Landesbeauftragter für den Datenschutz
Sachsen-Anhalt
Klaus-Rainer Kalk

28. DAFTA Köln

Referat für das Forum 7 am 19. November 2004
(Es gilt das gesprochene Wort)

Datenschutz und Datensicherheit bei Gesundheitskarte und JobCard
Die Reform des deutschen Gesundheitswesen - Hoffnung und Sorgen
aus der Sicht des Datenschutzes

Gesundheitskarte und JobCard sollen künftig vom Recht besonders geschützte personenbezogene Daten enthalten. Das vom Bundesverfassungsgericht im sog. Volkszählungsurteil vom 15. Dezember 1983 (BVerfG E 65,1) aus Artikel 1 Abs. 1 und Artikel 2 Abs. 1 Grundgesetz entwickelte (Grund-)Recht auf informationelle Selbstbestimmung garantiert und verlangt deshalb einen besonders sorgsamen Umgang mit diesen Karten und den auf diesen Karten vorgesehenen Daten über Millionen von Bürgerinnen und Bürgern.
Der von George Orwell in seinem Roman "1984" skizzierte total transparente Bürger kann und darf im demokratischen Rechtsstaat der Bundesrepublik Deutschland keine Wirklichkeit werden. Vielmehr sind mit dem Bundesverfassungsgericht mündige und selbstbewusste Staatsbürger zu fordern. Dazu gehört unabdingbar, dass die Betroffenen sowohl hinsichtlich ihrer gesundheitlichen als auch ihrer wirtschaftlichen Verhältnisse selbst bestimmen, was wer dazu in welchem Umfang über sie wissen darf - denn wir alle wissen:
Wissen über den Bürger ist Macht, und damit haben wir in unserer Geschichte der letzten 100 Jahre schlechte Erfahrungen gemacht.
Deshalb müssen im Zeitalter der modernen elektronischen Datenverarbeitung die Einführung solcher Cardsysteme, die blitzschnelle und oft unbemerkte Verarbeitungsprozesse über Millionen Staatsbürger ermöglichen, besonders sorgfältig vor ihrer Einführung geprüft und während ihres Gebrauches kontrolliert werden.

...

Teil A

Die elektronische Gesundheitskarte

Die Einführung der elektronischen Gesundheitskarte wird von der Politik (insbesondere Bundesministerin Schmidt) vorrangig mit zwei Argumenten begründet:

- es sei ein Instrument zur Verbesserung der Versorgungsqualität und
- eine neues fälschungssicheres Instrument gegen den bisherigen Chipkartenmiss-brauch

Insbesondere das zweite Argument der Fälschungssicherheit darf bezweifelt werden. Bisher hat die Praxis nach Einführung neuer elektronischer Mittel oder Verfahren auch die zügige Entwicklung von Missbrauchsmöglichkeiten ergeben.

Gliederung:

1. Rechtliche Grundlagen

Das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (BGBl. I 2003, S. 2190), das am 01.01.2004 in Kraft getreten ist, bildet die rechtliche Grundlage für die elektronische Gesundheitskarte (eGK). Im SGB V wurde der § 291 a eingefügt, wonach bis spätestens zum 01.01.2006 die bisherige Krankenversichertenkarte (GKV-Karte) (§ 291 Abs. 1 SGB V) zu einer eGK erweitert wird.

Anwendungen, die mit der eGK realisiert werden sollen:

• Administrativer Teil (verpflichtend):
  - Versicherungsangaben der bisherigen GKV-Karte (§ 291 Abs. 2 SGB V)
  - Berechtigung, im europäischen Ausland behandelt zu werden
  - papierlose Übertragung eines Rezeptes (Verordnung)

• Medizinischer Teil (freiwillig)
  - medizinische Notfallversorgungsdaten
  - elektronischer Arztbrief
  - Arzneimitteldokumentation
  - elektronische Patientenakte
  - Daten von oder durch den Versicherten
  - in Anspruch genommene Leistungen und deren vorläufige Kosten.

Nach Abs. 4 wird die Verarbeitung mit Hilfe der eGK auf das Erforderliche zur Versorgung beschränkt. Der Zugriff wird auf den Versicherten und die „Health Professionals“ begrenzt. Diese dürfen nach Abs. 5 S. 3 nur mit Hilfe eines elektronischen Heilberufsausweises, möglichst ausgestaltet als elektronische Signaturkarte zugreifen.
Auf Verlangen des Versicherten müssen Verordnungen und freiwillige Daten gelöscht werden (Abs. 6 S. 1).
Mindestens die letzten 50 Zugriffe auf die Daten müssen für Zwecke der Datenschutzkontrolle protokolliert werden (Abs. 6 S. 2).
Abs. 8 S. 1 verbietet es, vom Versicherten zu verlangen, den Zugriff auf Versichertendaten anderen als den gesetzlich Befugten zu gestatten.

2. Funktionen

2. 1. Ausweisfunktion

Durch die GKV-Karte erfolgt schon jetzt der Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung. Mit der eGK erfolgt

...

dies künftig auch innerhalb der gesamten europäischen Gemeinschaft (§ 291 a Abs. 2 S. 1 Nr. 2 SGB V).
In der Regel genügt die Vorlage der Karte zum Nachweis des Leistungsanspruchs. Damit keine Nichtberechtigten Leistungen mit der Karte in Anspruch nehmen können, sind Identifizierungsangaben des Berechtigten auf der Karte enthalten. Diese sind bisher auch schon Unterschrift, Name, Geburtsdatum, Anschrift, Krankenversichertennummer. Zukünftig werden diese ergänzt durch ein Lichtbild, das Geschlecht und den Zuzahlungsstatus.
Innerhalb Deutschlands kann die Berechtigung der Inanspruchnahme von Leistungen auch elektronisch überprüft werden. Der „europäische Auslandskrankenschein“ erscheint jedoch lediglich auf der Rückseite der eGK als Sichtdokument.

