LD4 71.03/01.008
LD4 Ö GesKarte
Stand 06.05.2004

Die elektronische Gesundheitskarte und der Datenschutz

von Thilo Weichert

I. Vorgeschichte

Bringt die elektronische Gesundheitskarte - auch Patienten-Chipkarte[1] genannt - den „**gläsernen Patienten**"? Diese Frage geistert als eine der vielen Angstthemen im Zusammenhang mit der Modernisierung und Automation des Gesundheitswesens durch die Diskussionen bei Ärzten, Patienten und in der Öffentlichkeit. Die Befürchtung, dass mit der elektronischen Gesundheitskarte (künftig abgekürzt eGK) das Ende von Wahlfreiheit und Vertraulichkeit im Gesundheitswesen kommen könnte, ist nicht völlig unbegründet. Nahm doch die Bundesgesundheitsministerin Ulla Schmidt den Lipobay-Skandal bei der Fa. *Bayer* Ende 2001 zum Anlass, die Diskussion über diese Karte neu zu initiieren, indem sie forderte, dass auf der eGK als Weiterentwicklung der Versichertenkarte der gesetzlichen Krankenversicherung (GKV-Karte) alle erfolgten Medikationen obligatorisch zu speichern seien, und zugleich versprach, mit einer solchen Karte hätte es den Skandal nicht gegeben.[2]

Als **Zwecke einer eGK** werden angegeben: Höhere Behandlungsqualität, mehr Effizienz im Gesundheitswesen (Wirtschaftlichkeit) und Stärkung der Patientenrechte.[3] Tatsächlich lassen sich diese Ziele alle mit einer über die eGK verbesserte elektronische Kommunikation zwischen den Beteiligten erreichen. Zwangsläufig sind diese Effekte jedoch nicht. Hauptmotivation für die Einführung der eGK und demgemäß Zentralmotiv bei der technischen Ausgestaltung ist i.d.R. das Einsparen von Kosten.[4] Auch die informationstechnische Wirtschaft demonstriert - angesichts der gewaltigen Verdienstmöglichkeiten verständlicherweise - ein nachhaltiges ökonomisches Interesse an der eGK.

Es dauerte offensichtlich lang, bis die Gesundheitsministerin von ihren Experten überzeugt werden konnte, dass eine Zwangs-Medikationskarte aus rechtlichen wie aus Akzeptanzgründen nicht durchgesetzt werden kann und dass eine solche Karte beileibe nicht alle Probleme im Gesundheitsbereich zu lösen in der Lage sein wird. Es zeugt von umfassender Einsicht, dass das *Bundesministerium für Gesundheit und soziale Sicherheit* (künftig BMGS) zusammen mit den Spitzenorganisationen der Gesundheitswirtschaft zum Einsatz von Telematik am 03.05.2002 über den Zusammenschluss *Aktionsforum Telematik im Gesundheitswesen* (ATG)[5] nicht den Zwang, sondern die **Freiwilligkeit für den Patienten** bei der eGK in den Vordergrund stellte: „Die Gesundheitskarte soll den europäischen Notfalldatensatz des Patienten, seine persönliche Identifikation/Authentifizierung sowie Verweisfunktionen u.a. auf die Arzneimitteldokumentation und das elektronische Zuzahlungsmanagement des Patienten enthalten. ... Es besteht Einigkeit, dass die mit dem Ausbau der Gesundheitskarte verbundene Speicherung und Verarbeitung der Gesundheitsdaten als freiwilliges Angebot an die Versicherten zu gestalten ist, insbesondere

- dass die Datenhoheit der Patienten und der Grundsatz der Freiwilligkeit der Speicherung von Gesundheitsdaten bewahrt wird,
- dass Patienten entscheiden können, welche Gesundheitsdaten aufgenommen und welche gelöscht werden,
- dass Patienten entscheiden können, ob und welche Daten sie einem Leistungserbringer zugänglich machen,
- dass keine zentral gespeicherten Datensammlungen über Patientinnen und Patienten entstehen,
- dass Patienten und Versicherte das Recht haben, über sie gespeicherte Daten vollständig zu lesen,

---

1 Patient Data Card - PDC, vgl. Teletrust Deutschland e.V., Kartenreport - Intelligente Chipkarten im Gesundheitswesen, März 2004, Kap. 2, Anhang A.

2 Tätigkeitsbericht (TB) 2002 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD SH), Kap. 4.8.2.

3 Bales, Vortragsfolien, Die Einführung der Telematik im Gesundheitswesen als Herausforderung für die Weiterentwicklung der Patientenrecht in Deutschland, Tagung der B.A.G.H. in Bonn am 07.11.2003; Teletrust, Kap. 3; Bundesbeauftragter für den Datenschutz (BfD), 19. Tätigkeitsbericht (TB) 2001/2002, Kap. 28.3.

4 Nachweise für Einsparpotenziale sind dokumentiert bei Gerhardt/Kaeding in Taeger/Wiebe, Informatik - Wirtschaft - Recht, Festschrift für Wolfgang Kilian, 2004, S. 198, 217 f.

5 BfD, 18. TB 1999/2000, Kap. 25.1.1.

– dass die Verwendung der gespeicherten Patientendaten selbstverständlich nur innerhalb des gesetzlichen Rahmens unter Wahrung des bestehenden Schutzniveaus (z.B. Beschlagnahmeschutz) in der Arztpraxis erlaubt ist."[6]

Dieses patientenorientierte Votum wurde von der 75. *Gesundheitsministerkonferenz* positiv aufgegriffen. Der Bundesgesetzgeber war also gut beraten, als er im Rahmen des Gesundheitsmodernisierungsgesetzes eine Regelung zur eGK aufnahm, die den genannten Grundsätzen der Wahlfreiheit und der Vertraulichkeit entspricht. So begrüßte die *Konferenz der Datenschutzbeauftragten des Bundes und der Länder* (DSB-Konferenz), bei mancher sonstigen harschen Kritik am Gesundheitsmodernisierungsgesetz Ende 2003, dass eine „datenschutzfreundliche Lösung" erreicht werden konnte, die die „Verfügungsgewalt der Patientinnen und Patienten" wahrt.[7]

In mehreren Pilotprojekten, u.a. im Rahmen des regionalen Praxisnetzes Flensburg, wird die eGK erprobt.[8] Dabei ist eine zentrale Erfolgsvoraussetzung, dass von Anfang an bei der Planung, Konzipierung, Erprobung und Umsetzung der **Datenschutz** bzw. das **Patientengeheimnis** mit berücksichtigt werden. Datenschutz und Patientengeheimnis, also die Vertraulichkeit des Behandlungsverhältnisses zwischen Arzt und Patient, sind wesentliche Voraussetzungen für die Effektivität des Gesundheitswesens.[9] Datenschutz steht einer modernen und effektiven, d.h. auch qualifizierten und schnell intervenierenden Gesundheitsversorgung nicht entgegen[10], sondern ist Voraussetzung für diese.

Die eGK soll bundesweit flächendeckend zum 01.01.2006 eingeführt werden.[11] Sie soll der elektronische Schlüssel sein zur Einrichtung der **übergreifenden Kooperation** bzgl. über 70 Mio. Versicherten zwischen den Beteiligten im Gesundheitswesen mit u.a. rund 270.000 Ärzten, 77.000 Zahnärzten, 2.000 Krankenhäusern, 22.000 Apotheken und über 300 Krankenkassen.[12]

II. Die Regelung des § 291a SGB V

Im Sozialgesetzbuch V (SGB V) wurde mit Wirkung vom 01.01.2004 ein „§ 291a Elektronische Gesundheitskarte" eingeführt, wonach bis spätestens zum 01.01.2006 „zur **Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz** der Behandlung" die bisherige GKV-Karte erweitert werden soll (Abs. 1).

Verpflichtend ist nach Abs. 2 zusätzlich zu den bisherigen Funktionalitäten der GKV-Karte „die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form" sowie der Krankenversicherungs-Berechtigungsnachweis nach dem Recht der Europäischen Union.

Wenn die **Einwilligung der Versicherten** vorliegt, muss die eGK nach Abs. 3 folgende Anwendungen der Datenverarbeitung unterstützen:

1. medizinische Notfallversorgungsdaten,
2. elektronischer Arztbrief (Befunde, Diagnosen, Therapieempfehlungen, Behandlungsberichte für einrichtungsübergreifende fallbezogene Kooperation),
3. Arzneimitteldokumentation,
4. elektronische Patientenakte (Arztbriefe sowie Impfungen für fall- und einrichtungsübergreifende Dokumentation),
5. freiwillige Daten von oder durch den Versicherten,
6. in Anspruch genommene Leistungen und deren vorläufige Kosten (§ 305 Abs. 2 SGB V).

---

6 Zit. nach Weichert, Patienten-Chipkarte, Vertrauensschutz und Datenschutz, Vortrag am 07.06.2002 in Bielefeld, www.datenschutzzentrum.de/material/themen/gesund/geschip.htm; dok. auch in BfD, 19. TB 2001/2002 (= BT-Drs. 15/888), Anlage 29.

7 66. DSB-Konferenz 25./26.09.2003 in Leipzig, www.lda.brandenburg.de/dsk/dsk66/dsk; zur Bedeutung des Nutzervertrauens in die Technik für die Kartenakzeptanz vgl. auch Teletrust (Fn. 1), Kap. 3.

8 Projektgruppe Gesundheitskarte SH, Einführung der elektronischen Gesundheitskarte in Schleswig-Holstein, 2004; TB 2003 ULD SH, Kap. 4.8.2.; TB 2004 ULD SH, Kap. 4.7.6.

9 BVerfGE 32, 380.

10 So aber z.B. Ludwig in Jäckel, Telemedizinführer Deutschland, 2004, S. 206.

11 Zum Zeitplan ausführlich Antwort der BReg. auf die Kleine Anfrage der Abg. Sehling u.a. (CDU/CSU), BT-Drs. 15/2708, BT-Drs. 2810 v. 30.03.2004; Zweifel am Zeitplan äußerten Krankenkassen, Ärzteorganisationen und Krankenhäuser, dpa 26.03.2004; vgl. auch Schulzki-Haddouti, c't 10/2004, 32 f.

12 Bales/Holland in Jäckel (Fn. 10), 18; Teletrust (Fn. 1), Kap. 3..

Spätestens bei der Versendung der Karte hat die Krankenkasse den Versicherten allgemein verständlich über die Funktionsweise zu informieren. Die vor der Verarbeitung einzuholende Einwilligung ist auf der Karte zu dokumentieren. Sie ist widerruflich und kann auf einzelne Anwendungen beschränkt werden. Das Nähere über Inhalt und Struktur der Verarbeitung ist in einer Vereinbarung der Spitzenorganisationen nach Abs. 7 zu regeln. Nach Abs. 5 S. 1 u. 2 erfolgt nicht nur die Erfassung und Speicherung, sondern auch das Auslesen der Daten durch Autorisierung des Versicherten (Ausnahme Notfalldaten).

Nach Abs. 4 wird die Verarbeitung mit Hilfe der eGK auf das **Erforderliche** „zur Versorgung" eingegrenzt; der Zugriff wird beschränkt auf den Versicherten sowie auf Ärzte, Zahnärzte, Apotheker. In eingeschränktem Umfang wird sonstigem pharmazeutischem Personal und sonstigen Erbringern ärztlich verordneter Leistungen bzw. Angehörigen eines Heilberufs der Zugriff und die Nutzung erlaubt. Der Zugriff der „Health Professionals" darf nach Abs. 5 S. 3 nur mit Hilfe eines elektronischen Heilberufsausweises, möglichst ausgestaltet als elektronische Signaturkarte, erfolgen. Ersatzweise dürfen auch andere geeignete technische Autorisierungsverfahren genutzt werden und auch Hilfspersonen zugreifen, wenn die nachprüfbare Protokollierung gesichert ist.

