

ELEKTRONISCHE GESUNDHEITSKARTE UND ELEKTRONISCHER HEILBERUFS AUSWEIS AUS DER SICHT DES DATENSCHUTZES

■ A. Schurig, A. Schneider

Sächsischer Datenschutzbeauftragter, Bernhard-von-Lindenau-Platz 1, D-01067 Dresden

1. Ausgangssituation

Die elektronische Gesundheitskarte, die in der Bundesrepublik Deutschland eingeführt werden soll, stellt eine der größten IT-technischen Herausforderungen der letzten Jahrzehnte dar. Die Karte soll nach dem Willen des Gesetzgebers flächendeckend eingeführt werden, ca. 70 Mio. Versicherte erfassen und der Kommunikation mit etwa 350.000 Ärzten, 2.000 Krankenhäusern und den zahlreichen Krankenkassen in Deutschland dienen. Die über Jahrhunderte gewachsenen und bewährten Kommunikationsabläufe zwischen Patienten und Leistungserbringern in einer komplexen IT-Architektur abzubilden, ist daher auch in Bezug auf das Volumen eine gewaltige Herausforderung. Nicht nur für die IT-Branche, Gesundheits-

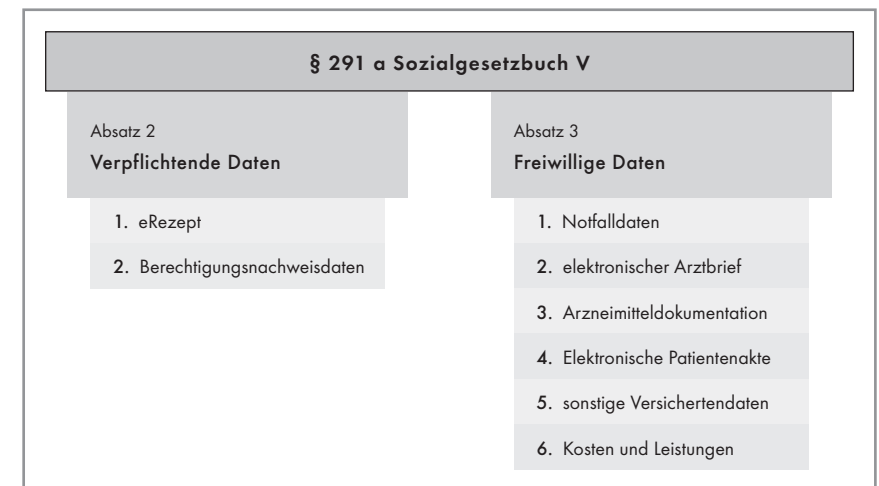


Abb. 1 Verpflichtende und freiwillige Daten auf der elektronischen Gesundheitskarte nach § 291 a Sozialgesetzbuch V

politiker und in Bezug auf den Ruf Deutschlands als Technologie-Standort steht viel auf dem Spiel. Große Bedeutung hat bei einer Speicherung von Gesundheitsdaten auf zentralen Servern, dass datensicherheitstechnische und datenschutzgerechte Belange umgesetzt werden, dass die Patientenrechte und das Grundrecht auf informationelle Selbstbestimmung der Patienten gewahrt bleiben.

Gesetzlicher Ausgangspunkt ist § 291 a Sozialgesetzbuch V (SGB V), wonach die elektronische Gesundheitskarte in Bezug auf die wesentlichen Datenverarbeitungsbereiche für die Patienten freiwillig ist. Dieses Freiwilligkeitserfordernis ist sachgerecht. Durch die Einführung der elektronischen Gesundheitskarte darf sich die datenschutzrechtliche Position des Patienten nicht verschlechtern. Die Zusammenführung von besonders schutzwürdigen medizinischen Daten über die betroffenen Patienten ist aus Verfassungs- und Akzeptanzgründen nicht ohne Einwilligung der Betroffenen umzusetzen (vgl. hierzu Weichert mit umfassenden und weiterführenden rechtlichen Ausführungen zur elektronischen Gesundheitskarte [1]). Dem Rechnung tragend hat der Gesetzgeber auch lediglich die Stammdaten und das elektronische Rezept (e-Rezept) für die Patienten zur Pflicht gemacht (vgl. Abb. 1).

2. Anforderungen an die elektronische Gesundheitskarte

Der Schutz des Patientengeheimnisses muss auch in einer zunehmend IT-gestützten Medizin wirksam gewährleistet sein [2]: Die Sicherheit des Systems selbst bemisst sich nach der Verlässlichkeit, der Verfügbarkeit, Integrität und Vertraulichkeit der Daten.