Nur an identifizierte Kassenmitglieder dürfen von ebenso zu identifizierten Leistungserbringern (HPC) Leistungen der gesetzlichen Krankenversicherung nach dem SGB V erbracht werden. Da mit der eGK diese Identifizierung des Leistungsberechtigten abschließend erfolgen soll, ist ein zusätzliches Anfordern von anderen Identitätsnachweisen ausgeschlossen.
Der Nachweis der Identität gegenüber dem System erfolgt über die Nutzung der eGK, evtl. ergänzt durch die Eingabe einer PIN oder durch einen biometrischen Abgleich (Authentifizierung).
Die eGK wird künftig dazu genutzt, dass bestimmte Rollen in den telemedizinischen Systemen wahrgenommen werden können. Wenn eine Person identifiziert oder eine erlaubte Rolle authentifiziert wurde, autorisiert die eGK zur Inanspruchnahme von Kassenleistungen sowie zu Wahrnehmung bestimmter Befugnisse zur Datenverarbeitung (z.B. Abruf von Daten).

Für eine Identifizierung müssen die Karte und der Versicherte auf jeden Fall eindeutig sein. Um dies zu realisieren, wird zunächst eine spezielle Kartennummer vergeben. Danach werden durch die Krankenkassen die Identifizierungsdaten auf die Karte geladen.

Die Krankenversichertennummer (KV-Nummer) muss nach § 290 Abs. 1 SGB V aus einem unveränderlichen Teil zur Identifikation des Versicherten und einem veränderlichen Teil, der nach bundeseinheitlichen Vorgaben die Krankenkasse und die Familienzugehörigkeit von

Mitversicherten erkennen lässt, bestehen. Eine zentrale Generierung der Nummer darf jedoch nicht zu einem zentralen Versichertenverzeichnis führen, da dieses unzulässig ist. Möglich wäre z.B., dass nach einer zentralen Nummernvergabe bei der Vergabestelle nur gespeichert bleibt, welche unveränderlichen Teile an welche Krankenkasse vergeben wurden. Darüber hinaus darf die KV-Nummer kein übergreifendes Personenkennzeichen werden.

Zur Vermeidung, dass Nichtberechtigte die eGK nutzen, soll vom Versicherten eine PIN verwendet werden (Authentifizierung). Diese zusätzliche Sicherheit ist gesetzlich nicht ausdrücklich geregelt, wird aber in § 291 a Abs. 5 S. 2 SGB V für die meisten freiwilligen Anwendungen vorausgesetzt. Einer ausdrücklichen gesetzlichen Regelung bedarf es erst dann, wenn die obligatorische Nutzung ausschließlich mit einer PIN möglich wäre. Es ist allerdings davon auszugehen, dass bestimmte Anwendungen der eGK von einer PIN-Eingabe abhängig gemacht werden. Hier entstehen dann Probleme z.B. bei älteren Menschen, die mit der PIN-Eingabe überfordert sein könnten. Es muss somit mindestens für die Pflichtanwendungen eine Alternative zur PIN-Nutzung geben (z.B. Nutzung einer Vertreter-PIN zur Einlösung eines Rezeptes).
Die Daten der Ausweisfunktion darf von den jeweiligen Leistungserbringern gelesen, d.h. erhoben werden.

Eine Authentifizierung der Leistungserbringer erfolgt per Signaturkarte, die über eine qualifizierte elektronische Signatur verfügt (§ 291 a Abs. 5 S. 3 SGB V).

2.2. Erklärungsfunktion

z.B. die Erklärung, mit Übergabe der eGK bestimmte medizinische Leistungen zu Lasten der GKV in Anspruch nehmen zu wollen

2.3 Dokumentations- oder Speicherfunktion

z.B. die Speicherung von Notfalldaten oder des Impfstatus

2.4. Übermittlungsfunktion

z.B. die Weitergabe von Identifikations- und medizinischen Daten an die verschiedenen Leistungserbringer

2.5. Verschlüsselungsfunktion

z.B. die Möglichkeit, mit Hilfe eines auf der Karte gespeicherten Schlüssels an anderer Stelle gespeicherte Daten zu entschlüsseln und zu nutzen

2.6. Verweisfunktion

Die eGK soll dazu genutzt werden, Daten über ein Netz zu übermitteln, ohne dass die Daten selbst, sondern nur ein Verweis hierauf auf der Karte gespeichert werden (Pointerfunktion).
§ 291 a SGB V enthält derzeit noch keine Festlegungen, welche Daten auf der Karte und welche auf einem Server gespeichert werden. Diese Festlegung soll im Rahmen des Standardisierungsprozesses erst nach Auswertung der Pilotphase vorgenommen werden.

• Nachteile einer Kartenspeicherung:

- Daten gehen mit Verlust der Karte verloren
- begrenzte Speicherkapazitäten
- eingeschränkte Sicherheitsfunktionalität

• Nachteile von netzbasierten Lösungen:

- Abhängigkeit der Verfügbarkeit von Daten von einem Netzanschluss
- bisher nur wenige praktikable Gesundheitsnetzwerke (z.B. Flensburg, Rheinland)

3. Anwendungen

3.1. E-Rezept

Es ist bisher nicht geklärt, ob die Speicherung der Rezeptdaten karten- oder servergestützt erfolgen soll.

