ARTIKEL 29- Datenschutzgruppe

00323/07/DE
WP 131

Arbeitspapier
Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)

15. Februar 2007

Z U S A M M E N F A S S U N G

Das Arbeitspapier der Artikel 29-Datenschutzgruppe **zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)** gibt eine Interpretationshilfe zu den auf EPA-Systeme anwendbaren Datenschutzbestimmungen und erläutert einige der allgemeinen Grundprinzipien. Es liefert darüber hinaus konkrete Hinweise zu den Anforderungen, die bei der Einrichtung von EPA-Systemen an den Datenschutz gestellt werden müssen, und zu den Schutzmechanismen, die diese Systeme bieten müssen.

Die Datenschutzgruppe geht zunächst auf die **allgemeinen Datenschutzbestimmungen** im Zusammenhang mit EPA-Systemen ein. Ausgehend von dem generellen Verbot der Verarbeitung personenbezogener Gesundheitsdaten in Artikel 8 Absatz 1 der Datenschutzrichtlinie 95/46/EG beschäftigt sie sich mit der Anwendbarkeit der Ausnahmeregelungen von Artikel 8, Absätze 2,3 und 4 auf EPA-Systeme und plädiert dabei für eine enge Auslegung dieser Vorschriften.

Des Weiteren stellt die Datenschutzgruppe Überlegungen zu einem **geeigneten Rechtsrahmen** für EPA-Systeme an und gibt **Empfehlungen zu elf Themenkomplexen** ab, bei denen der Bedarf an speziellen Maßnahmen zum Schutz der Daten eines Patienten und eines jeden Einzelnen besonders deutlich wird, nämlich:

1. Wahrung des Selbstbestimmungsrechts
2. Identifizierung und Authentisierung von Patienten und medizinischem Personal
3. EPA-Zugangsberechtigung zu Eingabe- und Konsultationszwecken
4. Verwendung der EPA für andere Zwecke
5. Organisationsstruktur eines EPA-Systems
6. In EPA gespeicherte Datenkategorien und Art ihrer Präsentation
7. Übermittlung medizinischer Daten in Drittländer
8. Datensicherheit
9. Transparenz
10. Haftung
11. Kontrollmechanismen für die Verarbeitung von EPA-Daten

Die Artikel 29-Datenschutzgruppe fordert die Ärzteschaft und Angehörigen der Heilberufe sowie alle sonstigen beteiligten Personen und Einrichtungen sowie die breite Öffentlichkeit auf, sich zu dem vorliegenden Arbeitspapier zu äußern.

INHALT

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz von Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1], insbesondere auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe b,

gestützt auf ihre Geschäftsordnung[2], insbesondere die Artikel 12 und 14,

HAT FOLGENDE STELLUNGNAHME ABGEGEBEN:

I. Einführung

Das vorliegende Arbeitspapier der Artikel 29-Datenschutzgruppe will eine Interpretationshilfe zu den für Systeme zur elektronischen Speicherung von Patientendaten (elektronische Patientenakten – EPA) geltenden Datenschutzbestimmungen geben und einige allgemeine Grundprinzipien formulieren. Darüber hinaus will die Stellungnahme abklären, welche Vorbedingungen bei der Einrichtung von EPA-Systemen erfüllt sein und welche Schutzgarantien diese Systeme bieten müssen.

Das öffentliche Gesundheitswesen leidet unter enormen Kostensteigerungen, weshalb die Regierungen nach neuen Strategien verlangen. Eine oft genannte Lösung besteht in der „elektronischen Patientenakte (EPA)". Synonyme wären elektronische Krankenakte, elektronische Gesundheitsakte, elektronisches Krankenblatt u.ä..