Die Patientenrechte dürfen sich durch die Einführung der elektronischen Gesundheitskarte nicht verschlechtern: Die hierfür erforderliche Beherrschbarkeit des Systems richtet sich nach der Zurechenbarkeit der Daten, Nicht-Abstreitbarkeit der Kommunikationsprozesse, Nutzungsfestlegung und Zugriffskontrolle, der Revisionsfähigkeit und Rechtssicherheit der Kommunikationsprozesse, der Durchsetzbarkeit der Betroffenenrechte (Auskunft, Berichtigung, Sperrung und Löschung), der Festlegbarkeit einer verantwortlichen Stelle für die Datenverarbeitung, Gewährleistung der freien Arztwahl, der Durchsetzbarkeit von Schadensersatzansprüchen und letztendlich auch nach der Praktikabilität für die Betroffenen (vgl. Tabelle 1; zu den grundlegenden Sicherheitsanforderungen an Medizinetze: vgl. [3]). Gerade in Bezug auf den letzten Punkt ist zu berücksichtigen, dass bestimmte Personen- und Gesellschaftsgruppen nicht durch eine zunehmend schwerer zu durchschauende Technik benachteiligt oder in der Wahrnehmung ihres Selbstbestimmungsrechts behindert werden.

Die Einführung der elektronischen Gesundheitskarte ist aber grundsätzlich geeignet, bei Beachtung der vorgenannten datenschutzrechtlichen Anforderungen die

Datenschutzanforderungen	Umsetzung
Zurechenbarkeit der Daten	Qualifizierte Signatur bei sämtlichen Patientendaten
Nicht-Abstreitbarkeit der Kommunikationsprozesse	Datenschutzgerechte Protokollierung und Quittierung der Kommunikationsprozesse
Nutzungsfestlegung / Zugangskontrolle	Festlegung der Informationsobjekte und deren angemessene Granularität
Revisionsfähigkeit / Rechtssicherheit	Voraussetzung: Nicht-Abstreitbarkeit und Authentizität der Daten; Sicherstellung durch entsprechende Gestaltung der Geschäftsprozesse
Durchsetzbarkeit der Betroffenenrechte	Voraussetzung: Festlegbarkeit einer datenverarbeitenden Stelle
Gewährleistung der freien Arztwahl	Entsprechende Nutzungsfestlegungen
Durchsetzbarkeit von Schadensersatzansprüchen	Voraussetzung: Rechtssicherheit
Praktikabilität für die Betroffenen	Herstellung der Alltagstauglichkeit durch Optimierung der Systemanforderungen in Bezug auf Einsatzmöglichkeiten unter Beschränkung auf das Erforderliche und leicht Verständliche bei Wahrung der Selbstbestimmungsmöglichkeiten

Tabelle 1 Datenschutzanforderungen und ihre mögliche Umsetzung

Transparenz des Behandlungsgeschehens und der Datenverarbeitungswege für die Patienten durchaus zu erhöhen, möglicherweise die medizinische Behandlung zu effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten zu senken und damit für die Patienten wie auch für die Leistungserbringer Vorteile mit sich zu bringen [4].

3. Einzelprobleme

Das zentrale Patientenrecht, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden [4–6], stellt für die technische Umsetzung eine zentrale Aufgabe dar, deren Lösung eines hohen Aufwandes bedarf. Jeder Patient, der eine Arztpraxis betritt, kann sich dafür entscheiden, dem jeweiligen Arzt alle freiwilligen Daten, nur einen Teil der Daten oder gar keine

freiwilligen Daten zur Verfügung zu stellen. Auch muss der Patient die Möglichkeit haben, gegenüber einem Arzt lediglich einzelne Dokumente, z. B. seiner Elektronischen Patientenakte, vorzuenthalten oder zu offenbaren. Das System darf nicht diejenigen, die ihre Daten aus den freiwilligen verarbeiteten Datenbereichen nur in Ausnahmefällen zugänglich machen wollen, benachteiligen. So kann nicht etwa die Freigabe der Elektronischen Patientenakte grundsätzlich vorausgesetzt werden, wenn der Patient sie nur in bestimmten Einzelfällen nutzen will und er dann bei den Behandlungsvorgängen jeweils zur Wahrung seiner Rechte dafür Sorge tragen muss, dass die Daten von den von ihm nicht autorisierten Leistungserbringern nicht verarbeitet oder genutzt werden können (zur Gefahr der pauschalen Offenbarung von Patientendaten, vgl. [6]).