Der verschreibende Arzt speichert auf bzw. 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 Medikaments. Die weitere Abrechnung für die Apotheke mit der Krankenkasse erfolgt über ein Apotheken-Rechenzentrum (§ 300 SGB V). Eine personenbezogene Speicherung der Verschreibungsdaten für nicht medizinische Zwecke ist nach erfolgter Abrechnung unzulässig.
Grundsätzlich ist der Zugriff auf die über die eGK erschlossenen Daten von einer Autorisierung mit einer HPC abhängig. Für Rezeptdaten soll der Zugriff auch durch Authentifizierung des Versicherten selbst ermöglicht werden (z.B. durch Karte und PIN).

3.2. Medizinische Notfallversorgungsdaten (freiwillig)

Durch Speicherung dieser Daten auf der Karte kann sichergestellt werden, dass die Daten für Akutbehandlungen jederzeit offline zur Verfügung stehen.
Wenn kein Notfall vorliegt, ist jedoch der Zugriff auf diese Daten auszuschließen.

Auf internationaler Ebene (G8) hat man sich dazu auf einen Datensatz geeignet, der auf der eGK digital gespeichert werden soll.

3.3. elektronischer Arztbrief

Die Arztbriefübermittlung ist als freiwillige Anwendung der eGK vorgesehen.

Das Verfahren ist dem E-Rezeptes gleich, nur, dass an die Stelle des Apothekers der weiter- bzw. nachbehandelnde Arzt bzw. der Hausarzt tritt. Dabei ist sicherzustellen, dass nur

...

der (ggf. noch unbekannte) Adressat (= Arzt) auf den an ihn gerichteten Arztbrief Zugriff hat.
Die Möglichkeit, dem Patienten Inhalte des Arztbriefes vorzuenthalten, ist mit der eGK technisch nicht mehr möglich, da dies eine Beschränkung des Verfügungsrechtes bedeuten würde.

3.4. Arzneimitteldokumentation

Hier können Probleme entstehen, da die elektronisch gespeicherte Einlösung des Rezeptes nicht identisch sein könnte mit der tatsächlichen Anwendung des Arzneimittels. Zu beachten ist ferner, dass eingenommene Medikamente nicht in der Dokumentation aufgenommen wurden.

Aus datenschutzrechtlicher Sicht ist es wichtig, dass der Apotheker für eine Verträglichkeitsprüfung nur solchen Datenzugriff erhält, der für diese Anwendung erforderlich ist.

3.5. elektronische Patientenakte

Datenschutzrechtliches Ziel muss es sein, dass durch die Erstellung von elektronischen Patientenakten keine zentralen medizinischen Datensammlungen entstehen. Egal ob eine zentrale oder dezentrale Speicherung von Gesundheitsdaten vorgenommen wird, es ist auszuschließen, dass zentrale Einheiten, wie z.B. die Krankenkassen, über diese Daten verfügen können.

Folgende Fälle sind zu unterscheiden:

- elektronische Patientenakte
  Hier handelt es sich um die beim Leistungserbringer Arzt geführte Patientenakte. Unbegrenzten Zugriff darauf hat ausschließlich der Leistungserbringer. Eine Zugriffsfreischaltung für weitere Leistungserbringer auf bestimmte Dokumente ist denkbar.

- elektronische Fallakte
  Hier führen mehrere Leistungserbringer, die einen Patienten gemeinsam bzgl. einer bestimmten Diagnose oder eines Behandlungskomplexes behandeln, gemeinsam eine elektronische Dokumentation.
  Für den Zugriff auf diese Daten sind zwei Alternativen denkbar:
  - alle berechtigten Leistungserbringer haben grundsätzlich auf sämtliche Daten Zugriff (Voraussetzung: ausdrückliche informierte Einwilligung des Patienten)
  - differenziertes Zugriffsregime durch den Patienten bestimmt.

- elektronisches Hausarztmodell
  Der Hausarzt ist in diesen Fällen allein verantwortliche Stelle im Sinne des Datenschutzrechts. Der Patient verpflichtet sich, alle medizinischen Leistungen nur vermittelt über den Hausarzt in Anspruch zu nehmen. Dadurch laufen alle Behandlungsdaten bei diesem zusammen und können von diesem beauskunftet werden. Dies bedeutet z.B., dass Arztbriefe von Spezialisten durch den Hausarzt in die Hausarztakte eingestellt werden. Der Hausarzt ist somit für die gesamte Dokumentation verantwortlich.

- elektronische Gesundheitsakten
  Hier erhält der Patient die Möglichkeit, eine unabhängige Dokumentation von wichtigen medizinischen Daten bei sich selbst als Kopie zu speichern. Der Zugriff durch einen Arzt kann dabei nur in Kombination von eGK und HPC erfolgen.

- Auskunft
  - über die in Anspruch genommenen Leistungen und deren vorläufige Kosten (§ 291 a Abs. 3 Nr. 6 i.V.m. § 305 Abs. 2 SGB V, Versichertenauskunft)
  - allgemeiner datenschutzrechtlicher Auskunftsanspruch über die gespeicherten Daten des Betoffenen, den Zweck der Speicherung, Herkunft und Empfänger (§ 291 a Abs. 4 S. 2 SGB V)
    Dieser Anspruch besteht gegen jede verarbeitende Stelle, d.h. gegenüber der Krankenkasse und den Leistungserbringern. Ziel dieses Auskunftsanspruches ist es, den Patienten zum „Herrn seiner Daten“ zu befähigen. Vorrangig handelt es sich um das Recht zur Einsichtnahme in die Behandlungsakte ohne eine zwingende Einbeziehung von Ärzten.