Auf Anforderung des Versicherten müssen gespeicherte Verordnungen sowie alle freiwilligen Daten nach Abs. 3 gelöscht werden (Abs. 6 S. 1). Mindestens die letzten 50 Zugriffe auf die Karte bzw. mit der Karte sind für Zwecke der Datenschutzkontrolle zu protokollieren. Abs. 8 S. 1 verbietet es vom Versicherten zu verlangen, den Zugriff auf Versichertendaten anderen als den gesetzlich Befugten zu gestatten. Die Nutzung der Karte bzw. die Verweigerung des Zugriffs hierauf darf weder zu einer Bevorzugung oder einer Benachteiligung führen (Abs. 8 S. 2). Die allgemeinen **datenschutzrechtlichen Vorschriften** zum Einsatz von Chipkarten (§ 6c BDSG) sind auch auf die eGK anzuwenden (Abs. 2 S. 2).

Neben dem § 291a SGB V bleibt weiterhin der § 291 SGB V zur „**Krankenversichertenkarte**" (GKV-Karte) anwendbar, der mit Wirkung zum 01.01.2004 auch geändert wurde. Diese Regelung legt fest, dass die GKV-Karte als Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung und für die Abrechnung mit den Leistungserbringern verwendet wird. Ergänzend zu den bisherigen Daten (Krankenkasse, Namen, Geburtsdatum, Anschrift, Krankenversichertennummer, Versichertenstatus und Gültigkeitsdaten) sind die Speicherung des Lichtbildes, des Geschlechtes und des Zuzahlungsstatus vorgesehen (§ 291 Abs. 2 SGB V).

Im Folgenden werden die **datenschutzrechtlichen Anforderungen** an die eGK dargestellt. Neben den zwingenden rechtlichen Anforderungen besteht die Pflicht, die Grundsätze der Datensparsamkeit und der Datenvermeidung zu beachten (§ 78b SGB X, § 9a BDSG, § 4 Abs. 1 LDSG SH). Außerdem gilt der Grundsatz, dass die Patientinnen und Patienten durch die eGK nicht schlechter gestellt werden dürfen, als dies zuvor der Fall war.[13] Nicht diskutiert werden sollen solche Fragen, die schon im Rahmen der Nutzung der bisherigen GKV-Karte geklärt sind. Schwerpunkt wird gelegt auf die rechtlichen und organisatorischen, nicht auf die technischen Fragestellungen. Dabei kann angesichts des relativ frühen Stadiums der Diskussion keine umfassende Darstellung erfolgen. Die Darstellung ist nicht nur noch nicht vollständig, sondern auch kritikbedürftig und -fähig. Der Autor ist sehr an konstruktiver Kritik interessiert, die zu Ergänzungen und Verbesserungen der hier formulierten Anforderungen beitragen kann.

Chipkarten können nicht separat datenschutzrechtlich bewertet werden, vielmehr muss deren Einbettung in eine **informationstechnische Infrastruktur** (Hintergrundsysteme) berücksichtigt werden. Da insofern noch viele Fragen offen sind, können vorliegend teilweise nur allgemein gehaltene Aussagen gemacht werden.

III. Wer ist verantwortliche Stelle?

Bei der Datenverarbeitung mit der eGK erfolgt eine Interaktion zwischen einer Vielzahl von unterschiedlichen Stellen, z.B. Krankenkasse, Arzt, Apotheker, sonstige Leistungserbringer, Patient. Die Verantwortlichkeit hierfür im Sinne des Datenschutzrechts liegt nicht ausschließlich bei der **Krankenkassen**. Diese sind vielmehr die „ausgebende Stelle", deren Verantwortung es zunächst ist, die Betroffenen über Funktionsweise, Betroffenenrechte und Umgang mit der Karte zu unterrichten (§ 6c Abs. 1 BDSG). Weiterhin muss die jeweilige Krankenkasse dafür Sorge tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte und Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen (§ 6c Abs. 2 BDSG).[14]

---

13 BfD (Fn. 6), Kap. 28.1.

14 Bizer in Simitis, Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. 2003, § 6c Rz. 24.

Verantwortlich für den jeweiligen Datenverarbeitungsvorgang sind diejenigen Personen oder Stellen, die die personenbezogenen Daten für sich erheben oder weiter verarbeiten, egal ob sie dies selbst tun oder durch andere im Auftrag vornehmen lassen (§ 67 Abs. 9 SGB X, § 3 Abs. 7 BDSG, § 2 Abs. 3 LDSG SH). Dies kann die Krankenkasse sein (z.B. bei der Ausstellung der eGK oder Erhebung von Abrechnungsdaten, vgl. § 284 SGB V), der Arzt oder ein Krankenhaus, die z.B. Notfalldaten erfassen, ein elektronisches Rezept oder einen elektronischen Arztbrief ausstellen, oder der Apotheker, der ein elektronisches Rezept abruft, um das Medikament auszugeben.[15]

Hinsichtlich des **anzuwendenden Rechts** gilt für diese Stellen nicht zwangsläufig das SGB V. Dies ist umfassend nur der Fall für die Krankenkassen (oder z.B. die kassenärztlichen Vereinigungen). Für ambulante Ärzte, Apotheker, private Krankenhäuser und sonstige Leistungserbringer gilt vorrangig das Bundesdatenschutzgesetz (BDSG, insbes. die §§ 27 ff. BDSG), für öffentlich-rechtliche Krankenhäuser das jeweilige Bundes- bzw. Landesdatenschutzgesetz (z.B. LDSG SH).

Die **Versicherten** sind in der Regel für die Datenverarbeitung im Datenschutzsinn nicht verantwortlich. Dies gilt selbst für den Fall, dass sie ihre Daten für die eGK selbst zur Verfügung stellen (§ 291 Abs. 3 Nr. 5 SGB V), wenn die Erfassung nach entsprechender Prüfung durch eine andere Stelle (z.B. durch den Arzt oder die Krankenkasse) erfolgt. Zwar ist es Bestandteil des Konzeptes der eGK, dass der Patient bzw. Betroffene „etwas selbst in der Hand hat".[16] Von Verantwortlichkeit i.S.d. Datenschutzrechtes des Betroffenen kann aber nur dann die Rede sein, wenn eine Datennutzung bzgl. Zweck, Adressat und Inhalt von diesem bestimmt wird.[17] Die Verantwortlichkeit liegt beim Patienten also nur bzgl. solcher Formen der Datenverarbeitung, bei denen er diese selbst festlegt. Angesichts des Umstandes, dass bei den Anwendungen nach § 291a Abs. 3 SGB V die Einwilligung zur Grundlage für die jeweiligen Formen der Datenverarbeitung gemacht werden, ist es in vielen Fällen von untergeordneter rechtlicher Bedeutung, wer für die ursprüngliche Speicherung der Daten als verantwortlich angesehen wird.

Soweit über die Karte **ärztliche Datenverarbeitung** erfolgt, sind die jeweiligen Ärztlichen Berufsordnungen anzuwenden (z.B. Berufsordnung der Ärztekammer Schleswig-Holstein, BO ÄK SH). Soweit auf bzw. über die Karte eine ärztliche Datenspeicherung stattfindet, wird damit der ärztlichen Dokumentationspflicht entsprochen. Daher darf der Arzt nicht ungeprüft Daten des Patienten erfassen. Ihm obliegt die Verantwortung für die Erforderlichkeit und Richtigkeit der Speicherungen. Es handelt sich aber in keinem Fall um den ärztlichen Originaldatenbestand (z.B. i.S.v. § 10 BO ÄK SH).[18] Dieser muss in konventioneller oder elektronischer Form gesondert geführt werden.

IV. Sensibilität der verarbeiteten Daten

Die über die eGK verarbeiteten Daten sind durchgängig von hoher Sensibilität. Soweit die Verarbeitung bei den Leistungserbringern erfolgt, unterliegen sie weitestgehend der beruflichen bzw. der ärztlichen Schweigepflicht (**Patientengeheimnis**) nach § 203 Abs. 1 StGB und den Ärztlichen Berufsordnungen (z.B. § 9 BO ÄK SH). Es handelt sich um **besondere Arten personenbezogener Daten** (vgl. § 3 Abs. 9 BDSG), deren Verarbeitung engen rechtlichen Anforderungen unterliegt (vgl. § 28 Abs. 6-9 BDSG). Zu diesen Anforderungen gehören: Einwilligungen müssen sich ausdrücklich auf die besonders sensiblen Daten beziehen (vgl. 4a Abs. 3 BDSG). Ohne Einwilligung ist die Verarbeitung nur zum Schutz lebenswichtiger Interessen des Betroffenen zulässig (vgl. § 28 Abs. 6 Nr. 1 BDSG). Erfolgt die Verarbeitung zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten, so muss sie durch ärztliches oder ähnlich schweigepflichtiges Personal vorgenommen werden (vgl. § 28 Abs. 7 S. 1 BDSG). Bei der Weitergabe der Daten sind strenge Zweckbindungen zu beachten (vgl. § 28 Abs. 7 S. 4, Abs. 8 BDSG).

Soweit die Verarbeitung der eGK-Daten bei Sozialleistungsträgern erfolgt, unterliegen die Daten dem **Sozialgeheimnis** (§ 35 SGB I, §§ 67 ff. SGB X). Es gilt, wenn sie über einen beruflichen Geheimnisträger erhoben wurden, eine besondere Zweckbindung (§ 76 SGB X). Auch bei der Weitergabe durch den Sozialleistungsträger sind enge Zweckbindungen zu beachten (§ 78 SGB X).

---

15 Weichert in Roßnagel, Handbuch Datenschutzrecht, Kap. 9.5 (Chipkarten), Rz. 25, 30.

16 Teletrust (Fn. 1).

17 Dammann in Simitis (Fn. 14), § 3 Rz. 233.

18 Bales/Holland in Jäckel (Fn. 10), 16.

Wird über die eGK eine **Auftragsdatenverarbeitung** ausgelöst, so sind die jeweiligen Regelungen zu beachten, d.h. für die Krankenkassen der § 80 SGB X, für private Leistungserbringer § 11 BDSG sowie für öffentliche Leistungserbringer die Norm zur Auftragsdatenverarbeitung nach Bundes- bzw. Landesrecht (z.B. § 17 LDSG SH). Unterfallen die dabei verarbeiteten Daten zugleich einem Berufsgeheimnis nach § 203 Abs. 1 StGB, was regelmäßig der Fall sein dürfte, so muss dies bei der Auftragsdatenverarbeitung berücksichtigt werden. Die bedeutet, dass i.d.R. die Auftragsdurchführung nur mit Pseudonymen zulässig ist, wenn zugleich sichergestellt ist, dass dem Auftragnehmer die Zuordnung des Pseudonyms zu einer konkreten Person nicht möglich ist.[19]

V. Funktionen

Chipkarten können eine große Zahl von **unterschiedlichen Funktionen** erfüllen.[20] Bei der eGK ist dies der Fall. Hierbei wird unterschieden zwischen

- **Ausweisfunktion** (z.B. Nachweis der Berechtigung zur Inanspruchnahme von medizinischen Leistungen, vgl. VI),
- **Erklärungsfunktion** (z.B. die Erklärung, mit Übergabe der Karte bestimmte medizinische Leistungen zu Lasten der gesetzlichen Krankenversicherung in Anspruch nehmen zu wollen; digitales Signieren eines Dokuments),
- **Dokumentations- oder Speicherfunktion** (z.B. die Speicherung von Notfalldaten oder Impfstatus),
- **Übermittlungsfunktion** (z.B. die Weitergabe von Identifikations- und medizinischen Daten an die verschiedenen Leistungserbringer),
- und **Verschlüsselungsfunktion** (z.B. die Möglichkeit, mit Hilfe eines auf der Karte gespeicherten Schlüssels an anderer Stelle gespeicherte Daten zu entschlüsseln und zu nutzen).

