Änderungen des SGB V wie auch zusätzliche Vorgaben zu Struktur und Finanzierung unterlaufen gegenwärtig als § 291b SGB V den parlamentarischen Prozess.

3 Herausforderung für die Informationstechnologie

3.1 Kernproblem der bestehenden Krankenhausinformations- und Praxissysteme

Die heutigen Krankenhausinformationssysteme (KIS) und die Anwendungssysteme niedergelassener Ärzte erfüllen noch nicht die Kriterien für die Kommunikation in einer integrierten Versorgung. Erst recht sind sie gegenwärtig nicht dazu geeignet, die papiergestützte Krankengeschichte durch eine gemeinsame elektronische Patientenakte zu ersetzen. Die Anwendungssysteme benötigen zusätzliche, möglichst einheitliche Funktionen für eine Vielzahl von Daten aus nahezu allen DV-Systemen eines Krankenhauses und seiner künftigen Partner. Ein KIS muss beispielsweise weit mehr leisten als – wie heute häufig üblich – den betriebswirtschaftlichen Erfolg eines Krankenhauses plan- und steuerbar zu machen und maximal mit den Krankenkassen zu kommunizieren. Die sektorübergreifende Behandlung muss transparent aufbereitet und das zugehörige komplexere gemeinsame Qualitätsmanagement berücksichtigt werden. Dabei ist die logische Integration der eGK unter Einhaltung gemeinsamer Standards notwendig.

3.2 Die Rahmenarchitektur

Die Rahmenarchitektur sollte aus Anwendersicht idealisiert formuliert weitgehend generisch orientiert sein und als Metaarchi-

tektur auf den neuesten Entwicklungen und Paradigmen (Modell getriebene Architektur, Komponentenorientierung, wissensbasierte Interoperabilität) basieren [Blob03]. Das Ergebnis, nämlich wie generisch Anwendungssysteme einerseits sein müssen und andererseits maximal sein dürfen, um den notwendigen Wettbewerb um die besten Produkte und die Anreize für die Hard- und Softwareanbieter zu erhalten, wird baldmöglichst herbeizuführen sein, um den engen Zeitplan des GMG einhalten zu können. Insofern kommt den erwähnten Modellvorhaben eine außerordentliche Bedeutung zu.

3.3 Die Geschäftsprozessmodellierung

Die wichtigste initiale Aufgabe für die Beschreibung des „Geschäftsprozesses Patientenversorgung" besteht in der exakten Analyse der gegenwärtigen Bedingungen und Interaktionen im Gesundheits-„markt". Dabei stellt der Patient den wichtigsten Faktor dar. Jede Veränderung im Patientenkollektiv, z. B. durch epidemiologische, demografische, verhaltens- oder arbeitsbedingte Faktoren, ruft weit reichende ökonomische Effekte hervor. Die Geschäftsprozessmodellierung des Projekts bIT4Health beschreibt generisch die Prozesse des Gesundheitswesens, welche durch die Einführung der eGK betroffen sein werden, nämlich:

- Vertragsdatenmanagement,
- Verordnungsmanagement,
- Behandlungsmanagement,
- Kartenmanagement.

Dabei erfolgt die Modellierung so, dass die internen Prozesse der Leistungserbringer und Kostenträger möglichst wenig beeinflusst werden. Nicht unerwähnt darf bleiben, dass sich die Arbeit der Selbstverwaltung auf eine eigene „Lösungsarchitektur" konzentriert, die zwar manche der Vorarbeiten von bIT4Health aufgreift, als unabhängiges Arbeitsergebnis der gesetzlich Beauftragten aber insgesamt eigene Wege geht.

4 Funktionsskizze einer elektronischen Patientenakte

Nach § 291a Abs. 3 Nr. 3 SGB V muss die eGK das Erheben, Verarbeiten und Nutzen von Daten einer elektronischen Patientenakte unterstützen (siehe oben 2.1). Diese ist für die Karteninhaber freiwillig, während sie für alle Leistungserbringer eine obligate Leistung bedeutet, die diese anbieten und erbringen müssen.