...

Zum Einen ist es daher möglich, dass die Krankenkasse als Herausgeberin der eGK auch für die sonstigen beteiligten Stellen die Auskunftserteilung im Auftrag übernimmt. Die Krankenkassen müssen den Versicherten dafür Geräte zur Verfügung stellen, die darüber hinaus verhindern, dass die Krankenkassen über die Betroffenenauskünfte Daten in Erfahrung bringen, auf die ansonsten keinen Zugriff und keinen Anspruch haben. Es ist daher erforderlich, dass sich der Versicherte mit der eGK und durch PIN-Eingabe eindeutig identifiziert.
Zum Anderen bietet sich eine patientenfreundliche Umsetzung des Auskunftsanspruchs bei den Endgeräten der Leistungserbringer an. In diesem Fall muss technisch sichergestellt werden, dass keine Daten in den Speicher des Leistungserbringers übernommen werden.

4. Datenschutzrechtliche Erfordernisse bei der Anwendung der eGK

Oberstes Ziel muss die Vermeidung des "Gläsernen Patienten" sein. In einem neueren Interview der Bundesministerin Ulla Schmidt wird dies bestätigt: (abgedruckt in "Moderne Verwaltung", November 2004, S. 34 f.: "Der Grundsatz der Freiwilligkeit der Speicherung von Gesundheitsdaten und die Datenhoheit der Patienten müssen gewahrt werden.")

4.1. Unterrichtung der Versicherten

Gem. § 291 a Abs. 3 S. 2 SGB V sind die Versicherten spätestens bei der Versendung der eGK durch die Krankenkasse 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 hat schriftlich zu erfolgen. Eine ergänzende oder vertiefende Darstellung z.B. im Internet ist zu empfehlen. Außerdem sollte ein zusätzliches Unterrichtungsangebot z.B. durch Berater oder Informationsveranstaltungen bereit gehalten werden.

Die Unterrichtung umfasst sowohl die obligatorischen als auch die freiwilligen Anwendungen. Bei der Darstellung hat eine korrekte Beschreibung zu erfolgen, die das Verständnis eines durchschnittlichen Versicherten nicht überfordert.
Auch müssen die Versicherten über ihre Rechte und über den Umgang mit der Karte informiert werden.

4.2. Einwilligung des Versicherten

Für das Erheben, Verarbeiten und Nutzen von Versichertendaten nach § 291 a Abs. 3 SGB V ist die Einwilligung des Versicherten gem. § 291 a Abs. 3 S. 3 SGB V erforderlich. Für eine wirksame Einwilligung bedarf es der Schriftform, allein die Hingabe der eGK genügt nicht.
Zuerst muss der Versicherte festlegen, welche Anwendungen wie zugelassen werden und welche Daten über die Karte gespeichert werden. Eine weitere eigenständige Entscheidung des Versicherten ist dann, welche Daten konkret erfasst und ob gespeicherte Daten zur Einsicht freigegeben werden sollen.
Wegen der Komplexität und der Differenziertheit der notwendigen Erklärungen und der evtl. begrenzten Verständnisfähigkeit der Versicherten müssen die Erklärungstexte so eindeutig und zugleich knapp wie möglich formuliert sein. Die Einwilligungserklärung muss aus sich selbst heraus verständlich sein.
Da die Einwilligung auf die einzelnen Anwendungen der eGK beschränkt werden kann, stellt dies das Minimum der Differenziertheit dar. Zusätzlich zu der allgemein erteilten schriftlichen Einwilligung muss der Patient vom Arzt mündlich gefragt werden, ob eine bestimmte Behandlung oder Verordnung aufgenommen werden soll. Außerdem darf der Patient nicht gezwungen sein, medizinische Daten aus einem anderen Behandlungszusammenhang offen legen zu müssen. Die Patientenentscheidung ist angemessen zu protokollieren.
Bzgl. der nutzungsberechtigten Leistungserbringer müssen die Einwilligungen ebenfalls hinreichend bestimmt sein, so dass es dem Versicherten möglich ist, bestimmte Ärzte von der freiwilligen Nutzung auszuschließen oder einzubeziehen. Die Vorlage der eGK genügt nicht für den Nachweis der Nutzungsberechtigung für den Leistungserbringer.

...

Gemäß § 291 Abs. 3 S. 3 SGB V ist die Einwilligung bei der ersten Verwendung der Karte vom Leistungserbringer zu dokumentieren.
Ferner kann die Einwilligung gem. § 291 Abs. 3 S. 3 2. HS SGB V jederzeit widerrufen werden. Der Widerruf kann sich auf einzelne Anwendungen beziehen und bedarf nicht zwingend der Schriftform.

4.3. Authentisierung der Leistungserbringer

Der Zugriff auf die eGK ist gem. § 291 a Abs. 5 S. 3 SGB V so zu organisieren, dass nur berechtigte Stellen die Möglichkeit des Lesens und Schreibens haben. Dies wird einerseits über den elektrischen Heilberufsausweis (HPC) realisiert. Für Institutionen werden andererseits elektronische Institutionsausweise (SMC) geschaffen, die delegationsfähig und übertragbar sind.

5. Architektur der Datenhaltung

Für die Kommunikationsprozesse im Gesundheitswesen lassen sich drei Kommunikationsformen unterscheiden:

- die adressierte Kommunikation = die zu übermittelnden Daten sind an eine bestimmte Person adressiert
- die gerichtete Kommunikation = Adressat ist eine Einrichtung
- die ungerichtete Kommunikation = beim Versand bzw. der Bereitstellung der Daten ist der spätere Empfänger noch nicht bekannt.