Eine Kombination von Übermittlungs- und Verschlüsselungsfunktion besteht in der **Verweisfunktion** (auch sog. Pointer- oder Ticket-Funktion): Damit können auf externen Servern von medizinischen Stellen gespeicherte Daten der Person des Patienten zugeordnet und mit Hilfe eines auf der Karte gespeicherten Schlüssels entschlüsselt und abgerufen werden. Die eGK wird in diesem Fall also dazu genutzt, Daten über ein Netz zu übermitteln, ohne dass die Daten selbst, sondern nur ein Verweis hierauf auf der Karte gespeichert wird. § 291a SGB V enthält generell keine Festlegung, welche Daten auf der Karte und welche auf Server gespeichert werden dürfen bzw. müssen. Die Festlegung soll im Rahmen des Standardisierungsprozesses erst nach Auswertung der Pilotphase vorgenommen werden.

Bei der eGK wird die Ausweisfunktion (Berechtigungsnachweis) und die Übermittlungsfunktion für die Rezeptübertragung obligatorisch eingeführt. Alle sonstigen Funktionen sollen fakultativ sein. Spätestens vom 01.01.2006 an sollen sämtliche **Pflichtfunktionen** bundesweit realisiert sein. Die freiwilligen Funktionen der eKG sollen zuvor oder danach schrittweise eingeführt werden.

VI. Ausweisfunktion

Die GKV-Karte dient derzeit schon zum Nachweis der **Berechtigung zur Inanspruchnahme von Leistungen** im Rahmen der vertragsärztlichen Versorgung (§ 291 Abs. 1 S. 3 SGB V). Künftig erfolgt dieser Berechtigungsnachweis innerhalb der gesamten europäischen Gemeinschaft (§ 291a Abs. 2 S. 1 Nr. 2 SGB V). Zum Nachweis des Leistungsanspruchs genügt i.d.R. die Vorlage der Karte. Um zu gewährleisten, dass keine Nichtberechtigten Leistungen mit der Karte in Anspruch nehmen, sind Identifizierungsangaben des Berechtigten auf der Karte enthalten. Dies sind schon bisher Unterschrift Namen, Geburtsdatum, Anschrift, Krankenversichertennummer und künftig zusätzlich Lichtbild und Geschlecht.[21]

Während die Berechtigung zur Inanspruchnahme von Leistungen innerhalb der Bundesrepublik auch elektronisch überprüft werden kann, soll die Aufnahme des **europäischen Auslandskrankenscheins** auf der Rückseite der eGK nur als Sichtdokument erfolgen (Dokument E 111).[22] Der Europäische Rat hat beschlossen, dieses ab dem 01.06.2004 europaweit einzuführen. Bis zum Ende dieser 2. Stufe (voraussichtlich 31.12.2005) findet die Plastikkarte als Sichtausweis parallel zum bisherigen Verfahren (Papierformular und Sichtkarte) Anwendung.

---

19 http://www.datenschutzzentrum.de/material/themen/gesund/patdvia.htm.

20 Siehe Überblick bei Weichert (Fn. 15), Rz. 4; Teletrust (Fn. 1), Kap. 2, unterscheidet nur zwischen Ausweis- und Datenträgerfunktion.

21 Gesetzesbegründung, zit. nach KKF, SGB V-Handbuch, 2004, S. 323.

22 EU-Kommission, ABl. der EU, L 276/1 v. 27.10.2003.

Das elektronische Lesen der europäischen Identifizierungsdaten wäre nach der gesetzlichen Regelung nicht ausgeschlossen. Als 3. Stufe ist ab 2008 ein Umstieg auf einen elektronischen Datenträger vorgesehen.[23]

Bei der Ausweisfunktion lässt sich unterscheiden zwischen der **Identifizierung**, der Authentifzierung und der Autorisierung. Identifizierung ist die (möglichst) zweifelsfreie Feststellung der Identität einer Person. Derzeit ist vorgesehen, dass Leistungen der gesetzlichen Krankenversicherung nach SGB V nur an identifizierte Kassenmitglieder von i.d.R. ebenso (per HPC) zu identifizierenden Leistungserbringer erbracht werden dürfen. Der Nachweis eines Pseudonyms genügt nicht. Mit der eGK soll die Identifizierung des Leistungsberechtigten abschließend erfolgen. Für ein ergänzendes Anfordern von Identitätsnachweisen (z.B. Personalausweis) gibt es keine rechtliche Grundlage. Authentifizierung ist der Nachweis der Identität gegenüber dem System. Dies erfolgt über die Nutzung der eGK, evtl. ergänzt durch die Eingabe einer PIN oder durch einen biometrischen Abgleich. Die eGK (ebenso die HPC) wird dazu genutzt, dass bestimmte Rollen in den telemedizinischen Systemen wahrgenommen werden können.

Autorisierung ist die Zuordnung von Rechten zu einem Subjekt. Dies setzt voraus, dass die Person identifiziert oder dass eine erlaubte Rolle authentifiziert wurde. Die eGK autorisiert zur Inanspruchnahme von Gesundheitsleistungen sowie auch zur Wahrnehmung bestimmter Befugnisse zur Datenverarbeitung (z.B. Abruf von Daten).

Voraussetzung für eine eindeutige Identifizierung durch die Karte ist deren Eindeutigkeit. Diese wird technisch zunächst durch eine spezielle Kartennummer (Kombination aus Kennnummern des Halbleiterherstellers, der Produktionsstätte, des Batches und der Seriennummer) realisiert. Im Rahmen der „Initialisierung" werden die Anwendungen für die eGK auf die Chipkarte geladen. Die **Personalisierung** erfolgt i.d.R. durch die ausgebende Stelle (Krankenkasse). Dabei werden die Identifizierungsdaten, weitere Grunddaten und das Foto auf die Karte aufgebracht. Danach soll die Karte als Unikat eindeutig einer Person zugeordnet sein.

Die Krankenkasse hat den Verzeichnisdienst über die bei ihr Versicherten zu führen. Ein zentrales kassenübergreifendes **Versichertenverzeichnis**, evtl. auch über einen gemeinsamen Auftragnehmer, ist unzulässig (vgl. § 80 Abs. 5 Nr. 2 S. 2 SGB X).

Die **Versichertennummer** (KV-Nummer) soll künftig nach § 290 Abs. 1 SGB V aus einem unveränderlichen Teil zur Identifikation des Versicherten bestehen sowie einem veränderlichen Teil, der nach bundeseinheitlichen Vorgaben die Krankenkasse und die Familienzugehörigkeit von Mitversicherten erkennen lässt. Wie die KV-Nummer erstellt wird, ist bis zum 30.06.2004 von den Spitzenverbänden festzulegen. Eine zentrale Generierung der Nummer ist nicht ausgeschlossen. Doch darf diese nicht zu einem zentralen Versichertenverzeichnis führen. Hierfür besteht keine Rechtsgrundlage. Denkbar ist z.B., dass nach einer zentralen Nummernvergabe bei der Vergabestelle lediglich gespeichert bleibt, welche unveränderlichen Teile an welche Krankenkassen vergeben wurden (vgl. das ähnliche Verfahren bei der Bundesdruckerei mit Pässen und Personalausweisen: § 16 Abs. 3 PassG, § 3 Abs. 3 PAuswG).

Die Karte wird durch die jeweilige Kasse herausgegeben. Bei **Kassenwechsel** wird der unveränderliche Teil der Versichertennummer übernommen. Dies kann direkt über die eGK erfolgen. Alternativ möglich ist die direkte Datenerhebung beim neuen Kassenmitglied oder die von diesem autorisierte Datenabfrage bei der alten Krankenkasse. Möglich wäre sogar die Übernahme der alten Karte durch die neue Krankenkasse unter teilweiser Beibehaltung der bestehenden Daten. Da die neue Krankenkasse zumindest bzgl. der Stammdaten die Verantwortlichkeit übernehmen muss, besteht insofern die Pflicht, diese Daten zu verifizieren.

Die **Identifizierung** über die eGK kann auf unterschiedliche Weise erfolgen, entweder optisch oder auch elektronisch. I.d.R. wird die Vorlage des Ausweises als Berechtigungsnachweis für eine zuvor definierte Gesundheitsleistung oder für eine informationstechnische Nutzung genügen. Im Zweifel müssen zusätzlich zur Vorlage der Karte Methoden der Identifzierung möglich sein. Der Abgleich einer Unterschrift wäre möglich, ist aber aus praktischen Gründen zu aufwändig. Daher wurde zusätzlich das Lichtbild in die eGK aufgenommen. Ein weiterer Vorteil des Lichtbildes besteht darin, dass Karten in Notfällen einem Patienten auch dann zugeordnet werden können, wenn dieser nicht ansprechbar ist.

Um zu vermeiden, dass Nichtberechtigte die eGK nutzen, soll für höchstpersönliche Zwecke vom Versicherten eine **PIN** (Personal Identification Number) genutzt werden. Diese zusätzliche Sicherheit ist gesetzlich nicht

---

[23] Bales/Holland in Jäckel (Fn. 10), 15 f.; Teletrust (Fn. 1), Kap. 5.3.; BReg., BT-Drs. 15/2810 (Fn. 11), Frage 35.

ausdrücklich geregelt, wird aber in § 291a Abs. 5 S. 2 SGB V für die meisten freiwilligen Anwendungen vorausgesetzt. Einer ausdrücklichen gesetzlichen Regelung bedarf es auch nicht, solange die obligatorische Nutzung ohne PIN möglich ist. Mittelfristig ist davon auszugehen, dass bestimmte Anwendungen der eGK (z.B. Eigenauskunft) von einer PIN-Eingabe oder vom Einsatz eines biometrischen Verfahrens abhängig gemacht werden. Auch die Nutzung der eGK für elektronische Erklärungen setzt zumindest die Nutzung einer PIN voraus. Praktische Probleme können dadurch entstehen, dass vor allem ältere Menschen mit der PIN-Funktionalität überfordert sein könnten. Auch deshalb muss es aus praktischer Sicht zumindest für die Pflichtanwendungen eine Alternative zur PIN-Nutzung geben.

Die eGK soll als Mikroprozessorkarte so ausgestaltet werden, dass mit ihr künftig eine **elektronische Signatur** erstellt werden kann (§ 291 Abs. 2a S. 3 SGB V); diese Funktionalität soll zunächst noch nicht realisiert werden. Sie soll aber entsprechend erweitert werden können. Damit würde die Karte auch neue Erklärungsfunktionen erfüllen können.[24]

Der Zugriff auf die freiwillig gespeicherten Patientendaten nach § 291a Abs. 3 S. 1 SGB V kann mittels einer eigenen Karte erfolgen, die über einen qualifizierten elektronischen Signaturschlüssel verfügt (§ 291a Abs. 5 S. 3 SGB V). Diese elektronische Signatur muss aber nicht über die eGK selbst erfolgen. Es bestehen Erwägungen, die für Arbeitnehmer vorgesehene digitale Signaturkarte (**JobCard**) mit der eGK zu kombinieren, so dass diese auch für elektronische Erklärungen im Bereich der gesetzlichen Krankenversicherung genutzt wird. Gegen derartige Planungen bestehen datenschutzrechtliche Bedenken, da durch eine bereichsübergreifende Nutzung eines bestimmten elektronischen Signaturverfahrens dieses rollenunabhängig zur Verknüpfung von zweckgebundenen Daten genutzt werden könnte.

Daten der Ausweisfunktion dürfen von den jeweiligen Leistungserbringern gelesen, d.h. erhoben werden. Eine **Speicherung dieser Daten** ist dagegen nur im Rahmen der Erforderlichkeit zulässig. So ist das Speichern von Unterschrift und Lichtbild generell nicht für die weitere Aufgabenerfüllung erforderlich. Deren Speicherung bei den Leistungserbringern ist daher unzulässig.