4.1 Integrationsaspekte (Heterogenität und Datensicherheit)

Für die technische Realisierung gibt es eine Reihe unterschiedlicher Ansätze, aus denen gegenwärtig eine Arbeitsgruppe der in § 291a Abs. 7 SGB V genannten Einrichtungen der Selbstverwaltung ein einheitliches und funktionell konsolidiertes Konzept erarbeitet [ATG04]. Zwar ist noch keine abgerundete Detailstruktur beschlossen, wichtige Grundansätze sind aber bereits absehbar.

Das am weitesten fortgeschrittene Musterkonzept geht gegenwärtig von lokalen Computersystemen der Versorger, eGKs der Patienten, HPCs der Leistungserbringer und einem heterogen organisierten, aber geschlossenen Netz aus, zu dem nur Angehörige der Heilberufe, Kostenträger und vergleichbare Stellen mittels ihrer HPCs Zugang erhalten.

Jede Einrichtung im Gesundheitswesen betreibt wie bisher datenschutzrechtlich verantwortlich ihre eigene Datenhaltung und muss diese wirksam gegen fremden Zugriff schützen. Dies beinhaltet eine selbstständige Nutzerverwaltung, Zugriffsschutz und Virenkontrolle. Neben der lokalen Verfügbarkeit werden die Daten auch für Dritte bereitgestellt. Es ist jedoch davon auszugehen, dass Gesundheitsinformationen aus vielen solcher lokalen Einrichtungen nach deren Betriebsschluss für Dritte nicht abrufbar sind. Hier kann also keine 24 Stunden/365 Tage-Verfügbarkeit angenommen werden [Stat02].

Aufbau und Inhalt so gespeicherter Daten werden auf absehbare Zeit „proprietär" bleiben, da die Beteiligten ihre bewährten Endsysteme weiterverwenden müssen. Es ist zwar absehbar, dass durch die Vernetzung von Funktion und Inhalt mit externen Stellen ein erheblicher Druck zur Standardisierung entstehen wird, der eine weitere Konsolidierung der heute noch mehr als 180 Praxiscomputersysteme der ambulanten und mehr als 60 KIS der stationären Versorgung hervorrufen dürfte. 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 lokalen Informationssysteme im Gesundheitswesen heute schon zunehmend Methoden des Informationstransfers. Diese Tendenz birgt die Keimzelle eines künftigen, einheitlichen „Gesundheitsnetzes", dessen Einrichtung Teil der in § 291a Abs. 7 SGB V vorgeschriebenen Informations-, Kommunikations- und Sicherheitsinfrastruktur sein wird. Allerdings ist auf absehbare Zeit von einer dezentral und heterogen aufgebauten, finanzierten und organisierten Struktur auszugehen.

4.2 Einrichtung eines geschlossenen Netzes („first line of defense")

Das geplante Gesundheitsnetz wird zwar funktionell auf die bewährte Technologie des Internets in neuester Ausprägung (mit IPv6 und SSL) aufbauen, jedoch als eigenständiges, geschlossenes Netz konzipiert und betrieben werden. Dieses dient als erste Schutzmaßnahme *(„first line of defense")* für alle angeschlossenen Nutzer und transportierten Daten. Das schließt allerdings weder die Einbindung verschiedener Dienstleister mit unterschiedlichen Server-Strukturen nach einer zentral administrierten Policy noch abgesicherte Gateways zu Kommunikationsstrukturen außerhalb des Gesundheitswesens aus. Migrationskonzepte werden eine Integration neuer Anforderungen, Konzepte und Funktionen ermöglichen. Es zeichnet sich ein Konsens über die Notwendigkeit eines sehr sicherheitsbewussten Vorgehens unter Ausschluss aller „Experimentierwiesen" ab.