Aufgrund der freien Arztwahl und dem informellen Selbstbestimmungsrecht des Patienten ist die ungerichtete Kommunikation im Gesundheitswesen die häufigste Kommunikationsform. Diese ist somit als Standardfall anzusehen. Außerdem ist eine Architektur, die die ungerichtete Kommunikation ermöglicht, ebenso in der Lage, die adressierte und gerichtete Kommunikation abzudecken.

...

5.1. E-Rezept

• Trennung und Selektion der einzelnen Rezepte muss möglich sein, so dass bei Einlösung des Rezeptes, die sonstigen Rezepte von diesem Leistungserbringer nicht zur Kenntnis genommen werden können

• kartenbasierende Lösung:
  - Verfügbarkeit der Rezeptdaten abhängig von der Verfügbarkeit der eGK
  - bei Verlust oder Funktionsunfähigkeit kann das Rezept vom Arzt neu ausgestellt werden
  - Patient ist im alleinigen Besitz der Rezeptdaten
  - keine Datenverschlüsselung erforderlich

• Hybridlösung:
  - verordnende Arzt speichert das Rezept auf einem Rezeptserver und auf der eGK wird lediglich ein entsprechender Pointer erzeugt
    Pointer = alle notwendigen Informationen zur eindeutigen Identifizierung eines Objektes (hier: Rezept) und dessen Speicherort (hier: Rezeptserver)
  - Rezepte von vielen Patienten werden auf Rezeptservern gespeichert
  - von Serverausfall sind viele Patienten betroffen
  - bei Nicht-Verfügbarkeit oder Nicht-Funktionsfähigkeit der eGK kann das Rezept des jeweiligen Patienten nicht referenziert werden
  - Rezepte auf den Servern sind zu verschlüsseln

➔ kartenbasierende Lösung ist einfacher und technisch weniger aufwendig

5.2. Überweisung/Einweisung

• Möglichkeit zur Einzelselektion und Trennung, da verschiedene Dokumente für verschiedene Weiterbehandler bestimmt sein können

• serverbasierende Lösung:
  - abhängig von der Verfügbarkeit der Server und Netzwerkverbindungen
  - betroffene Personenkreis ist u.U. sehr groß
  - Zwischenspeicherung von Überweisungen auf den Servern erforderlich
  - Verschlüsselung erforderlich

• Hybridlösung:
  - abhängig von der Verfügbarkeit der Server und Netzwerkverbindungen und der Pointer auf der eGK
  - betrifft nur einzelne Patienten
  - betroffene Patient kann sich die entsprechenden Daten vom Arzt neu ausstellen lassen
  - Überweisungen werden auf Servern gespeichert, Pointer auf der Karte abgelegt

• kartenbasierendes System:
  - nur abhängig von der Verfügbarkeit der eGK
  - bei Nicht-Verfügbarkeit ist die Neuausstellung durch den Arzt möglich
  - alle Daten sind im Besitz des Patienten

5.3. Fallakte

• kartenbasierte Lösung
  - Rekonstruktion dieses Datenbestandes ist praktisch nicht möglich

• serverbasierte Lösung für zentrale Akte
  - Speicherung der Falldaten auf diversen Servern
  - Daten sind zu verschlüsseln
  - Verschlüsselungsverfahren für serverbasierte Architektur sind problematisch

• Hybridlösung der virtuellen Fallakte
  - Speicherung der Referenzdaten für die Dokumente eines Patienten auf dessen eGK
  - Dokumente sind auf Dokumentenservern gespeichert
  - Verschlüsselung der Dokumente mit dem Schlüssel des Patienten

6. Datenschutzrechtliche Zusammenfassung

Durch die Einführung der eGK darf sich die datenschutzrechtliche Position der Patienten nicht verschlechtern. Die Patienten sind bisher Herr ihrer Daten und das muss auch so bleiben. Der Betroffene muss durch die dafür erforderlichen technischen Sicherheitsfunktionen auf der Kartenbetriebsebene in die Lage versetzt werden, jederzeit abgestuft über den Teil- oder Gesamtzugriff auf seine Gesundheitsdaten zu entscheiden. Das bedeutet, dass folgende datenschutzrechtliche Parameter erfüllt sein müssen:

- Die Datenhoheit der Patienten und der Grundsatz der Freiwilligkeit der Speicherung von Gesundheitsdaten müssen bewahrt werden.
- Die Patienten müssen darüber entscheiden können, welche ihrer Gesundheitsdaten aufgenommen und welche gelöscht werden.
- Die Patienten müssen darüber entscheiden können, ob und welche Daten sie einem Leistungserbringer zugänglich machen.
- Die Patienten müssen das Recht haben, die über sie gespeicherten Daten zu lesen.

Die Regelung des § 291a SGB V bietet den normativen Rahmen, der diesen Parametern in ausreichender Form Rechnung trägt. Die technische Umsetzung darf nicht dazu führen, dass datenschutzrechtliche Einbußen erfolgen.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb unter Vorsitz des BfD eine Unterarbeitsgruppe des Arbeitskreises "Gesundheit und Soziales" zum Problembereich Gesundheitskarte gebildet. Diese strukturiert z.Zt. die datenschutzrechtlichen Problemkreise und entwirft Vorgaben für die Rahmenarchitektur der beauftragten Projektträger. Der BfD hat dazu mit Schreiben vom 05. November 2004 bereits in sechs Punkten Anmerkungen zum derzeitigen Stand der Planungen übermittelt.