VII. Elektronisches Rezept

Mit dem elektronischen Rezept (**E-Rezept**) sollen bei der Rezepterstellung, -einlösung und -abrechnung Medienbrüche vermieden werden. Hier liegt angesichts von jährlich ca. 700 Mio. Rezepten ein sehr großes Einsparpotenzial. Es ist bisher nicht geklärt, ob künftig die Speicherung der Rezeptdaten karten- oder servergestützt (über ein Pointerverfahren) erfolgen wird.[25] Technisch wie auch datenschutzrechtlich möglich ist u.U. sogar eine alternative Nutzung oder eine Mischform beider Techniken. Für die E-Rezept-Anwendung können die Medikationsdaten nach Einlösung und Abrechnung wieder gelöscht werden.

Der verschreibende Arzt speichert über die eGK das zu verschreibende Medikament. Der Apotheker hat die Befugnis zum Auslesen der Verschreibung und zur Deaktivierung bzw. Löschung der Eintragung nach Ausgabe des Medikamentes. Die weitere Abrechnung für die Apotheke mit der Krankenkasse erfolgt über ein Apothekenrechenzentrum (§ 300 SGB V). Gemäß der aktuellen Rechtslage besteht keine Pflicht und auch keine Recht, **nach erfolgter Abrechnung** eine personenbezogene Speicherung der Verschreibungsdaten für sonstige Zwecke beizubehalten. Wegen der abschließenden gesetzlichen Regelungen im SGB V ist auch auf Grund einer ausdrücklichen schriftlichen Einwilligung des Patienten unter Benennenung eine Weiterspeicherung der Kundendaten für Werbezwecke durch die Apotheke nicht zulässig.[26] Für weitere Auswertungen muss die Apotheke zumindest den Personenbezug zum Verschreibungsdatensatz unwiderbringlich beseitigen. Das SGB V erlaubt auf Einwilligung basierende Weiterspeicherungen insbesondere für die Applikation Arzneimitteldokumentation und für die Ausstellung von Zuzahlungsbescheinigungen (s.u. VIII).

Grundsätzlich ist der Zugriff auf die über die eGK erschlossenen Daten von einer Autorisierung mit einer HPC/SMC abhängig. Für Rezeptdaten wird darüber hinausgehend vorgesehen, den Zugriff auch durch **Authentifizierung des Versicherten** selbst zu ermöglichen (z.B. mittels PIN oder biometrischen Verfahren), ohne also auf Seiten der Leistungserbringer weitere technische Vorkehrungen für den Zugriff zu verlangen. Damit sollen Rezepte auch in Ländern eingelöst werden können, in denen keine HPC/SMC im Einsatz ist.[27]

---

24 Bales/Holland in Jäckel (Fn. 10), 16.

25 Teletrust (Fn. 1), Kap. 5.2.; 18. TB BfD 1999/2000, Kap. 25.1.3; 19. TB BfD 2001/2002, Kap. 28.2.

26 19. TB BfD 2001/2002, Kap. 28.7.3; TB 2002 ULD SH, Kap. 4.8.7.

27 Gesetzesbegründung (Fn. 21), S. 327 f.

Die konkrete Ausgestaltung soll „im Einvernehmen mit dem Bundesbeauftragten für den Datenschutz erfolgen".[28]

VIII. Notfalldatenübermittlung, Arztbriefübermittlung, Arzneimitteldokumentation, vom Versicherten zur Verfügung gestellte Daten

Aus praktischen Gründen ist es sinnvoll, die **Notfalldaten** direkt auf der Karte zu speichern. Nur so kann sichergestellt werden, dass die Daten für Akutbehandlungen jederzeit auch offline zur Verfügung stehen.[29] Was alles zu den Notfalldaten zu zählen ist, ist nach medizinischen Kriterien durch die Spitzenverbände nach § 291a Abs. 7 SGB V festzulegen. Hierzu können Angaben zu chronischen Erkrankungen gehören (Diabetis, Bluter, Herzschrittmacher, Allergien, Arzneimittelunverträglichkeiten), Angaben zu Implantaten, zu Impfungen sowie bestimmte bleibende persönliche medizinische Angaben (z.B. Blutgruppe). Zu den Notfalldaten können auch die Angaben zu behandelnden Ärzten (z.B. Hausarzt) und zu im Notfall zu benachrichtigenden Personen zählen. Auf internationaler Ebene hat man sich auf einen **europäischen Notfalldatensatz** geeinigt, der auf der eGK digital gespeichert werden soll.[30]

Die **Arztbriefübermittlung** ist - anders als das E-Rezept - als freiwillige Anwendung der eGK vorgesehen. Die technische Realisierung unterscheidet sich von dem oben beschriebenen Verfahren zum E-Rezept nicht, wobei an die Stelle des Apothekers der weiter- bzw. nachbehandelnde Arzt bzw. der Hausarzt tritt. Bezieht der empfangende Arzt den Arztbrief in seine Behandlung mit ein, muss er diesen in seine Dokumentation über den Patienten nach der Ärztlichen Berufsordnung (z.B. § 10 BO ÄK SH) aufnehmen. Dies kann nach Ausdruck in konventioneller Form erfolgen oder als elektronische Speicherung.

Der Apotheker - oder auch der Arzt - kann - evtl. mit Hilfe eines Abgleichs der Rezeptdaten mit einer zentralen Medikamentendatenbank und evtl. unter Berücksichtigung von Angaben aus dem Gesundheits-/Notfalldatensatz (Allergien, Impfungen) - feststellen, ob bei dem Medikamentenmix für den Patienten Risiken bestehen oder Kontraindikationen beachtet werden müssen (Unverträglichkeiten, Wechselwirkung mit anderen Medikamenten). In der **Arzneimitteldokumentation** wird nicht nur das verabreichte Medikament (mit Pharmazentralummer) gespeichert, sondern auch die vorgesehene Form bzw. der Umfang der Verabreichung. Die Verabreichungshistorie wird mit einbezogen. Arzt und Apotheker müssen beachten, dass die elektronisch gespeicherte Einlösung eines Rezeptes nicht identisch ist mit der tatsächlichen Anwendung des Arzneimittels. Von noch größerer Bedeutung ist das Bewusstsein, dass u.U. für eine Verträglichkeitsprüfung relevante eingenommene Medikamente nicht in der Dokumentation aufgenommen sind. Der Apotheker bzw. der Arzt kann den Patienten anhand der Daten beraten.[31] Die technische Zugriffsmöglichkeit für den Apotheker muss auf die für diese Anwendung erforderlichen Daten beschränkt bleiben. Grundlage für die Beratung ist i.d.R. eine Medikamentendatenbank, die Auskunft über die Wirkstoffe, über Risiken, Neben-, Wechsel- und Nachwirkungen gibt.

Die eGK soll weiterhin dem Patienten die Möglichkeit gewähren, zusätzlich zu den konkreten o.g. Anwendungen auf freiwilliger Basis Leistungserbringern Daten zur Verfügung zu stellen. Dies können aus der Sicht des Patienten wichtige ärztliche Dokumente zur medizinischen Vorgeschichte oder auch persönliche Dokumente sein. In dem **Patientenfach** können Angaben zu Fremdsprachenkenntnissen des Versicherten, zur Organspendebereitschaft, zu Blutspenden oder zu Angehörigen, die in bestimmten Fällen zu benachrichtigen sind, aufgenommen werden. Gespeichert werden können auch Anweisungen hinsichtlich der Anwendung intensivmedizinischer und lebensverlängernder Verfahren in bestimmten Fällen (Patientenverfügungen).[32]

IX. Elektronische Patientenakte

Die elektronische Patientenakte (EPA) soll zu einem wichtigen Informationsbindeglied für die unterschiedlichen Träger der Versorgung im ambulanten, stationären und rehabilitativen Bereich werden. Sie soll den informatorischen Unterbau für die integrierte Versorgung und für Disease-Management-Programme liefern.[33] Dabei sind verschiedene **Modelle** zu unterscheiden:

---

28 Gesetzesbegründung (Fn. 21), S. 326.
29 Bales/Holland in Jäckel (Fn. 10), 17.
30 Teletrust (Fn. 1), Kap. 6.
31 TB 2003 ULD SH, Kap. 4.8.2; Bales/Holland in Jäckel (Fn. 10), 14.
32 Teletrust (Fn. 1), Kap. 6.
33 Allgemein zur EPA BfD 19. TB 2001/2002, Kap. 28.4.

1. die beim jeweils behandelnden Arzt **in elektronischer Form geführte Patientenakte**, auf die u.U. andere Leistungerbringer gezielt zugreifen können,
2. eine **elektronische Fallakte mehrerer Leistungserbringer** bzgl. eines Patienten und einer bestimmten Diagnose,
3. die zentral beim **Hausarzt** für einen Patienten geführte Akte, die auch Daten von anderen Leistungserbringern enthält,
4. eine „**elektronische Gesundheitsakte**" in der Datenhoheit des Patienten, in der sich Kopien von Patientenakten von Leistungsempfängern befinden und auf die der Patient Zugriff gewährt.

Zu 1.
Bei der **elektronisch geführten Patientenakte** ergeben sich - abgesehen von der veränderten Speicherform - gegenüber der konventionellen Aktenführung keine wesentlichen Änderungen. Die Daten können beim Leistungserbringer selbst oder in verschlüsselter Form bei einem Auftragnehmer gespeichert sein.[34] Unbegrenzten Zugriff darauf hat, evtl. unterstützt durch die HPC, ausschließlich der Leistungserbringer.[35] Denkbar ist, dass der Zugriff auf bestimmte Dokumente für weitere Leistungserbringer freigeschaltet ist. Der Zugriff der Dritten kann durch die HPC, evtl. gekoppelt durch die eGK zugelassen werden. Die eGK kann jedenfalls, solange über sie nicht ein technisch gesichertes Authentisierungsverfahren besteht, nicht als ausschließlicher Zugriffsausweis genutzt werden. Die Zugriffserlaubnis erfolgt durch den Leistungserbringer, nicht den Patienten, z.B. durch entsprechendes Freischalten.

Zu 2.
Bei der **elektronischen Fallakte** führen mehrere Leistungserbringer, die einen Patienten gemeinsam bzgl. einer bestimmten Diagnose oder eines Behandlungskomplexes behandeln, gemeinsam eine elektronische Dokumentation. Typisch hierbei ist, dass alle berechtigten Leistungserbringer grds. auf sämtliche Daten zugreifen können. Hierzu muss der Patient seine ausdrückliche informierte Einwilligung erteilt haben. Möglich ist aber auch ein vom Patienten bestimmtes differenziertes Zugriffsregime. Die inhaltliche Verantwortlichkeit für einen bestimmten Datensatz übernimmt der eingebende Leistungserbringer, z.B. durch elektronisches Signieren des Dokuments. Datenschutzrechtlich handelt es sich bei der Fallakte um eine gemeinsame Datei (z.B. § 6 Abs. 2 BDSG, § 8 Abs. 1 LDSG SH). Die tatsächliche Datenverarbeitung erfolgt entweder bei einem der Leistungserbringer oder in Form der verschlüsselten Auftragsdatenverarbeitung auf dem Server eines externen Dienstleisters. Ein Anwendungsfall kann die integrierte Versorgung nach den §§ 140a ff SGB V sein.[36] Als weiterer Anwendungsfall kommt die einrichtungsübergreifende Fallakte für die Behandlung chronisch Kranker im Rahmen des Disease Managements in Betracht. Die Regelungen zu Disease Management Programmen (§§ 137f f. SGB V) sind bisher noch nicht mit den Möglichkeiten der eGK synchronisiert. Ähnlich wie bei der elektronischen Patientenakte (s.o. 1.) erfüllt die eGK derzeit hierfür keine zentrale, sondern allenfalls eine unterstützende Funktion.