Geplant ist, dass in diesem Gesundheitsnetz professionell betriebene Speicherstellen i. S. v. „data repositories" durch Einrichtungen des Gesundheitswesens oder Dritte angeboten werden können. Diese heterogen organisierten, dezentralen Stellen setzen für die bei ihnen gelagerten Daten die 24 Stunden/365 Tage-Verfügbarkeit um. Ihre Datenbestände sind nach der Reform des § 97 Abs. 2 Satz 2 StPO vom strafrechtlichen Beschlagnahmeschutz erfasst. Nichtsdestotrotz sind sie besonderen datenschutzrechtlichen Gefährdungen ausgesetzt. Deshalb muss jede Möglichkeit einer fremden Einsichtnahme oder Nutzung nachweisbar technisch ausgeschlossen werden.

4.3 Die eGK als „second line of defense"

Hierfür bietet die eGK den entscheidenden Mechanismus. Werden unter Mitwirkung der Patienten Gesundheitsdaten für andere Leistungserbringer zur Verfügung gestellt, so geschieht dies immer mittels eines durch die eGK verschlüsselten Extrakts und Ko-

pie 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 Daten sind mit einem Hybridverfahren verschlüsselt. Die Nutzdaten werden mit einem einmaligen symmetrischen Session- oder Objektschlüssel verschlüsselt. Dieser ist wiederum mit dem öffentlichen, asymmetrischen Schlüssel des Patienten verschlüsselt und den Nutzdaten beigefügt. So kann nur der Patient mit seinem privaten Schlüssel, der seine eGK nie verlässt, den symmetrischen Objektschlüssel wieder herstellen und zur Nutzung bereitstellen. Die Verfügungsgewalt des Leistungserbringers über diesen Schlüssel stellt keine eigenständige Bedrohung dar, sofern seine Preisgabe über entsprechende Policy-Vereinbarungen (oder noch zu definierende Rechtskonstrukte) den gleichen Regeln unterworfen wird wie die Weitergabe der Gesundheitsdaten selbst. Die eGK dient so als wichtigste Schutzmaßnahme des Patienten („*second line of defense*“) in dem hoch sensiblen Konstrukt der vernetzten Bereitstellung und Nutzung von Gesundheitsdaten.

Neben dieser Schlüsselfunktion soll die eGK Verweise (Pointer) auf die im Netz hinterlegten, verschlüsselten Kopien der Daten enthalten. Diese Pointer weisen auf alle im Gesundheitsnetz – auch oder gerade in unterschiedlichen Data Repositories – hinterlegten Informationen. Daneben ist die Speicherung originärer Nutzdaten auf der eGK aus funktionellen Überlegungen sinnvoll, sofern sich diese in Datenvolumen und absehbarem Nutzen einer Offline-Nutzung erschließen (z. B. bei Notfalldaten oder den Daten zur Prüfung der Arzneimitteltherapiesicherheit). Durch diese Funktionen wird die eGK zu einem entscheidenden Dreh- und Angelpunkt im Gesundheitssystem. Sinnvoll erscheint, für den Fall ihres Verlusts Nutz- und Pointerdaten zusätzlich bei einer Treuhänderstelle zu speichern, z. B. bei einem Leistungserbringer des Vertrauens, bei dem die Daten einem Beschlagnahmeverbot unterliegen.

5 Kosten-Nutzen-Gesichtspunkte

Das letztliche Verhältnis von Kosten und Nutzen der Telematik-Infrastruktur kann derzeit nicht exakt bestimmt werden. Zur Evaluation werden wissenschaftliche Begleitstudien angestoßen, die jedoch noch keine Ergebnisse geliefert haben.

Die eGK bietet durch die künftig einheitlichen Schnittstellen und Datenformate, die Verfügbarkeit administrativer Versicherteninformationen und die Bereitstellung von Notfall- und Pointerdaten enorme Vorteile für die Administration und Behandlung (Bild 4). Durch die eGK dürfte es konsekutiv zu deutlichen Einsparungen kommen, beispielsweise durch Vermeidung von Doppeluntersuchungen (v. a. Röntgen, CT, MRT und Labor) und „Doktor-Hopping“. Die Qualität der Behandlung wird verbessert, da mittels der Karte Gesundheitsinformationen hochverfügbar bereitgestellt werden. Ein elektronischer Medikamentenpass kann z. B. die Zahl der Tetanus-Impfungen verringern, die bislang bei