...

Zuvor hatte der Arbeitskreis "Technik" der DSB-Konferenz bereits darauf hingewiesen, dass bestimmte Sicherheitsfunktionen zugunsten des Patienten und seiner Daten auf der späteren Karte nur realisierbar sind, wenn diese auch auf der Kartenbetriebsebene vorhanden sind (Beispiel: Deactivate Record). Fehlen solche Sicherheitsfunktionen im technischen Konzept, gehen die später getroffenen rechtlichen Rahmenbedingungen ins Leere!

Literatur:

Thilo Weichert in DuD (7) 2004, S. 391

Teil B

Die JobCard

Anzumerken ist zunächst, dass schon der Name irreführend ist, wie Walter Ernestus zu Recht in seinem **Literaturbeitrag in der DuD (7) 2004, S. 404**, feststellt. Die Karte befasst sich nicht mit dem Job, sondern soll vorrangig dann eingesetzt werden, wenn der Betroffene seinen Job verloren hat. Falsch ist auch das Etikett der Bundesregierung: "Bürokratieabbau". Der Abbau von Bürokratie ist zwar die vornehmste Pflichtaufgabe der Regierung, die dies bei dem Themenkreis aber nicht erfüllt. Aus dem Einführungsprospekt zur JobCard ergibt sich vielmehr, dass keine einzige der vom Arbeitgeber geforderten Meldepflichten beseitigt wird. Damit wird die in allen Datenschutzgesetzen des Bundes und der Länder enthaltene Verpflichtung zur Datensparsamkeit nicht umgesetzt, sondern lediglich mit der Behauptung unterlaufen, mit der neuen Card sei alles viel einfacher. Ehrlicher ist da schon die im Einführungsprospekt gegebene Erklärung zur Einführung: Die JobCard soll die Verbreitung der IT-Technologie in Deutschland forcieren. Also sollen Millionen abhängig Beschäftigter in Wahrheit als Versuchskaninchen für Staat und Wirtschaft genutzt werden. Unzureichende Aufgabenerledigungen eines Arbeitgebers und der Bundesagentur für Arbeit, als die in der derzeitigen Praxis bekannten tatsächlichen Hemmnisse für den Arbeitnehmer, werden durch die Einführung der Card in keiner Weise kompensiert.

...

1. Grundlagen

Die JobCard soll der zentralen Speicherung von Arbeitnehmerdaten im weitesten Sinne unter Einsatz einer Signaturkarte mit einer qualifizierten Signatur sowie einer Datenbank dienen.
Die Einführung ist zum 01.01.2006 geplant (Beschluss der Bundesregierung vom 21.08. 2002).
Derzeit besteht die Projekterlaubnis für zwei Teile, JobCard I und JobCard II.
Die Pilotierungsphase begann im September 2003 für das Projekt JobCard I und ist bereits seit April 2004 abgeschlossen. Teilnehmer waren u.a. die Lufthansa, VW, Steuerberater, die Datev, die Stadtverwaltung Frankfurt und die frühere BfA. Das Projekt JobCard II soll zum 30. Juni 2005 abgeschlossen werden.

2. JobCard I

2.1. Verfahren

Die Teilnehmer am Verfahren JobCard I sind der Arbeitgeber, die Bundesagentur für Arbeit (BA), eine Zentrale Speicherstelle (ZSS), das Trust Center, der Arbeitnehmer und die Registrierungsstelle Verfahrensteilnehmer.

Durch die JobCard soll die Arbeitsbescheinigung nach § 312 SGB III erfolgen.

Der Arbeitnehmer lässt seine Signaturkarte (vorausgesetzt dieser besitzt eine) mit einer qualifizierten elektronischen Signatur bei einer noch nicht bestimmten Registrierstelle für das Verfahren registrieren. Die Registrierstelle prüft anhand der gültigen Ausweispapiere die Legitimation und macht ein aktuelles Lichtbild mit einer Digitalkamera.

Anschließend wird der Antrag an ein frei wählbares und durch die Regulierungsbehörde für Telekommunikation und Post genehmigtes Trust Center gesandt, welches dann eine persönliche Signaturkarte, die JobCard, ausstellt. Diese wird per Einschreiben dem Antragsteller zugestellt.

...

Auf dem Chip der JobCard sind folgende Daten gespeichert:

- die Identifikationsnummer (ID) der Karte
- der vollständige Name
- die elektronischen Schlüssel
- die elektronische Signatur.

Außerdem verknüpft die Registrierstelle die eindeutige Kennung der Signatur mit der Rentenversicherungsnummer. (Da Beamte keine Rentenversicherungsnummer haben, erhalten sie eine entsprechende Nummer zur Verwendung im System.)

Der Arbeitgeber meldet die nach § 312 SGB III vorgeschriebenen Daten für die Arbeitsbescheinigung unter Angabe der Rentenversicherungsnummer an die ZSS.
Der Betroffene sucht dann eine Geschäftsstelle der BA auf, um sich Arbeit suchend oder arbeitslos zu melden und Arbeitslosengeld zu beantragen.

Durch die elektronische Signatur mit Hilfe der JobCard (Authentifizierung durch PIN und ggf. später durch einen biometrischen Abgleich), sowie der Legitimation des Mitarbeiters der BA (auch durch Signaturkarte) werden zunächst folgende Überprüfungen durchgeführt:

- Gültigkeit der Karte
- Zulässigkeit der Karte für das Verfahren
- Verifikation der Abfrage-Berechtigung des Mitarbeiters der BA
- sind alle Verfahrensteilnehmer auf Arbeitgeber- und Arbeitnehmerseite registriert.