Zu 3.
Die **elektronische Hausarztakte** wird grds. im Rahmen des Hausarztmodells geführt (§§ 65a, 73 Abs. 1b SGB V). Der Hausarzt ist in diesen Fällen allein verantwortliche Stelle i.S.d. Datenschutzrechts. Der Patient verpflichtet sich, sämtliche medizinischen Leistungen nur vermittelt über den Hausarzt in Anspruch zu nehmen mit der Folge, dass sämtliche Behandlungsdaten bei diesem zusammenlaufen und von diesem beauskunftet werden können. Der Spezialist, an den der Patient überwiesen wurde, stellt dem Hausarzt seinen Arztbrief elektronisch zur Verfügung, der diesen in seine Hausarztakte einstellt.[37] Ausschließlich verfügungsbefugt über die Dokumentation ist der Hausarzt. Der Spezialist führt seine eigene Akte.[38] Auch hier hat die eGK allenfalls eine unterstützende Funktion.

Zu 4.
Die Krankenkassen können ihren Versicherten **persönliche Gesundheitsakten** finanzieren. Diese sollen eine Dokumentation unabhängig von derjenigen ihrer Behandler aufbauen und führen, indem sie Kopien wichtiger medizinischer Dokumente bei sich selbst speichern und die sie, z.B. bei Wohnortwechsel, anderen Behandlern zur Verfügung stellen können. Mit dieser Akte sollen nicht auf verschiedenen Rechnern liegende Originaldokumente zusammengeführt werden, sondern diese sollen als Kopie sofort gemeinsam unter der Ägide

---

34 Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig (Autorenteam), Datenschutz und Telemedizin, 2002, S. 8, 15; abzurufen unter www.bfd.bund.de.

35 Autorenteam (Fn. 34), 17 f.

36 Gerhardt/Kaeding (Fn. 4), S. 208 f.

37 Gerhardt/Kaeding (Fn. 4), S. 207 f.

38 Autorenteam (Fn. 34), S. 17 f.

des Patienten verwaltet werden. Hierfür müssen die Versicherten über eine mit einer qualifizierten elektronischen Signatur versehene Karte verfügen.[39] Im Rahmen von Erprobungsverfahren ist auch denkbar, dass die eGK gekoppelt mit einem weiteren individuellen Authentisierungsmittel (z.B. PIN) vorläufig genügt. Der Zugriff zu der persönlichen Gesundheitsakte durch einen Arzt kann nur in Kombination von eGK und HPC zugelassen werden. Bei der persönlichen Gesundheitsakte kann nicht mehr der Arzt als verfügungsbefugt und damit als verarbeitende Stelle angesehen werden. Hier liegt die Verfügungsbefugnis ausschließlich beim Patienten. Dieser kann aber nur bestimmen, ob ein authentisches ärztliches Dokument aufgenommen wird oder nicht, bzw. wer auf welche Dokumente Zugriff erhält. Eigenständige inhaltliche Änderungen an den Dokumenten kann der Patient nicht vornehmen. Diese Bestimmungsmöglichkeit des Patienten kann zur Unvollständigkeit der Dokumentation führen.[40]

X. Versichertenauskunft

Eine konkrete Anwendung der eGK besteht darin, den **Versicherten Auskunft** zu geben über die in Anspruch genommenen Leistungen und deren vorläufige Kosten für den Versicherten (§ 291a Abs. 3 Nr. 6 i.V.m. § 305 Abs. 2 SGB V). Diese Anwendung soll zur Transparenz der finanziellen Vorgänge für den Karteninhaber beitragen.

Da sich der **Zuzahlungsstatus** (§ 291 Abs. 2 S. 1 SGB V), d.h. die Berechtigung zur Zuzahlungsbefreiung eines Versicherten, ändern kann, können Angaben hierzu auf der Karte aktualisiert werden. Die Aktualisierung ist von einer Entscheidung der Krankenkasse abhängig. Das Update auf der Karte soll online, u.U. bei einem Leistungserbringer, vorgenommen werden können.

Von der Versichertenauskunft gemäß § 305 Abs. 2 SGB V zu unterscheiden ist der allgemeine datenschutzrechtliche **Auskunftsanspruch** des Versicherten. Danach ist dem Betroffenen Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, den Zweck der Speicherung, Herkunft und Empfänger. Da die Krankenkasse nicht die einzige Daten verarbeitende Stelle bei eGK-Anwendungen ist, besteht auch ein Auskunftsanspruch gegenüber den diese Karte nutzenden Leistungserbringern (§ 83 SGB X, § 34 BDSG bzw. Landesrecht, z.B. § 27 LDSG SH). Die eGK soll einen „Paradigmenwechsel" bzgl. der Rechte des Patienten mit sich bringen. Dieser soll zum „Herr seiner Daten" werden. Über die eGK soll das heute schon bestehende Recht, Einsicht in die Behandlungsakte zu nehmen, erheblich erleichtert werden.[41] Adressat des Anspruchs ist jeweils die verarbeitende Stelle. Vom Auskunftsanspruch erfasst sind nicht nur die auf der Karte gespeicherten Daten, sondern auch die über die eGK erschlossenen, auf Servern gespeicherten Daten. Um zu vermeiden, dass der Versicherte sich an eine Vielzahl von Stellen wenden muss, empfiehlt es sich, dass die Krankenkasse als Herausgeberin der eGK auch für die sonstigen beteiligten Stellen die Auskunftserteilung im Auftrag übernimmt.[42]

Technisch kann die Auskunftserteilung in der Form erfolgen, dass die Krankenkasse **Geräte zur Verfügung** stellt, die von den Versicherten ohne unzumutbare Anreisewege erreicht und ohne Barrieren genutzt werden können.[43] Es ist aber technisch zu verhindern, dass die Krankenkasse über die Betroffenenauskünfte Daten in Erfahrung bringt, auf die sie ansonsten keine Zugriff und keinen Anspruch hat. Hierfür ist es erforderlich, dass sich der Versicherte mit Hilfe der Karte und durch Eingabe einer PIN oder auf andere Weise eindeutig identifiziert (s.o.). Die Daten müssen separat nach verantwortlicher Stelle gespeichert bleiben.

Eine patientenfreundliche technische Umsetzung des Auskunftsanspruchs kann auch darin bestehen, dass eine Auskunft an die Versicherten über die **Endgeräte der Leistungserbringer** ermöglicht wird. Um zu vermeiden, dass der Leistungserbringer im Rahmen der Auskunftserteilung von Daten Kenntnis erlangt, zu denen er sonst keinen Zugriff hat, muss im Fall einer derart realisierten Selbstauskunft sichergestellt werden, dass keine Übernahme der Fremddaten in den eigenen Speicher erfolgt.

Vom Inhaber der eGK darf nicht gefordert werden, dass er anderen als den im Gesetz Genannten Zugriff auf die Daten gewährt. Eine entsprechende Verpflichtung des Versicherten ist unzulässig. Dieser darf weder bevorzugt noch benachteiligt werden, weil er den Zugriff auf die Daten zugelassen oder erlaubt hat (§ 291a Abs. 8 SGB V). Mit der Regelung soll verhindert werden, dass die Daten der eGK für andere Zwecke genutzt werden als die der Patientenversorgung und Abrechnung. Insbesondere soll ausgeschlossen werden, dass **Selbstauskünfte** von

---

39 Bales/Holland in Jäckel (Fn. 10), 17 f.
40 Gerhardt/Kaeding (Fn. 4), S. 210.
41 Bales (Fn. 3).
42 Weichert (Fn. 15), Rz. 51.
43 Bizer in Simitis (Fn. 14), Rz. 57 ff.

Arbeitgebern, privaten Versicherungen oder auch von öffentlichen Stellen fachfremd genutzt werden. Das in Absatz 8 enthaltene Verbot bezieht sich nicht nur auf die Datenverarbeitung mit der Karte selbst, sondern auch auf die Daten, die z.B. über eine Auskunft an den Betroffenen erlangt wurden.[44]

XI. Anforderungen an die Unterrichtung des Versicherten

Die Herstellung einer **ausreichenden Transparenz** für die Versicherten wie auch für die informationstechnisch i.d.R. wenig geschulten Leistungserbringer ist eine der größten Herausforderungen bei der Realisierung der eGK. Nach § 291a Abs. 3 S. 2 SGB V sind die Versicherten spätestens bei der Versendung der Karte „umfassend und in allgemein verständlicher Form über deren Funktionsweise, einschließlich der Art der auf ihr oder durch sie zu erhebenden, zu verarbeitenden oder zu nutzenden personenbezogenen Daten zu informieren". Die Unterrichtung muss bzgl. jeder konkreten Anwendung Angaben über die verarbeiteten Daten und die beteiligten Stellen bzw. Personen enthalten.

Die Unterrichtung hat **in schriftlicher Form** z.B. über ein Hinweisblatt oder über eine Broschüre zu erfolgen. Eine mündliche Information ist schon wegen der damit verbundenen Flüchtigkeit der Angaben nicht ausreichend. Eine Unterrichtung ausschließlich über elektronische Medien ist ebenso nicht ausreichend, da deren Nutzung durch sämtliche Versicherten derzeit nicht gewährleistet ist.[45] Auch die Komplexität der Datenverarbeitung bei der eGK gebietet eine schriftliche Unterrichtung.[46] Eine ergänzende, u.U. vertiefende Darstellung z.B. im Internet ist nicht nur förderlich, sondern dringend zu empfehlen. Die Krankenkassen sind gut beraten, wenn sie für ihre Versicherten ein differenziertes zusätzliches Unterrichtungsangebot bereit halten, z.B. durch Berater oder Informationsveranstaltungen.

Die Unterrichtung umfasst **sämtliche Formen der Nutzung**, also sowohl die obligatorischen (Abs. 2) wie auch die freiwilligen Anwendungen (Abs. 3). Während bei der Formulierung der Einwilligungen nicht nur auf Verständlichkeit, sondern auch auf Kürze Wert gelegt werden muss (s.u. XII), kann die Unterrichtung ins Detail gehen. Dabei darf aber der Verständnishorizont eines durchschnittlichen Versicherten nicht überfordert werden. Bei der Darstellung ist eine korrekte Beschreibung geboten. Abstriche vom Wahrheitsprinzip dürfen auch nicht im Interesse der Verständlichkeit erfolgen. Dies ist insbesondere relevant bei der Darstellung der Verantwortlichkeit, der Beschreibung, welche Daten auf der eGK und welche über diese auf regionalen Servern verarbeitet werden, der Verschlüsselungsmethoden und bei der Differenzierung zwischen Pseudonymisierung und Anonymisierung. Zu den Aufgaben der Krankenkassen gehört es auch, die Betroffenen über ihre Betroffenenrechte und über den Umgang mit der Karte zu unterrichten (§ 6c Abs. 1 BDSG).[47]

Für die Akzeptanz und im Interesse einer störungsfreien Anwendung der eGK-Datenverarbeitung ist es von zentraler Bedeutung, dass auch die **Leistungserbringer** über die Funktionalitäten und Abläufe informiert werden. Unterstützend sind hier die Software-Anbieter einzubeziehen. Über Fortbildungsveranstaltungen und elektronische Hilfen sind die Leistungsanbieter sowohl bei der Einführung wie auch im laufenden Betrieb über sämtliche relevanten Umstände zu informieren.

XII. Anforderungen an die Einwilligung des Versicherten

Für die Datenverarbeitung nach § 291a Abs. 3 S. SGB V bedarf es der Einwilligung des Versicherten. Erfolgt die Erprobung der eGK im Rahmen eines Modellvorhabens, so verlangt auch § 63 Abs. 3a SGB V die Einwilligung der betroffenen Versicherten. Welche Einwilligungsvoraussetzungen bestehen, richtet sich nach dem **jeweiligen Recht**, das für die verarbeitende Stelle gilt. Für Sozialversicherungsträger (inbes. Krankenkassen) gilt § 67b Abs. 2 SGB X, für private Stellen § 4a BDSG, für öffentliche Stellen in den Ländern das jeweilige Landesdatenschutzrecht (z.B. § 12 LDSG SH), soweit das SGB V nicht eigene Regelungen enthält. Da die datenschutzrechtlichen Einwilligungsnormen inhaltlich weitgehend übereinstimmen, kann eine gemeinsame Darstellung erfolgen.