Für die Zwecke des vorliegenden Arbeitspapiers bezeichnet der Ausdruck „elektronische Patientenakte (EPA)"

> *„eine ausführliche Krankenakte oder ein ähnliches Dokument, in dem der frühere und aktuelle körperliche und geistige Gesundheitszustand einer Person in elektronischer Form festgehalten ist, so dass diese Daten zum Zwecke der ärztlichen Versorgung oder zu verwandten Zwecken umgehend abgerufen werden können*[3]*."*

Bisher war es so, dass sich die Unterlagen über empfangene medizinische Leistungen bei den unterschiedlichen Leistungserbringern befinden und nicht in einer einzigen Akte gesammelt werden. Das Konzept der „EPA" bezweckt die zentrale Erfassung aller verfügbaren Unterlagen über die medizinische Versorgung einer Person aus verschiedenen Quellen und Zeitabschnitten. Sie würde demnach einen möglichst kompletten Überblick über den früheren und aktuellen Gesundheitszustand einer Person über längere Zeit hinweg und vielleicht sogar während des gesamten Lebens („von der Wiege bis zur Bahre") liefern. Die zentral erfassten EPA-Daten wären dann in elektronischer Form allen medizinischen Fachkräften und Einrichtungen, die über eine Zugangsberechtigung verfügen, zugänglich, wo und wann immer sie benötigt würden.

---

1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31 (nachstehend kurz "die Richtlinie"); abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_de.htm..

2 Annahme durch die Datenschutzgruppe auf ihrer dritten Sitzung am 11.9.1996.

3 Der Passus „zum Zwecke der medizinischen Versorgung und zu verwandten Zwecken" umfasst die in Artikel 8 Absatz 3 der Richtlinie genannten Verwendungszwecke.

Die elektronische Patientenakte gilt als geeignetes Instrument, um

- die Qualität der Behandlung zu verbessern, da sich der Leistungserbringer ein besseres Bild von dem Patienten machen kann
- die Wirtschaftlichkeit der medizinischen Behandlungen zu erhöhen und damit eine weitere Kostenexplosion im Gesundheitswesen zu verhindern
- Daten zum Zwecke der Qualitätskontrolle sowie zu statistischen und Planungszwecken im öffentlichen Gesundheitswesen zu erheben, was sich wiederum positiv auf die Kostenentwicklung im öffentlichen Gesundheitswesen auswirken könnte.

Die Antworten von europäischen Datenschutzbehörden auf einen 2005 in Umlauf gebrachten Fragebogen zeigten, dass EPA-Systeme in den meisten Mitgliedstaaten ein höchst aktuelles Thema sind. Die Umsetzung derartiger Pläne ist allerdings unterschiedlich weit gediehen: lediglich in einigen wenigen Mitgliedstaaten sind EPA-Systeme zumindest teilweise schon eingeführt, in den meisten Mitgliedstaaten sind sie hingegen noch in der Diskussion.

Da Leistungen des Gesundheitswesens zunehmend auch grenzüberschreitend erbracht werden, hat die Kommission in ihrer Mitteilung *„Elektronische Gesundheitsdienste - eine bessere Gesundheitsfürsorge für Europas Bürger: Aktionsplan für einen europäischen Raum der elektronischen Gesundheitsdienste“*[4] auf die Bedeutung von elektronischen Gesundheitsdiensten und die Interoperabilität elektronischer Patientenakten hingewiesen. Darüber hinaus finanziert die Europäische Gemeinschaft auch konkrete Projekte in diesem Bereich, u.a. zur elektronischer Speicherung von Patientendaten oder zur Patientenkennung (Beispiel: die europäische Krankenversicherungskarte). Bei der Durchführung derartiger Programme muss die Europäische Kommission in Zusammenarbeit mit den Mitgliedstaaten sicherstellen, dass alle einschlägigen Rechtsvorschriften im Bereich des Schutzes personenbezogener Daten eingehalten und gegebenenfalls Mechanismen eingeführt werden, die die Vertraulichkeit und die Sicherheit dieser Daten gewährleisten[5].