Danach sendet die ZSS die erforderlichen Leistungsdaten, wie:

- aktuelle Daten der Beschäftigungszeit
- die Höhe der Entgeltzahlungen
- Angaben zur Auflösung des Arbeitsverhältnisses.

Die BA soll damit sofort in der Lage sein, den Leistungsanspruch zu berechnen und einen entsprechenden Bewilligungsbescheid zu veranlassen. Der Antragsteller ist von einer Bringschuld weiterer Daten zur Leistungsberechnung befreit.

Die dem Mitarbeiter der BA ausgestellte elektronische Vollmacht ist zeitlich und auf die Daten beschränkt, die für den Leistungsantrag erforderlich sind. Nach Ablauf der Frist ist ein wiederholter Zugriff auf die Daten nicht mehr möglich. Auf welchen Zeitraum sich die Frist bezieht, ist bisher nicht definiert.

2.2. Die ZSS

In der ZSS werden die vom Arbeitgeber übermittelten Daten gespeichert und zum Abruf bereitgehalten. Aufgrund der Vielzahl der dort gespeicherten Daten ist die Sicherheit der ZSS ein wesentliches Element bei der JobCard.

Folgende Sicherheitsvorgaben sind vorgesehen:

- Die Komponenten (Netzwerkelemente, Server usw.) der schreibenden Stellen (Arbeitgeber) sind strikt von den Stellen, die lesen dürfen (BA, Betroffener) zu trennen.
- Subsysteme, die Internetzugriff haben, haben keinen Zugriff auf die zentrale Datenbank und umgekehrt.
- Alle zu verarbeitenden (speichernden) Daten werden nur verschlüsselt in einer Datenbank abgespeichert.

Die Kommunikation zwischen Arbeitgeber und ZSS ist ebenso verschlüsselt wie die zwischen BA und ZSS.
Verbunden mit der Verschlüsselung ist auch eine Authentifizierung des Arbeitgebers und des abrufenden Mitarbeiters der BA.
Innerhalb der ZSS werden schreibende und lesende Zugriffe protokolliert und dokumentiert.

Datenschutzrechtliche Probleme:

Ein aus Sicht des materiellen Datenschutzrechts problematische Sachverhalt besteht aufgrund der vorgesehenen Vorratsspeicherung der Daten. Der Arbeitgeber meldet grundsätzlich bei **jeder** Kündigung die Daten an die ZSS, gleichgültig, ob diese überhaupt benötigt

werden oder nicht. (Kernaussage der Bundesverfassungsgerichtsentscheidung im Volkszählungsurteil vom 15.12.1983, BVerfG E 65,1 ff: Ein Zwang zur Abgabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind.) Eine Vorratsdatenhaltung ist deshalb grundsätzlich unzulässig.
Allerdings soll der Zweck der möglichen Verwendung detailliert gesetzlich beschrieben werden. Aber für die Einzelperson bliebe offen, ob die Daten jemals benötigt werden.

Außerdem sind aus datenschutzrechtlicher Sicht Modelle abzulehnen, die die Nutzung der Rentenversicherungsnummer zur Generierung der Identifikationsnummer einbeziehen. Die Verwendung der Rentenversicherungsnummer als eindeutiges Kennzeichen in der Datenbank würde die Erstellung von Persönlichkeitsprofilen ermöglichen. Bei der Wiedervereinigung Deutschlands wurde deshalb das im Gebiet der ehemaligen DDR verwendete Personenkennzeichen im Grundlagenvertrag als unzulässig bezeichnet und verboten. Aus diesem Grund besteht das gesetzliche Verbot der Nutzung einer SV-Nummer (§ 95 SGB IV).
Weitere rechtliche Probleme sind:

- der Arbeitnehmer weiß nicht, ob das, was der Arbeitgeber an die ZSS übermittelt, vollständig und richtig ist
- der Arbeitnehmer hat keine Kontrolle über die bei der ZSS zu seiner Person tatsächlich verarbeiteten Daten
- durch mögliche technische Ausfälle auf drei Ebenen (beim AG intern, auf dem Netzweg, bei der ZSS intern) sind zumindest die gesetzlich vorgegebenen Grundsätze der Vertraulichkeit, der Verfügbarkeit und der Revisionsfähigkeit in Frage gestellt

Noch nicht abschließend geregelt ist die Frage, wie viele Schlüssel und für welchen Zweck auf der Signaturkarte bereitgestellt werden müssen und wie der Zugriff auf diese zu erfolgen hat.

Ebenfalls noch ungeklärt ist, wo die ZSS angesiedelt wird. Da in der ZSS alle Daten aller abhängigen Beschäftigten über Jahre gespeichert werden sollen, wird derzeit davon ausgegangen, dass die ZSS nur bei einer Stelle des öffentlichen Rechts eingerichtet werden kann.

...

Dies lässt aber die Gefahr des umfassenden Herrschaftswissen beim Staat über die finanziellen Verhältnisse von über 60 Millionen Bürgern entstehen. Dabei darf die schon heute beim Staat nach anderen Rechtsvorschriften bestehende Übersicht über alle Bankkonten nicht vergessen werden!
Ähnliche Überlegungen gelten auch für die Einrichtung der Registrierstelle.