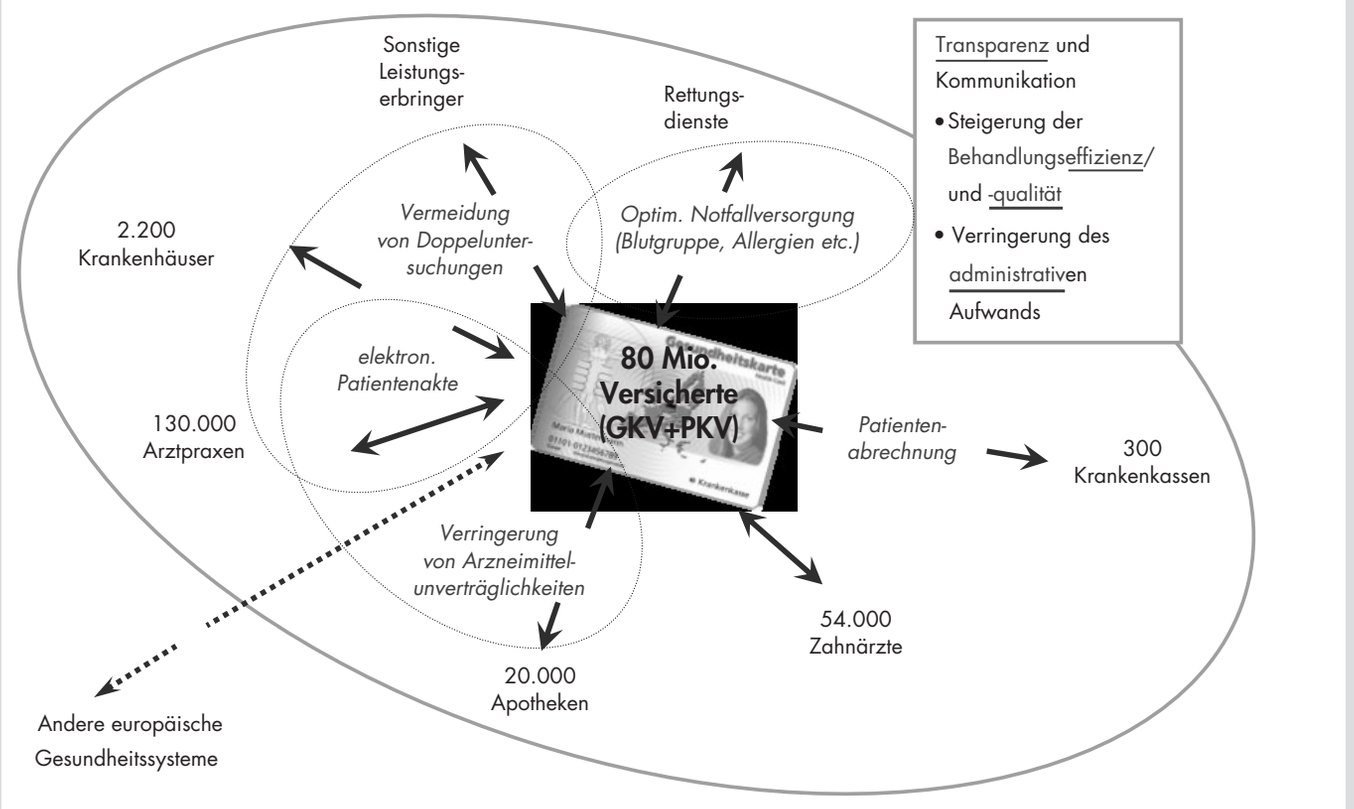

Bild 4 Interaktionsszenario und Nutzenaspekte der eGK

Unfällen häufig nur deshalb vorgenommen werden, weil in der Eile nicht geklärt werden kann, wann die letzte Impfung erfolgte. Er trägt auch zur Verringerung der Zahl von Todesfällen aufgrund von Arzneimittelunverträglichkeiten bei. Außerdem wird die eGK die Abrechnung zwischen den Leistungserbringern und den Krankenkassen erleichtern und deren Transparenz verbessern.