EPA-Systeme können qualitativ bessere und abgesichertere medizinische Informationen liefern als die herkömmlichen Arten medizinischer Dokumentation. Aus Sicht des Datenschutzes ist allerdings darauf hinzuweisen, dass EPA-Systeme nicht nur mehr personenbezogene Daten verarbeiten können (z.B. in einem neuen Kontext erhobene oder angehäufte Daten), sondern dass diese Daten auch schneller einem größeren Kreis von Empfängern zur Verfügung gestellt werden können.

Zu beachten ist ferner, dass elektronisch gespeicherte medizinische Daten nicht nur für medizinische Fachkräfte von Interesse sind, sondern auch das Interesse von Dritten wie etwa Versicherungsunternehmen oder Strafverfolgungsbehörden wecken können. Aus Sicht des Datenschutzes bergen die EPA-Systeme, die die medizinischen Daten einer Person aus verschiedenen Quellen zentral erfassen und diese sensiblen Daten weiteren Kreisen leichter zugänglich machen, ein neues Risikopotenzial, das die Dimensionen des möglichen Missbrauchs medizinischer Daten einzelner Personen völlig verändert. Auch wenn dieses neue Gefahrenpotenzial in den meisten Fällen erst zu einem späteren Zeitpunkt, nämlich dann, wenn das System bereits flächendeckend eingeführt ist, in vollem Ausmaß deutlich werden wird, muss das Bewusstsein hierfür schon jetzt, da die vorhandenen Modelle noch begrenzt oder partiell zum Einsatz kommen (z.B. lediglich Erfassung einiger medizinischer

[4] KOM(2004) 356 endg.

[5] Siehe Artikel 5 Absatz 5 der Entscheidung 1786/2002/EG.

Grunddaten und Bereitstellung lediglich für Krankenhäuser einer bestimmten Region), geschärft werden, da es nur eine Frage der Zeit ist, bis sie generell Anwendung finden.

II. Die für elektronische Patientenakten geltenden datenschutzrechtlichen Rahmenbestimmungen

Die Verarbeitung personenbezogener Daten in EPA-Systemen muss unter Beachtung der datenschutzrechtlichen Vorschriften erfolgen. Die Datenschutzgruppe verweist darauf, dass die für EPA geltenden rechtlichen Rahmenbedingungen aus dem zweiten Erwägungsgrund der Richtlinie hervorgehen, welcher besagt: „*Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen*“.

Das Grundrecht auf Schutz personenbezogener Daten beruht im Wesentlichen auf Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) und auf Artikel 8 der EU-Grundrechtscharta[6]. Konkretere Vorschriften enthalten unter anderem die EG-Datenschutzrichtlinie 95/46/EG und die Richtlinie 2002/58/EG über den Schutz der Privatsphäre in der elektronischen Kommunikation[7] sowie die gesetzlichen Regelungen der Mitgliedstaaten, mit denen die Richtlinien in innerstaatliches Recht umgesetzt wurden.

Die Verarbeitung personenbezogener Daten in EPA-Systemen unterliegt ferner den Vorschriften des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV. 108) und dem Zusatzprotokoll bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV. 181).

Da es in diesem Fall um elektronische Patientenakten geht, sei zudem besonders auf die Empfehlung des Europarates Nr. R (97) 5 zum Schutz medizinischer Daten vom 13. Februar 1997) verwiesen. Zu erwähnen sind schließlich auch die Empfehlungen, die von der Internationalen Arbeitsgruppe "Datenschutz in der Telekommunikation" in dem Arbeitspapier über den Online-Zugang zu elektronischen Patientendaten ausgesprochen werden[8].

1. Allgemeine Grundsätze

Wer im Rahmen von EPA-Systemen Daten erhebt, muss dabei die folgenden allgemeinen Datenschutzgrundsätze beachten:

- Grundsatz der eingeschränkten Verwendung (Zweckbindung): Dieser Grundsatz, der seinen Ursprung teilweise in Artikel 6 Absatz 1 Buchstabe b hat, untersagt unter anderem eine mit dem eigentlichen Zweck (den eigentlichen Zwecken) der Erhebung nicht zu vereinbarende Weiterverarbeitung der Daten.