Eine Lösungsarchitektur hat insofern häufig auftretende Fallgruppen zu berücksichtigen, damit nicht die differenzierte Einräumung der Nutzungsberechtigungen durch den Patienten gegenüber den Leistungserbringern in der Praxis erschwert wird und für den sein Selbstbestimmungsrecht ausübenden Patienten unpraktikabel wird. Darüber hinaus haben auch perspektivisch Lösungen zu unterbleiben, die nur die Patienten finanziell besser stellen, die den zusätzlichen Nutzungen der elektronischen Gesundheitskarte zugestimmt haben. Dass ein Patient sein informationelles Selbstbestimmungsrecht ausübt, kann ihm bei einer wirklichen Freiwilligkeitslösung nicht zum Nachteil gereichen. Beitragsrückerstattungen, z. B. etwa für pauschal einwilligende Patienten, haben daher zu unterbleiben. Derartige Modelle sind nicht mit dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten in Einklang zu bringen [7].

Gegen die Einwilligungslösung, bei der die differenzierte Zustimmung des Patienten die Voraussetzung für die automatisierte Verarbeitung über die elektronische Gesundheitskarte ist, wird häufig grundsätzlich eingewandt, dass die Datendokumentation damit zwangsläufig für die Leistungserbringer nicht vollständig sei. Dem ist entgegenzuhalten, dass das Arzt-Patienten-Geheimnis notwendigerweise eine Unvollständigkeit der Datenweitergabe einschließt. Zu vergessen ist auch nicht, dass es sich bei den automatisiert verarbeiteten Patientendaten um Kopien handelt. Der behandelnde Arzt verfügt über die eigentliche vollständige Dokumentation in Bezug auf die Behandlung seines Patienten. Dass damit die Erwartungen in Bezug auf die Einsparmöglichkeiten und den Nutzen der Karte selbstverständlich nicht zu hoch gesteckt werden können, sollte man insofern wegen der Rechtslage voraussetzen.

Einen weiteren Problembereich stellt die aufgrund des Selbstbestimmungsrechts des Patienten differenziert auszugestaltende Nutzungsberechtigungsarchitektur dar. Der Patient muss die Möglichkeit haben, bei der Einräumung der Datenverarbeitung in Bezug auf den Leistungserbringer sowohl nach einzelnen Personen als auch nach einzelnen Dokumenten zu differenzieren. Gegebenenfalls sollte auch

nach einzelnen Facharztgruppen und Krankenhaus-Organisationseinheiten unterschieden werden können. Ferner muss in der technischen Umsetzung dafür Sorge getragen werden, dass die Informationsobjekte in einer Granularität, die wirklich eine datenschutzgerechte Wahrnehmung des Selbstbestimmungsrechts der Patienten gewährleistet, verarbeitet werden.

In Bezug auf die Integrität und Zurechenbarkeit der Daten ist eine qualifizierte elektronische Signatur erforderlich. Dabei spielt der Heilberufsausweis die entscheidende Rolle. Der Gesetzgeber hat ihn und die qualifizierte Signatur ausdrücklich vorgesehen, § 291 a Abs. 5 Satz 3 SGB V. Dabei sind sämtliche patientenbezogenen Dokumente von ihrem Urheber bzw. Verantwortlichen zu signieren. Dies kann einen in der Praxis nicht zu unterschätzenden Aufwand darstellen. Auch die weitere Pflege der Daten kann aufwendig sein, sind doch z. B. nach dem Ablauf einer gewissen Zeit Signaturen zu erneuern oder möglicherweise Datenformate anzupassen.

Hinsichtlich der Speicherung auf zentralen Servern ergeben sich neben allgemeinen Datensicherheitsaspekten durchaus auch im Zusammenhang mit der Nutzung durch andere Stellen ungewollte rechtliche Implikationen. Von einer nur auf das Patienten-Arzt/Apotheken-Verhältnis bezogenen Nutzung kann nicht mehr ohne weiteres ausgegangen werden. Ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht in Bezug auf die Daten, die auf der Karte gespeichert sind, besteht nicht mehr ohne weiteres ([4], vgl. die Stellungnahme der Datenschutzbeauftragten u. a. hierzu). Bei der Auswahl der datenverarbeitenden Stelle sollte dieser Gesichtspunkt nicht unbeachtet bleiben.