Um mit den künftig sektorübergreifenden Netzen eine optimale Behandlung von Patienten sicherzustellen und gleichzeitig Einspareffekte erzielen zu können, sind zunächst erhebliche Investitionen in die notwendige IT-Plattform erforderlich. Mittlerweile wird von Seiten der Selbstverwaltung mit Kosten von etwa 1,8 Mrd. Euro gerechnet [PfRe04; Bloe04].

6 Status quo im März 2005 und Ausblick

Leistungserbringer und Kostenträger hätten in Entsprechung der gesetzlichen Vorgaben ihr Konzept zur Lösungsarchitektur bis zum 2004-09-30 dem BMGS vorlegen müssen. Dies ist nur zum Teil geschehen, da sich beide Seiten über wesentliche Ausgestaltungspunkte nicht einigen konnten. Das vorliegende Konzept enthält aber jene Impulse aus „bIT4health“, die seitens der Selbstverwaltung für richtig und zweckdienlich erachtet wurden und weitere Festlegungen zur Lösungsarchitektur.

Das BMGS hat die Planungen nicht mittels einer Ersatzvornahme abgelehnt, sondern unter Auflagen den Auftrag zur Weiterführung gegeben und gleichzeitig eine Gesetzesänderung auf den Weg gebracht, damit Entscheidungen künftig im Mehrheitsprinzip zwischen Leistungserbringern und Kostenträgern getroffen werden können. Diese wiederum haben nun die eigenständige Gesellschaft „gematik“ geschaffen, die die weiteren Arbeiten koordiniert, entscheidet und vorantreibt [HAK05]. Für die konzeptionelle Weiterarbeit hat das BMGS einen Forschungs- und Entwicklungsauftrag vergeben, dessen Ergebnisse von der Selbstverwaltung für eine endgültige Lösungsarchitektur übernommen und in der gematik umgesetzt werden sollen.

Ausgehend von der so entstehenden Lösungsarchitektur sollen dann erste Modellversuche beginnen, an denen sich die Bundesländer freiwillig beteiligen können, soweit sie eine entsprechend anteilige Finanzierung gewährleisten. Die Gesundheitskarte ist auch Teil der „eCard-Strategie“ der Bundesregierung, die diese am 2005-03-09 vorgelegt hat [Bund05]. Dabei liegt es auf der Hand, dass koordinierende, selektierende und priorisierende Arbeiten noch vor Beginn der ersten Modellprojekte geleistet werden müssen, auch wenn einige Projektregionen inzwischen eher unkoordiniert voranzuschreiten scheinen. Die weitere Arbeit soll wissenschaftlich begleitet werden.

Die informationstechnologische Vernetzung stellt eine besondere Herausforderung für die integrierte Versorgung dar. Das sog. „Case Management“, letztlich die lebenslange Logistik bzw. Steuerung der Patientenbehandlungen, aller zugehörigen Informationen, der Verbrauchsmaterialien sowie des Kapitals ist nur mit einem umfassenden Informationssystem möglich. Dies bedingt die Beachtung des Datenschutzes und die Einrichtung einheitlicher Schnittstellen und eines modular aufgebauten Systems, das sich sowohl an ein KIS als auch an ein Praxisinformationssystem anbinden lässt, eingebettet in eine Rahmenarchitektur für die Vernetzung mit allen sonstigen Leistungsanbietern, Krankenkassen und Apotheken [Kraf03]. Der Einsatz der eGK für Patienten, der HPC für Ärzte und Apotheker und der zugehörigen Lesegeräte für beide Gruppen einerseits, die Einhaltung von Standards sowie die Berücksichtigung von Datensicherheitsmaßnahmen andererseits sind hierfür Grundvoraussetzung.