Für eine wirksame Einwilligung in die Datenverarbeitung über die eGK bedarf es der **Schriftform** oder eines adäquaten elektronischen Ersatzes. Jede andere Form der Einwilligung wäre nicht angemessen (vgl. § 4a Abs. 1 S. 3 BDSG). Allein die Hingabe der Karte genügt bei einwilligungsbedürftiger Datenverarbeitung nicht den

---

44 Zum Verbot der Vorlage von Selbstauskünften allgemein Weichert CR 1995, 361 ff.

45 Bizer in Simitis (Fn. 14), § 6c Rz. 36.

46 Weichert (Fn. 15), Rz. 48.

47 Ausführlich Bizer in Simitis (Fn. 14), § 6c Rz. 42 ff.

Formerfordernissen.[48] Wegen der Sensibilität der Daten und der Komplexität der Verarbeitung genügt auch nicht die einfache Hervorhebung im Rahmen weiterer schriftlicher Erklärungen.[49] Vielmehr bedarf es einer gesonderten Erklärung, am besten mit einer entsprechenden Unterschrift. Streichlösungen entsprechen den Anforderungen nicht. Werden eine Vielzahl von differenzierten Erklärungen abgegeben (z.B. im Hinblick auf unterschiedliche Anwendungen nach § 291a Abs. 3 SGB V), so empfiehlt sich eine Ankreuzlösung. Da die Erklärung „ohne jeden Zweifel" abgegeben sein muss (vgl. Art. 7 lit. a) Europäische Datenschutzrichtlinie - EU-DSRL), gibt es bzgl. der Gestaltung keine Alternative zu einem Ankreuzen „ja/nein". Es empfiehlt sich, bundesweit bzw. zunächst projektweit standardisierte einheitliche Formulare zu verwenden.

In der Regel erfolgt bei der Datenverarbeitung über die eGK eine **zweistufige Einwilligung**: Zunächst muss sich der Versicherte grds. für die medizinische Nutzung der Gesundheitskarte entscheiden, d.h. er legt fest, welche Anwendungen in Bezug auf seine Person wie zugelassen werden und welche Daten über die Karte gespeichert, d.h. erfasst und gelöscht werden. Einer eigenständigen Entscheidung des Versicherten unterliegt es in einer zweiten Stufe, ob er Daten zur Speicherung und die gespeicherten Daten zur Einsicht freigibt und nicht.[50]

Während bzgl. der ersten Stufe der Einwilligung hohe Anforderungen im Hinblick an Form und Inhalt gestellt werden müssen (s.u.), können im Interesse der Praktikablität bzgl. der **konkreten Abfrage** geringere Anforderungen ausreichend sein, soweit die zuvor erfolgten Festlegungen bestimmt genug waren. Bei der konkreten Datennutzung erfolgt ein Zusammenspiel von eGK, HPC und Zustimmungen von Leistungserbringer und Patienten.[51] Um bzgl. der Zustimmung des Patienten eine ausreichende Transparenz zu erreichen, muss der Vorgang auf einem Bildschirm für den Patienten nachvollziehbar gemacht werden. Einwilligungen bzgl. konkreter Datenverarbeitungen müssen in jedem Fall - auch wenn keine ausdrückliche schriftliche Erklärung erfolgt - revisionsfest dokumentiert werden (s.u. XIV).

Inhaltlich müssen wirksame Einwilligungen zur Verarbeitung medizinischer Daten über die eGK höchsten Anforderungen genügen. Wegen der Komplexität und Differenziertheit der notwendigen Erklärungen einerseits und der teilweise nur begrenzten Verständnisfähigkeit bei den Versicherten sind die Erklärungstexte so eindeutig und zugleich so knapp wie möglich zu formulieren. Aus den Texten müssen der verfolgte Zweck, die Art der verarbeiteten Daten sowie die beteiligten Personen bzw. Stellen **so bestimmt wie möglich** gefasst sein. Die Einwilligungserklärung muss aus sich selbst heraus verständlich sein. Der Verweis auf ein nicht direkt damit verbundenes Hinweisblatt o.Ä. genügt nicht.

Wegen der nötigen Standardisierung der eGK kann auf individuelle Wünsche des Versicherten nur in dem technisch zuvor festgelegten Rahmen eingegangen werden. Die Einwilligung kann auf **einzelne Anwendungen** der eGK beschränkt werden (§ 291a Abs. 3 S. 3 2. HS SGB V). D.h. Minimum bei der Differenziertheit ist die gesonderte Erklärung bzgl. der Zwecke Notfallversorgung, elektronischer Arztbrief, Arzneimitteldokumentation, elektronische Patientenakte, zusätzliche Versichertenangaben, Leistungsauskunft. Soweit darüber hinausgehende Zwecke verfolgt werden (s.u.), müssen auch diese ausdrücklich benannt werden. Dabei sind die Zwecke neutral zu beschreiben; beschönigende bzw. manipulative Beschreibungen (z.B. „damit wir Sie noch besser behandeln können") führen wegen ihrer Unbestimmtheit zur Unwirksamkeit der jeweiligen Erklärung.

Aus der Differenzierung nach Anwendungen ergeben sich auch Differenzierungen in Bezug auf die **Art der Daten**. Damit allein wird aber der Wahlfreiheit der Versicherten nicht genügt. Grds. muss es diesen möglich sein, individuelle Besonderheiten berücksichtigt zu bekommen. Dies betrifft zunächst generell die Frage, ob ein Datum auf der Karte gespeichert (bzw. über die Karte erschlossen) wird. Es steht dem Patienten frei zu entscheiden, ob z.B. Bagatellbehandlungen mit aufgenommen werden oder ob besonders sensible Medikationen oder Behandlungen mit gespeichert werden oder nicht. D.h. zusätzlich zu der allgemein erteilten schriftlichen Einwilligung muss der versicherte Patient vom Arzt mündlich gefragt werden, ob eine bestimmte Behandlung, Diagnose, Medikation usw. aufgenommen werden soll. Dem Patienten steht es also nicht nur zu, nachträglich bestimmte Daten löschen zu lassen (§ 291a Abs. 6 S. 1 SGB V), er muss schon bei der erstmaligen Speicherung konkret gefragt und in die Entscheidung über die Speicherung einbezogen werden.

Eine differenzierte Wahlmöglichkeit muss dem Patienten auch im Hinblick auf **Behandlungszusammenhänge** gegeben werden: Er darf nicht faktisch gezwungen sein, medizinische Daten aus einem anderen Zusammenhang

---

48 Autorenteam (Fn. 34), S. 6.
49 Weichert (Fn. 15), Rz. 36.
50 Teletrust (Fn. 1) Kap. 2.
51 Teletrust (Fn. 1), Kap. 4.

offenlegen zu müssen. So ist z.B. einer Frau die Möglichkeit zu geben, im Rahmen einer Allergiebehandlung den Zugriff auf gynäkologische oder chirurgische Befunddaten auszublenden.

Die Patientenentscheidung ist angemessen zu **protokollieren**, z.B. durch das Ankreuzen eines entsprechenden Feldes in der ärztlichen Patientendokumentation. Die Konsequenz dieser Wahlfreiheit muss den Leistungserbringern, insbesondere den Ärzten und Apothekern bewusst sein: Zwar besteht die Gewähr der Richtigkeit der auf der Karte oder über die Karte gespeicherten Informationen. Keine Gewähr kann es aber geben bzgl. der Vollständigkeit der Daten.[52] Der Leistungserbringer kommt also auch bei Nutzung einer Anwendung nicht umhin, den Patienten ergänzend mündlich zu fragen, ob evtl. relevante weitere Daten nicht gespeichert sind.

Auch bzgl. der **nutzungsberechtigten Leistungserbringer** müssen die Einwilligungen hinreichend bestimmt sein. Es muss z.B. den Versicherten möglich sein, bestimmte Ärzte von der freiwilligen Nutzung auszuschließen bzw. diese einzubeziehen. Die Vorlage der eGK durch den Versicherten genügt nicht für den Nachweis der Nutzungsberechtigung für den Leistungserbringer. Zum einen würde dadurch nicht der Differenzierungsmöglichkeit nach Anwendungen Rechnung getragen. Außerdem sind auch Datennutzungen möglich, ohne dass der Versicherte persönlich (mit der Karte) beim Leistungserbringer vorspricht. In der Regel wird man davon ausgehen können, dass ein Versicherter sämtliche Ärzte bzw. Leistungserbringer eines bestimmten örtlichen Bereiches zur Nutzung zulassen will, sofern er bei diesen in Behandlung ist bzw. von diesen Leistungen in Anspruch nimmt. Daher dürfte eine generelle Freischaltung der Regelfall sein, was dann auch ausdrücklich erklärt werden muss. Um aber der Wahlfreiheit der Patienten zu genügen, müssen auch Ein- und Ausschlussmöglichkeiten vorgesehen werden. Dies lässt sich dadurch realisieren, dass den Versicherten die Möglichkeit eingeräumt wird, bestimmte Leistungserbringer ausdrücklich auszuschließen (Opt-Out) bzw. ausschließlich oder ergänzend zu einer Regelliste einzubeziehen (Opt-In). Um dies praktikabel umzusetzen, sollte dem Versicherten eine entsprechende Liste aller an ein regionales Netz angeschlossenen Leistungserbringer zur Verfügung gestellt werden.

Gemäß § 291a Abs. 3 S. 3 SGB V ist die Einwilligung bei erster Verwendung der Karte vom Leistungserbringer auf der Karte zu **dokumentieren**. Entgegen dem Wortlaut der Regelung muss die Dokumentation jedoch nicht direkt auf der Karte erfolgen. Möglich dürfte wohl auch ein technisches Verfahren sein, bei dem die Dokumentation auf einem Server erfolgt und bei der Kartennutzung die entsprechende Nutzungsberechtigung elektronisch festgestellt wird. Mit der in der Regelung vorgesehenen Dokumentation wird lediglich die elektronische Umsetzung des Berechtigungsprofils bezweckt. Unabhängig davon muss eine Dokumentation bei dem jeweiligen Leistungserbringer erfolgen, die z.B. bei Ärzten den standesrechtlichen Anforderungen genügt.[53] Die elektronische Dokumentation des Berechtigungsprofils muss der externen Dokumentation entsprechen.