4. Resümee

Präzise Ausführungen zur technischen Umsetzung der datenschutzrechtlichen Grundforderungen wurden bisher nicht vorgestellt. Angesichts des Zeitplans – die Gesundheitskarte soll zum 01.01.2006 eingeführt sein – sind die nach dem Gesetz zur Schaffung der Sicherheitsinfrastruktur verantwortlichen Krankenkassen, Kammern und Berufsorganisationen unter Handlungsdruck, was aber in keinem Fall zu datenschutzrechtlichen Einbußen führen darf.

Ein nachhaltiger Akzeptanz- und Vertrauensverlust auf Seiten der Patienten in Bezug auf die über die elektronische Gesundheitskarte zu verarbeitenden besonders schützenswerten Daten, die generell der ärztlichen Schweigepflicht unterliegen, ist geeignet, das Projekt ökonomisch und wegen seiner Sinnhaftigkeit in Frage zu stellen. Dies spätestens dann, wenn ein nicht unerheblicher Anteil der Patienten nicht bereit ist, die freiwilligen Möglichkeiten der Gesundheitskarte aus Selbstbestimmungsüberlegungen heraus zu nutzen.

5. Zusammenfassung

Im Mittelpunkt der Einführung der elektronischen Gesundheitskarte steht datenschutzrechtlich die Datenhoheit des Patienten, der Grundsatz der Freiwilligkeit der Speicherung von Gesundheitsdaten. Der Patient entscheidet – und selbstverständlich, wenn er dies will, jeweils in jedem Einzelfall – welche Gesundheitsdaten aufgenommen und gelöscht werden, wem sie zugänglich gemacht werden. Er hat darüber hinaus das grundsätzlich uneingeschränkte Recht, alle über ihn gespeicherten Daten zu lesen. Der elektronische Heilberufsausweis, der über eine qualifizierte Signatur zu verfügen hat, ist gesetzlich „der Schlüssel“ für die Leistungserbringer, z. B. Ärzte, zur Erhebung, Nutzung und Verarbeitung der Daten über die elektronische Gesundheitskarte. Er kann nur gemeinsam mit der elektronischen Gesundheitskarte, also mit bewusster Beteiligung des Patienten (von Notfallsituationen abgesehen), genutzt werden.

Wegen des Rechts des Patienten auf informationelle Selbstbestimmung und der Sensibilität der über die Karte verarbeiteten Gesundheitsdaten, die generell der ärztlichen Schweigepflicht unterliegen, bedarf es bezogen auf die Informationsobjekte einer hinreichend differenzierten Nutzungsfestlegung. Die Dateneinheiten sind wiederum in einer angemessenen Granularität festzulegen. Die sich aus den Datenschutzgesetzen ergebenden Sicherheitsanforderungen sind einzuhalten (vgl. z. B. § 9 Bundesdatenschutzgesetz, § 9 Sächsisches Datenschutzgesetz). An die Sicherheit des Systems sind wegen des Schutzbedarfs hohe Anforderungen zu stellen. Hinreichend präzise Vorschläge zur technischen Umsetzung der Datenschutzanforderungen, die eine datenschutzrechtliche Bewertung möglich machen, sind bisher noch nicht vorgestellt worden.

Schlüsselwörter: informationelle Selbstbestimmung, Arzt-Patienten-Geheimnis, Einwilligung (des Patienten in die automatisierte Datenverarbeitung), qualifizierte Signatur

6. Literatur

- [1] Weichert T: Die elektronische Gesundheitskarte. DuD 28 (2004), 391–403.
- [2] Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Dresden, 27.–28. März 2003: Entschließung – Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung, www.bfd.bund.de (23.11.2004).
- [3] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Datenschutz und Telemedizin – Anforderungen an Medizinetze – Stand 10/02, S. 5 ff., www.bfd.bund.de (23.11.2004).
- [4] 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Dresden, 27.–28. März 2003: Entschließung – Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung, <http://www.bfd.bund.de> (23.11.2004).
- [5] 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Münster, 24.–26. Oktober 2001: Entschließung – Datenschutzrechtliche Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte Versicherte), <http://www.bfd.bund.de> (23.11.2004).
- [6] 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Bremen, 9.–10. November 1995: Entschließung – Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen, <http://www.bfd.bund.de> (23.11.2004).
- [7] 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Potsdam, 9.–10. März 1994: Entschließung – Chipkarten im Gesundheitswesen, <http://www.bfd.bund.de> (23.11.2004).