7 Zusammenfassung

Durch das GMG wurden in § 291a SGB V detaillierte Regelungen für die Einführung der eGK zum 2006-01-01 festgeschrieben. Dieses Zeitziel wird trotz erkennbarer Fortschritte zunehmend kritisch beurteilt. Deshalb reagiert der Gesetzgeber derzeit mit einer Anpassung der organisatorischen Regelungen. Für den ersten Schritt der Entwicklung der technischen Infrastruktur ist der normative Rahmen dagegen, von Ausnahmen im Detail abgesehen, hinreichend. Er bedarf jedoch der technischen Ausfüllung sowohl bei der Zugriffsorganisation für die auf oder mithilfe der eGK gespeicherten Daten, als auch im Bereich der technischen Zusammenarbeit der Vielzahl von Beteiligten an der Telematik-Infrastruktur. Die neuen §§ 140a, 140b SGB V sehen hierzu eine bessere Verzahnung zwischen ambulanter und stationärer Versorgung vor: Die weitgehende Abschottung der Behandlungskreise von niedergelassenen Vertragsärzten und Krankenhäusern soll – ebenfalls bis 2006 – überwunden werden. Die informationstechnologische Vernetzung stellt eine besondere Herausforderung dar, sollte aber letztlich zu den dringend notwendigen Einsparungen im Gesundheitswesen führen und die Qualität der Behandlung verbessern helfen.

Es ist erkennbar, 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 Entwick-

Abstract

The Prospective Telematics-Framework for Health Care? Legal Framework, Technology, Infrastructure and Economic Aspects

The new regulation of § 291a SGB V as well as political goals mandate the nationwide rollout of an electronic health insurance card in Germany by the 1st of January 2006. The legal framework is laid by the Modernization law for Statutory Health Care. However, major challenges remain in the development of the necessary framework architecture and the integration into existing hospital and physicians' offices management systems. The health insurance card opens the perspective for electronic patient records, promising direct advantages for patients as well as for the health care providers involved. However, it remains to be seen how the currently ongoing dispute about the technical implementation of sensitive data storage involved (card or server based systems) might delay the realization of this ambitious project.

Keywords: Framework Architecture, Health Insurance Card, Electronic Patient Record, Business Processes, Legal Framework, Data Protection

lung Zuständigen hier alle wesentlichen Überlegungen und Funktionen, damit das kommende Konstrukt der elektronischen Patientenakte mit bester Aussicht auf Erfolg und Akzeptanz durch Patienten, Leistungserbringer, Gesetzgeber und Datenschutzbehörden ein funktionierendes Gesamtes werden kann, welches die nächste Dekade des deutschen Gesundheitswesens mit Modellcharakter für europäische Entwicklungen prägen wird.

Literatur

[ATG04] Aktionsforum für Telematik im Gesundheitswesen der GVG, Gesellschaft für Versicherungswissenschaft und -gestaltung e.V.: ATG-Management-Papier, „Elektronische Patientenakte". http://atg.gvg-koeln.de/xpage/objects/patientenakte/docs/4/files/MP_ePa_050118.pdf, Dezember 2004, Abruf am 2005-03-03.

[Beul02] *Beulke, W.:* Strafprozessrecht. 6. Auflage, C. F. Müller, Heidelberg 2002.

[Blob03] *Blobel, B.:* Framework architecture. In: *Blobel, B.; Goldschmidt, A. et al.:* EU-Proposal of common interest in the field of trans-European telecommunications network. Referenz: eTEN 2003/1 (Call for proposals).

[Bloe04] *Blöß, T.:* Telematik im Gesundheitswesen. „Größte elektronische Baustelle weltweit." In: Deutsches Ärzteblatt 101 (2004) 45, C2417.

[Bund05] http://www.bundesregierung.de/-,413.799497/artikel/eCard-Strategie-der-Bundesregi.htm, 2005-03-09, Abruf am 2005-03-11.

[BWB+02] *Bultmann, M.; Wellbrock, R.; Biermann, H.; Engels, J.; Ernestus, W.; Höhn, U.; Wehrmann, R.; Schurig, A.:* Datenschutz und Telemedizin. Anforderungen an Medizinnetze. http://www.bfd.bund.de/technik/telemed.pdf, Stand 10/2002, Abruf am 2005-03-03.

[DNG03] *Dierks, C.; Nitz, G.; Grau, U.:* Gesundheitstelematik und Recht. Rechtliche Rahmenbedingungen und legislativer Anpassungsbedarf. Medizinrecht.de, Frankfurt am Main 2003.