Nur die **freiwillig** erteilte Einwilligung entfaltet datenschutzrechtliche Wirkung. Davon kann keine Rede sein, wenn der Nutzung der eGK unter Zwang zugestimmt wurde. Angesichts des faktischen Abhängigkeitsverhältnisses des Patienten von den Leistungserbringern sind bzgl. der Freiwilligkeit hohe Anforderungen zu stellen. Eine Voraussetzung ist, dass durch die Erteilung und die Verweigerung bzw. den Widerruf dem Versicherten keine faktischen Vor- oder Nachteile entstehen dürfen, die über das hinaus gehen, was mit der Datenverarbeitung selbst ermöglicht wird (vgl. § 291a Abs. 8 S. 2 SGB V). In der Praxis dürfte die Sicherstellung der Freiwilligkeit nicht immer einfach sein, da für die Leistungserbringer Einwilligungen u.U. massive Vorteile bringen, z.B. in Bezug auf die verfügbare Datenbasis oder bzgl. der Vermeidung von kostenaufwändigen Medienbrüchen bei der Dokumentation. Um die Gefahr einer manipulativen Aufklärung durch den Leistungserbringer zu reduzieren, ist es daher geboten, die Information über die Freiwilligkeit und über das Nachteilsverbot dem Versicherten ausnahmslos schriftlich zukommen zu lassen. Die Beschränkung einer solchen Information auf ein entsprechendes Verlangen des Versicherten (vgl. § 4a Abs. 1 S. 2 BDSG) genügt den Anforderungen an die Freiwilligkeit hier nicht.[54]

Die Einwilligung ist jederzeit **widerruflich** (§ 291a Abs. 3 S. 3 2. HS SGB V). Der Widerruf kann sich auf einzelne Anwendungen beziehen, die zuvor über eine Einwilligungserklärung konsentiert wurden. Bzgl. der Form gibt es keine Vorgaben; d.h. die schriftlich erteilte Einwilligung kann auch mündlich widerrufen werden. Da jedoch der schriftlichen Erklärung ein hoher Beweiswert zukommt, ist es im Interesse aller Beteiligten dringend geboten, auch den Widerruf schriftlich vorzunehmen bzw. zumindest zu dokumentieren. Bzgl. des Widerrufs bestehen die gleichen Differenzierungsmöglichkeiten wie bei der Erteilung der Einwilligung; der Widerruf kann demnach umfassend als auch partiell erfolgen. Der Widerruf macht die bisherige Datenverarbeitung nicht

---

52 Bales/Holland in Jäckel (Fn. 10), 16.

53 Bales/Holland in Jäckel (Fn. 10), 16.

54 Weichert (Fn. 15), Rz. 39.

unzulässig. Er entfaltet lediglich bzgl. der künftigen weiteren Datenverarbeitung Wirkung, und zwar vom Zeitpunkt der Erklärung an. Direkter Adressat des Widerrufs sollte die Person bzw. Stelle sein, gegenüber der auch die Einwilligung erklärt wurde. Um sie aber mit Rechtswirkung zu versehen, muss sie der jeweiligen Stelle, die zur Datenverarbeitung nicht mehr berechtigt sein soll, zur Kenntnis gelangen. Daher muss organisatorisch geregelt und sichergestellt sein, dass ein Widerruf bzgl. sämtlicher betroffenen Adressaten vom Empfänger der Widerrufserklärung weitergeleitet wird. Alternativ kommt auch der Widerruf gegenüber der nicht mehr berechtigten Stelle in Betracht. Diese muss dann gewährleisten, dass der Widerruf auch dem Empfänger der ursprünglichen Einwilligungserklärung zur Kenntnis gelangt.

Die einwilligungsbasierte Datenverarbeitung mit Hilfe der eGK in § 291a Abs. 3 SGB V bezieht sich zunächst auf die dort aufgeführten Anwendungen (Notfallversorgung, elektronischer Arztbrief, Arzneimitteldokumentation, elektronische Patientenakte, freiwillige Angaben, Versichertenauskunft). Es stellt sich die Frage, ob per Einwilligung auch **darüber hinausgehende Zwecke** verfolgt werden dürfen. Solche Zwecke können z.B. im Marketing durch die Leistungserbringer liegen. Insofern besteht ein sehr großes Interesse z.B. bei Apotheken. Für eine einwilligungsbegründete Öffnung der Zwecke spricht Nr. 5 der Regelung, die bzgl. des Datenumfangs eine Wahlklausel für den Versicherten enthält, sowie der Umstand, dass die Aufzählung der Anwendungen nach dem Gesetzeswortlaut nicht abschließend formuliert wurde („insbesondere"). Auf der Karte können aber keine beliebigen zusätzlichen Applikationen aufgenommen werden. Sie müssen vielmehr der medizinischen Versorgung, d.h. der „Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz der Behandlung" (§ 291a Abs. 1 SGB V) dienen. Reine Werbezwecke dürfen z.B. mit der eGK nicht verfolgt werden.

XIII. Authentisierung von Leistungserbringern - Health Professional Card

Der Zugriff auf die eGK muss so organisiert sein, dass nur berechtigte Stellen die technische Möglichkeit des Lesens und des Schreibens haben (§ 291a Abs. 5 S. 3 SGB V). Dies darf teilweise nur über den **elektronischen Heilberufsausweis**, die sog. Health Professional Card (HPC) realisiert werden. Die HPC soll als optischer Sichtausweis wie auch als elektronische Karte als offizieller Arzt- bzw. Berufsausweis ausgegeben werden. Die Spezifikation für die HPC-D (Ärzte) wurde im Januar 2000 gemeinsam von der Kassenärztlichen Bundesvereinigung (KBV) und der Bundesärztekammer (BÄK) beschlossen und für Pilotprojekte freigegeben. Mit einer HPC wird außerdem der Zweck verfolgt, medizinische elektronische Dokumente sowohl im Verfügungsbereich des Leistungserbringers, vor allem aber auch außerhalb dieses Bereichs zuverlässig zu verschlüsseln und zu signieren. Während die eGK im SGB V näher geregelt ist, finden sich dort keine näheren Festlegungen zur HPC. Die Ausgabe von Arztausweisen und sonstigen Ausweisen für Angehörige von Heilberufen richtet sich nach Landesrecht.[55]

Bei der Schaffung der Ausweise kommt den **Kammern** als berufliche Standesorganisationen eine wichtige Rolle zu. Bei der Karte handelt es sich um eine Karte zum elektronischen Signieren. Das Signaturgesetz findet Anwendung. Denkbar ist, dass Kammern, u.U. auch im Auftrag anderer Kammern, als Zertifizierungsdiensteanbieter (Trustcenter) die HPC herausgeben. Es ist davon auszugehen, dass durch die Einführung einer bundesweit einsetzbaren HPC eine bundesweit einheitlich aufgebaute Arztnummer etabliert wird. Noch unklar ist, wer für die Ausgabe der HPC für Angehörige von Heilberufen verantwortlich sein soll, für die es keine Kammern gibt (z.B. Hebammen, Pflegepersonal).

Nach dem derzeitigen Stand soll die HPC **drei Verschlüsselungsfunktionen** als elektronischer Arztausweis erfüllen. Ein erstes Schlüsselpaar dient der sicheren Anmeldung gegenüber einem beliebigen Rechnersystem mittels assymmetrischem Verfahren. Ein zweites Schlüsselpaar realisiert eine wirksame Transportverschlüsselung beim Versand von Gesundheitsdaten. Ein drittes Schlüsselpaar dient als signaturgesetzkonforme elektronische Unterschrift. Dieser Unterschrift können ein oder mehrere sog. „Attributszertifikate" beigefügt werden.[56]

Regelmäßig erfolgt die Erkennung der Berechtigung (Authentisierung) über die Kartennutzung und zusätzlich die Eingabe einer **Persönlichen Identifikationsnummer** (PIN). Möglich wäre auch eine Authentisierung mit Hilfe von biometrischen Verfahren. Die Rechteverwaltung der HPCs erfolgt i.d.R. über ein Trustcenter.

Während die Datennutzung über eine HPC einer bestimmten Person erlaubt wird, kann über Karte die Datennutzung auch einer Institution zugestanden werden. Dem dienen elektronische Insitutionsausweise (**Secure**

---

55 BReg., BT-Drs. 15/2810 (Fn. 11), S. 5 f.

56 Teletrust (Fn. 1), Anhang A; zur Entwicklung der Spezifikation für den HPC vgl. BReg., BT-Drs. 15/2810 (Fn. 11), Fragen 9-13.

Module Card - SMC). Diese Karten sind delegationsfähig und übertragbar. Sie ermöglichen Mitarbeitern einer Einrichtung im Rahmen einer definierten Rolle (z.B. Personal einer bestimmten Krankenhausstation, einer bestimmten Apotheke, § 3 Apothekenbetriebsordnung) Daten zu verarbeiten (vgl. § 291a Abs. 5 S. 4 SGB V). Die SMC kann u.U. auch bei sonstigen im SGB V vorgesehenen Leistungserbringern oder sonstigen berechtigten Personen (z.B. Rettungsassisten bzgl. Notfalldaten) eingesetzt werden.[57]

XIV. Technisch-organisatorische Rahmenbedingungen

Die eGK muss, um wirksam werden zu können, in eine umfassende und flächendeckende Telematikinfrastruktur eingebettet sein, die den datenschutzrechtlichen Anforderungen in Bezug auf **Verfügbarkeit, Integrität und Vertraulichkeit** entspricht. Die rechtlichen Anforderungen an die technisch-organisatorischen Maßnahmen sind, jeweils bezogen auf die verantwortlichen Stellen, in den § 78a SGB X (incl. Anlage), in § 9 BDSG (incl. Anlage) oder im Landesrecht (z.B. §§ 5 f. LDSG SH) geregelt.[58]

Der Gesetzgeber wollte offensichtlich lediglich die Nutzung der aktuellen Technologie von Karten erlauben, auf denen optisch lesbar Foto und Unterschrift untergebracht werden können. Nicht auszuschließen ist, dass künftig **andere Medien** (z.B. USB-Sticks, CDs) mit vergleichbaren Funktionalitäten zum Einsatz gebracht werden.

Zu den **technischen Sicherungen** gehört zunächst, dass lediglich die optisch auf der eGK lesbaren Daten auch problemlos elektronisch gelesen werden können. Das Betriebssystem der eGK muss hinsichtlich der Datensicherheit vor dessen Zulassung zertifiziert werden.[59] Für den Zugriff auf die freiwilligen Anwendungen (nach § 291a Abs. 3 SGB V) und auf die Anwendung E-Rezept bedarf es der zusätzlichen Authentisierung durch eine HPC (§ 291a Abs. 5 SGB V). Die Autorisierung durch den Patienten selbst nach § 291 Abs. 5 S. 2 SGB V muss technisch, z.B. durch eine PIN, abgesichert werden. Die Autorisierung durch den Patienten kann das Fehlen einer HPC bzw. SMC ersetzen (§ 291a Abs. 5 S. 5 SGB V).

Auf der Karte sind zumindest die letzten 50 Zugriffe zu protokollieren (§ 291a Abs. 6 S. 2 SGB V). In den Hintergrundsystemen der jeweiligen Leistungserbringer und sonstigen Nutzenden sind ebenso **Protokollierungen** über die Datenkommunikationen vorzunehmen. Die Protokolldaten sind verschlüsselt abzulegen, so dass ein unberechtigter Zugriff ausgeschlossen wird.

Die Nutzung der Protokolldaten ist ausschließlich für **Zwecke der Datenschutzkontrolle** zulässig (§ 291a Abs. 6 S. 3 SGB V). Zugriff dürfen nur diejenigen Instanzen nehmen können, die mit datenschutzrechtlichen Kontrollaufgaben betraut sind, also u.U. Vorgesetzte und betriebliche/behördliche Datenschutzbeauftragte sowie in jedem Fall die zuständigen Datenschutzkontrollbehörden. Für die stelleninterne Datenschutzkontrolle dürfen nur die eigenen Daten zugänglich sein. Bzgl. des Zugriffs auf Protokolldaten durch Datenschutzkontrollbehörden muss eine vollständige Lesemöglichkeit eröffnet werden. Zu diesem Zweck mag es sinnvoll sein, diesen Behörden Superlese-Befugnisse in Bezug auf die Kartendaten zu geben. Eine Differenzierung nach Kontrollzuständigkeiten (BfD, LfD, Aufsichtsbehörde nach § 38 BDSG) ist nicht erforderlich und auch nicht wünschenswert, da für eine Datenschutzkontrolle u.U. Datenkenntnisse aus Verarbeitungsvorgängen erforderlich sind, die nicht direkt der eigenen Kontrollzuständigkeit unterliegen.

Geregelt ist, dass bzgl. der freiwilligen Anwendungen die Löschung durch den Versicherten initiiert werden kann (§ 291a Abs. 6 S. 1 SGB V). Diese **gewillkürten Löschungen** können problemlos über die jeweils verantwortlichen Stellen erfolgen. Im Interesse der Patientenfreundlichkeit wäre es, wenn bei den Leistungserbringern und bei den Krankenkassen auch Löschungen von Daten vorgenommen werden können, für deren Speicherung andere Stellen verantwortlich sind.