Ein besonderes Problem der Datensicherheit, aber auch der materiellen Verfügbarkeit, besteht darin, dass als Transportweg für die Datenübermittlung das Internet eingesetzt werden soll. Es wäre damit das erste Mal, dass von Staats wegen angeordnet ein privater Übermittlungsweg benutzt wird - noch dazu ein höchst unsicherer. Bekanntlich haben die Betreiber des Internets keine globale Rechtsverantwortung, sie garantieren auch niemandem einen ständigen gesicherten Betrieb; schon deshalb ist das Internet als Baustein in einem staatlich betriebenen, rechtsrelevanten Verbindungsgefüge völlig ungeeignet.

3. JobCard II

3.1. Verfahren

Das Verfahren JobCard I wird für das Verfahren JobCard II um folgende Elemente erweitert:

- der Arbeitgeber sendet eine monatliche Meldung an die ZSS
- hierzu wird ein Datenkranz definiert, der alle Daten enthält, die heute in Bescheinigungen benötigt werden und gesetzlich vorgeschrieben sind (bis zu 400 Merkmale pro Arbeitnehmer)
- die abrufberechtigte Stellen werden auf jene Behörden und Institutionen ausgeweitet, die für die Leistungsgewährung dann zuständig sind.

Das Zweite Gesetz für Moderne Dienstleistungen am Arbeitsmarkt (BGBl. I 2002, S. 4621) sieht bereits vor, dass die Arbeitgeber ihre Meldungen zur Sozialversicherung ab 01.01.2006 nur noch maschinell beibringen dürfen.
Das Grundmodell von JobCard II kann diese gesetzliche Meldepflicht nach § 28 a SGB IV auffangen.

...

3.2. Die ZSS

Die ZSS erhält demnach die Entgeltdaten aller in Deutschland beschäftigten Arbeitnehmer über Jahre. Der hohe Sicherheitsbedarf zeigt sich bei der Vorstellung, dass ein gelungener Angriff auf die ZSS mit der Zerstörung von Entgeltdaten aller Arbeitnehmer einher gehen würde.

Die sonstigen Abläufe entsprechen denen der JobCard I.

Das datenschutzrechtliche Problem der Vorratsspeicherung von Daten stellt sich hier erneut. Eine Minimierung dieses Problems kann nur durch eine gesetzliche Verpflichtung einer Zwangsprotokollierung aller Transaktionen in der Datenbank und der Möglichkeit diese Protokolldaten jederzeit dem Betroffenen zur Verfügung zu stellen erreicht werden. Die Realisierung des Auskunftsrechts erweist sich jedoch auch als problematisch, da zum Einen ein Datenzugriff nur mit zwei „Unterschriften“ möglich ist und zum Anderen nicht alle Daten abgerufen werden können, sondern nur die, die für einen bestimmten Leistungsantrag benötigt werden. Die Selbstauskunft muss daher durch eine zweite Karte einer berechtigten Stelle bestätigt werden. Auch dürfen die Daten dann nicht an diese Stelle, sondern an die Adresse des Betroffenen gesandt werden (in Papierform oder in elektronische Form).

Ein besonderes datenschutzrechtliches Problem entsteht im Zusammenhang mit der Plausibilitäts- und Vollständigkeitsprüfung der gemeldeten Daten durch die ZSS. Infolge dieser Prüfung ist die Entschlüsselung der Daten in der ZSS erforderlich. Anschließend werden die Daten zwar wiederum durch die ZSS verschlüsselt, für einen Moment sind die Daten jedoch in der ZSS unverschlüsselt „verfügbar“. Das heißt, der oder die Betroffene hat nicht die volle technische Verfügungsbefugnis über seine/ihre Daten. Die Mehrheit der Datenschützer fordert deshalb eine Ende-zu-Ende-Verschlüsselung. Dazu gibt es einen Gutachtenauftrag der 68. DSB-Konferenz vom 28./29. Oktober 2004, der die Vor- und Nachteile einer solchen Verschlüsselung unter besonderer Berücksichtigung der Datensicherheit beleuchten soll. Die Projektgruppe der Krankenversicherungen (ITSG) lehnt diese Verschlüsselung bisher ab.

Zudem ist es datenschutzrechtlich erforderlich, dass alle Datenflüsse über sichere Leitungen laufen. Eine Verwendung des Internets erfüllt dies nicht. Denn - wie bereits vorstehend auf Seite 21 ausgeführt - gibt es beim Internet weder eine Garantie für die ständige Funktionsbereitschaft noch ist eine geschützte Übertragung mit der erforderlichen Sicherheit gegen fremde Zugriffe möglich. Es ist deshalb zu fordern, dass ein Verfahren verwendet wird, das eine sichere Übermittlung ohne Datenverlust gewährleistet (ggf. auch Reserveverfahren für den Ausfall).

4. Übergreifende Aspekte

Es bestehen Erwägungen, die JobCard mit der eGK zu kombinieren. Hier gilt es zu vermeiden, dass durch eine bereichsübergreifende Nutzung einer bestimmten elektronischen Signatur diese rollenunabhängig zur Verknüpfung von zweckgebundenen Daten genutzt wird.

5. Datenschutzrechtliche Zusammenfassung

Die Einführung der JobCard ist ein rechtlich wie technisch hoch brisantes Unternehmen, das den Schutz der Persönlichkeitsrechte von Millionen abhängig Beschäftigter erheblich gefährdet. Die bisherige Konzeption ist aus datenschutzrechtlicher Sicht "löcherig" und in vielerlei Hinsicht unausgegoren. Ein möglicher legaler oder illegaler Missbrauch des in einer ZSS gesammelten Datenbestandes über Millionen von Bürgern schwächt deren autonome Stellung als Souverän des Staates und gefährdet die Demokratie.