[Fues99] *Fuest, B.:* Datenschutzrechtliche Probleme beim Einsatz von Patientenchipkarten. Univ. Dissertation, Mainz 1999.

[Goet01] *Goetz, C.:* Online-Sicherheit von Patientendaten. Telematische Sicherheitskonzepte für niedergelassene Ärzte. DuD Fachbeiträge, Vieweg Verlag, Braunschweig 2001.

[Gold03] *Goldschmidt, A.:* Der „Markt" Gesundheitswesen. In: *Beck, M.; Goldschmidt, A.; Greulich, A.; Kalbitzer, M.; Schmid, R.; Thiele. G. (Hrsg.):* Management Handbuch DRGs. Hüthig/Economica, Heidelberg 2003, C3720/1-24.

[GGH04] *Goldschmidt, A.; Goetz, C. F-J; Hornung, G.:* Die elektronische Gesundheitskarte. Recht, Technologie, Infrastruktur und Ökonomie. In: *Fischer, H.; Gerhardt, E.-P.; Greulich, A.; Räpple, T.; Schneider, E.; Thiele, G.; Ulmer, H. U.; Degener-Hencke, U. (Hrsg.):* Management Handbuch Krankenhaus. Hüthig/Economica, Heidelberg 2004, C790/1-33.

[HAK05] Neue Betriebsorganisation soll Start der Gesundheitskarte beschleunigen. Ärztezeitung, 2005-01-12.

[Horn04] *Hornung, G.:* Der zukünftige Einsatz von Chipkarten im deutschen Gesundheitswesen. In: *Horster, P. (Hrsg.):* D-A-CH Security 2004. Syssec, Klagenfurt 2004, S. 226–237.

[KDSB01] *Konferenz der Datenschutzbeauftragten des Bundes und der Länder:* Entschließung der 62. Konferenz zu Datenschutzrechtlichen Anforderungen an den „Arzneimittelpass" (Medikamentenchipkarte). http://www.datenschutz-berlin.de/doc/de/konf/65/top07.htm, 2001, Abruf am 2005-03-03.

[Kraf03] *Kraft D.:* Telematik im Gesundheitswesen, Vertragsarzt- und Datenschutzrechtliche Aspekte. Deutscher Universitätsverlag, Wiesbaden 2003.

[MeGo04] *Meyer-Goßner, L.:* Strafprozessordnung. Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen. 47. Auflage, C. H. Beck, München 2004.

[Mert04] *Merten, M.:* Europäische Krankenversicherungskarte – Das Fundament ist gelegt. In: Deutsches Ärzteblatt 101 (2004) 1–2, C 17.

[PfRe04] *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), 2004-2-21.

[Rabb05] *Rabbata, S.:* Elektronische Gesundheitskarte: Kein Start auf Knopfdruck. Deutsches Ärzteblatt 102 (2005) 4, A 96.

[Roßn04] *Roßnagel, A.:* Einleitung zum Signaturgesetz. In: *Roßnagel, A. (Hrsg.):* Recht der Multimedia-Dienste. Kommentar zum IuKDG und zum MDStV. Loseblatt, C. H. Beck, München, Stand: Juni 2004.

[SCB03] 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, 2003.

[Stat02] *Statz A.:* Aktionsforum Gesundheitsinformationssystem für Deutschland (AFGIS). In: *Klusen N., Meusch A.* (Hrsg): Gesundheitstelematik, Medizinischer Fortschritt durch Informationstechnologie. Nomos Verlagsgesellschaft, Baden-Baden 2002.

[TAB02] *Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB):* Biometrische Identifikationssysteme – Sachstandsbericht. BT-Drs. 14/1005, 2002.

[Ward02] *Warda F.; Noelle G.:* Telemedizin und eHealth in Deutschland: Materialien und Empfehlungen für eine nationale Telematikplattform. Deutsches Institut für medizinische Dokumentation und Information, 2002.

[Weic04] *Weichert, T.:* Die elektronische Gesundheitskarte. In: Datenschutz und Datensicherheit 28 (2004) 7, S. 391–403.