Klärungsbedürftig bleibt der quantitativ voraussichtlich größere Anteil der **nicht-gewillkürten Löschungsvorgänge**. Auch im Kontext der eGK dürfen Datenspeicherungen nicht länger erfolgen, als dies für den jeweiligen Zweck erforderlich ist (vgl. § 84 Abs. 2 S. 2 SGB X, §§ 20 Abs. 2 Nr. 2, 35 Abs. 2 Nr. 3 BDSG). Da mit den Kartenspeicherungen nicht den nach ärztlichem Standesrecht festgelegten Dokumentationspflichten entsprochen wird, gilt die standesrechtliche Mindestspeicherfrist von 10 Jahren nicht. In den Vereinbarungen nach § 291a Abs. 7 sollten Maximalspeicherfristen für die einzelnen Anwendungen festgelegt werden. Die Löschungen sollten automatisch erfolgen.

---

57 Vgl. Gesetzesbegründung (Fn. 21), S. 327.

58 Ludwig in Jäckel (Fn. 10), 206 ff.

59 Gesetzesbegründung (Fn. 21), S. 324.

Ein relativ leicht technisch zu lösendes Problem besteht darin, im Fall des **Verlustes einer eGK** den Zugriff Unberechtigter auf Kartendaten zu verhindern. Lediglich die optisch aufgebrachten Daten lassen sich der Karte direkt entnehmen. Sämtliche elektronisch gespeicherten Daten sollen grds. nur durch Nutzung einer HPC erlangt werden (Notfalldaten), evtl. gekoppelt mit einer Autorisierung durch den Versicherten selbst. Schwieriger ist die Restaurierung der Daten im Fall des Kartenverlustes. Die Originaldaten der auf und über die Karte gespeicherten Daten befinden sich bei verschiedenen verantwortlichen Stellen (Kasse, Leistungserbringer). Das Aufspielen der Daten bedarf daher grds. der Anlieferung durch all diese Stellen. Bei länger zurückliegenden Speicherungen dürfte auf diesem Weg ein vollständiges Verfügbarmachen des ursprünglichen Datenbestandes nicht möglich sein. Hierfür bedürfte es der regelmäßigen Speicherung eines Sicherungsdatenbestandes an einer Stelle (z.B. bei der Krankenkasse). Zugriff hierauf kann und darf aber ausschließlich der Patient selbst erhalten.

Die Kommunikation zwischen eGK und Hintergrundsystemen kann nach derzeitigem Stand nur durch direkten Kontakt zugelassen werden. Die Nutzung von **drahtloser Kommunikation** (RFID-Technik) verbietet sich wegen der vom Gesetz geforderten aktiven Beteiligung der Versicherten.

Die Kommunikation zwischen der eGK, der HPC/SMC, den Systemen der Leistungserbringer und der Krankenkassen sowie ergänzenden Servern hat in einem **geschützten Netz** zu erfolgen, zu dem Nichtberechtigte keinen Zugang haben (sog. Virtual Private Networks - VPN). Es bietet sich an, für diese Kommunikation die Infrastruktur von derzeit entstehenden regionalen Praxisnetzen zu nutzen.[60]

XV. Verfahrensfragen

Das BMGS hat den in § 291a Abs. 7 SGB V Beteiligten für die **Vereinbarung der Spitzenverbände** über die Schaffung der für die Einführung der eGK erforderlichen Informations-, Kommunikations- und Sicherheitsinfrastruktur eine **Frist** bis zum 01.10.2004 gesetzt. Die Spitzenverbände haben dazu einen Planungsauftrag erteilt, den die Bundesregierung als wichtigen Beitrag für die Einführung des eGK ansieht, auch wenn sie „nicht mit allen Aussagen ... übereinstimmt“ [61] In der Vereinbarung sind technische Schnittstellen, Formulare und Standards festzulegen. Hierbei sind die Grundsätze der Datensparsamkeit und Datenvermeidung zu beachten. Es müssen Festlegungen bzgl. der mindestens zu fordernden Datensicherheit bzgl. aller beteiligten Komponenten (Karten, Hintergrundsysteme, Server, Netze) erfolgen. Es ist vorgesehen, dass vor der Genehmigung durch das BMGS eine Stellungnahme des BfD einzuholen ist (§ 291a Abs. 7 S. 3 SGB V).

Nach den Angaben der Bundesregierung ist der Bundesbeauftragte für den Datenschutz (BfD) bei allen Verfahrensschritten zur Einführung der eGK eng eingebunden. Die Einbeziehung der Landesbeauftragten für den Datenschutz (LfDs) soll über den BfD erfolgen.[62] Dies erfolgt v.a. über den Arbeitskreis „Gesundheit und Soziales“ der Konferenz der **Datenschutzbeauftragten** des Bundes und der Länder. Die LfDs sind außerdem durch die Durchführung von Modellprojekten zur eGK in einzelnen Ländern mit dem Thema betraut. Die für die Datenschutzkontrolle der meisten Leistungserbringer zuständigen Datenschutzaufsichtsbehörden nach § 38 BDSG sind bei der Einführung der EGK bisher überhaupt nicht beteiligt worden.

Im Interesse der Förderung der Akzeptanz der eGK bei Leistungserbringern wie Versicherten ist dringend zu empfehlen, vor der Etablierung des Verfahrens bzw. vor Beginn des Wirkbetriebes ein **Datenschutzaudit** durchzuführen. Gesetzliche Regelungen für ein solches Audit gibt es in § 9a BDSG, § 78c SGB X sowie in einigen Landesdatenschutzgesetzen. Eine umfassendes Regelwerk und ein eingeführtes Verfahren gibt es bisher jedoch nur in Schleswig-Holstein (§ 43 Abs. 2 LDSG SH). Das dort praktizierte Verfahren ist aber auch für sonstige Datenschutz-Auditverfahren anwendbar. Mit dem Audit wird nach einem festgelegten Verfahren die Datenschutzkonformität eines Gesamtverfahrens geprüft und offiziell bestätigt.[63]

Nach Angaben der Bundesregierung wurden **Verbraucherschutzorganisationen** und die für die Wahrnehmung der Interessen der Patientinnen und Patienten und der Selbsthilfe chronisch Kranker und behinderter Menschen maßgeblichen Organisationen umfangreich in die Konzeptarbeiten zur Entwicklung und Einführung der eGK einbezogen.[64] Tatsächlich sind aber die Strukturen der Interessenorganisationen von Betroffenen bisher nicht stark genug, um effektiv die Einführung eines derart komplexen Systems wie das der eGK gestaltend zu

---

60 Z.B. Gesundheitsnetzwerk Flensburg (gn.fl), dazu Projektgruppe Gesundheitskarte SH (Fn. 8), Kap. 3.18.1 od. 3.22.

61 BReg., BT-Drs. 15/2810 (Fn. 11), u.a. Frage 7.

62 BReg., BT-Drs. 15/2810 (Fn. 11), Fragen 32 u. 34.

63 Ausführlich Weichert, MedR 2003, 674 ff.

64 BReg., BT-Drs. 15/2810 (Fn. 11), Frage 33.

begleiten. Daher beschränkte sich deren Funktion auf die von kritischen Begleitern. Im Interesse einer mehrseitigen Sicherheit auch in Bezug auf Patientengeheimnis und medizinisch-informationeller Selbstbestimmung ist es geboten, Betroffenen-Interessenverbände besser zu unterstützen und diese mit Verfahrensrechten auszustatten. Dies gilt insbesondere für die Phase der praktischen Anwendung der eGK, zumal die Versicherten mit einer komplizierten Technik und einer Vielzahl von Entscheidungsnotwendigkeiten konfrontiert sein werden. Um hier selbstbestimmt agieren zu können, benötigen die Versicherten unabhängige vertrauenswürdige Unterstützung.

XVI. Schlussbemerkungen

Die eGK befindet sich derzeit noch mitten im Entstehungsprozess. Die bisherige Entwicklung spricht dafür, dass Vertraulichkeit und Wahlfreiheit für die Versicherten nicht auf der Stecke bleiben müssen. Die eGK ist zweifellos ein Schlüssel für eine vereinfachte elektronische Kommunikation der am Gesundheitswesen Beteiligten. Dabei soll aber weder vom Erforderlichkeitsgrundsatz noch vom Grundsatz der Patientenautonomie abgewichen werden. Derzeit ist nicht absehbar, dass es über die eGK zur großen, evtl. zentralen Medizindatenbeständen kommen wird. Vielmehr haben alle Beteiligten erkannt, dass das für die Einführung der eGK nötige Vertrauen nur dann erreicht werden kann, wenn dieses auch tatsächlich begründet ist. Der „**gläserne Patient**" lässt sich mit Hilfe der eGK und der damit zum Einsatz kommenden Telematikinfrastruktur verwirklichen. Die Rahmenbedingungen sind aber auch geeignet, den „gläsernen Patienten" zu verhindern, ja den Patienten mehr Information und mehr Bestimmungsmöglichkeiten über seine medizinischen Daten zu geben.

Die eGK eröffnet natürlich auch Perspektiven zum „gläsernen Leistungserbringer" bzw. „**gläsernen Arzt**". Durch die bisher vorgesehenen Abschottungsmechanismen und Zugriffsbeschränkungen dürfte sich nach den aktuellen Regelungen durch die eGK selbst kein erhöhter Kontrolldruck für die Leistungserbringer ergeben. Hierzu dienen andere im Rahmen der Gesundheitsreform eingeführten Instrumente des SGB V.

Kurz nach Einführung der GKV-Karte im Jahr 1995 wurden entsprechende Versicherungskarten auch durch **private Krankenversicherungsunternehmen** eingeführt. Eine vergleichbare Entwicklung ist nach Einführung der eGK zu erwarten.[65] Dies hat rechtliche Konsequenzen: Das relativ komplexe, mehrere Parteien berücksichtigende Recht des SGB V muss auf den privatrechtlichen Bereich übertragen werden. Dabei ist sicherzustellen, dass unter Beachtung des privatrechtlichen Gestaltungsspielraums die Verfügungsbefugnis der Patienten über ihre Daten nicht zu Gunsten der Versicherungsunternehmen verschoben wird.

Die Instrumente für eine mögliche Gesundheitsüberwachung der Betroffenen werden zweifellos mit der eGK erweitert. Dass diese nicht missbraucht werden, setzt die **Wachsamkeit** von denjenigen voraus, die für die Patientenrechte eintreten. Der *Deutsche Bundestag* hat am 26.09.2003 die Erwartung zum Ausdruck gebracht, dass bei der Umsetzung der Neuregelungen zur Gesundheitsreform insbesondere im Hinblick auf die Datensparsamkeit und Datenvermeidung eine Evaluierung erfolgt und dass ihm bis Ende 2008 auf Grundlage der Evaluierungserfahrungen vom BMGS ein Bericht vorgelegt wird.[66] Den Datenschutzbeauftragten kommt bei der datenschutzrechtlichen Begleitung der weiteren Entwicklung sowie bei der genannten Evaluation eine zentrale Stellung zu. Künftig sollten aber auch die Verbraucher- und Patienteninitiativen mit mehr Rechten und Einfluss ausgestattet werden. Zwar sind für die eGK einige Weichen gestellt, viele richtungsweisenden Entscheidungen sind aber noch nicht getroffen. Diese dürfen nicht dazu führen, dass die Patientenautonomie ihre bisherige wichtige Rolle verliert. Die unter dem Vorzeichen der Patientenautonomie eingeführte eGK darf nicht sukzessiv zu einer Zwangskarte gemacht werden, so wie dies zunächst von einigen Gesundheitspolitikern propagiert wurde.

Für Hinweise und Verbesserungsvorschläge zu obigem Text danke ich Antje Glimm, Prof. Norbert Luttenberger und Torsten Koop. Anregungen an den Autor sind herzlich willkommen.

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Tel.: 0431/988-1205 (d), -1200 (z), -1223 (fax)
weichert@datenschutzzentrum.de

---

65 BReg., BT-Drs. 15/2810 (Fn. 11), S.1.

66 BT-Drs. 15/XX, S. 10.