---

[6] Das Recht auf Schutz personenbezogener Daten ist kein absolutes Recht; es kann aus Gründen des öffentlichen Interesses eingeschränkt werden. Ein Eingriff in dieses Recht aus Gründen des öffentlichen Interesses ist jedoch nur gerechtfertigt, wenn der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer und dabei der Grundsatz der Verhältnismäßigkeit gewahrt ist (Artikel 8 Abs. 2 EMRK).

[7] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ABl. L 201 vom 31.7.2002, S. 37).

[8] Die Empfehlungen wurden auf der 39. Sitzung der Arbeitsgruppe in Washington D.C. am 6. und 7. April 2006 angenommen (http://www.berlin-privacy-group.org).

- Grundsatz der Datenqualität: Diesem Grundsatz zufolge müssen die personenbezogenen Daten für die Zwecke, für die sie erhoben werden, erheblich sein und dürfen nicht darüber hinausgehen. Es dürfen somit keine irrelevanten Daten erhoben werden; falls dies dennoch geschehen ist, müssen sie gelöscht werden (Artikel 6 Absatz 1 Buchstabe c). Darüber hinaus müssen die Daten sachlich richtig und auf dem neuesten Stand sein.
- Grundsatz der Datenvorhaltung: Personenbezogene Daten dürfen nicht länger aufbewahrt werden, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.
- Informationspflichten: Nach Artikel 10 der Richtlinie sind die für die Verarbeitung von EPA-Daten Verantwortlichen verpflichtet, den Betroffenen bestimmte Informationen zu übermitteln, beispielsweise wer die Daten erhebt und zu welchem Zweck, für wen die Daten bestimmt sind und dass sie ein Auskunftsrecht haben.
- Auskunftsrecht: Artikel 12 der Richtlinie gibt den Betroffenen die Möglichkeit, die Richtigkeit und Aktualität der Daten zu überprüfen. Dieses Recht gilt ohne Abstriche auch für die Erhebung personenbezogener Daten in EPA-Systemen.
- Grundsatz der Datensicherung: Artikel 17 der Datenschutzrichtlinie verpflichtet die für die Verarbeitung Verantwortlichen, geeignete Maßnahmen zum Schutz gegen die zufällige oder unrechtmäßige Zerstörung oder die unberechtigte Weitergabe der Daten zu ergreifen. Dabei kann es sich um organisatorische oder technische Maßnahmen handeln.

2. Besonderer Schutz sensibler personenbezogener Daten

Die Verarbeitung personenbezogener Daten, die sich auf den Gesundheitszustand einer Person beziehen, ist besonders heikel und erfordert daher besondere Sicherheitsvorkehrungen.

> In Artikel 2 Buchstabe a der Richtlinie 95/46/EG sind personenbezogene Daten wie folgt definiert:
>
> *" alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind"*.
>
> In Artikel 8 Absatz 1 der Richtlinie sind besondere Kategorien von personenbezogenen Daten aufgeführt:
>
> *„Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben."*

Der Hinweis, dass sich eine Person am Fuß verletzt hat und halbtags krankgeschrieben ist, gehört zu den personenbezogenen Daten über die Gesundheit im Sinne von Artikel 8 Absatz 1 der Richtlinie 95/46[9]. Dasselbe gilt auch für personenbezogene Daten, die einen eindeutigen, engen Bezug zur Beschreibung eines Gesundheitszustands einer Person aufweisen: Daten

[9] Urteil des EuGH vom 6. November 2003 in der Rechtssache C-101/01 - Bodil Lindqvist.

über die Einnahme von Arzneimitteln oder Alkohol- und Drogenkonsum sowie genetische Daten gehören zweifellos zu den „personenbezogenen Daten über Gesundheit“, speziell wenn sie in eine Krankenakte aufgenommen wurden. Auch andere in den Behandlungsunterlagen eines Patienten enthaltene Daten – z.B. administrative Daten (Sozialversicherungsnummer, Einlieferungsdatum in die Klinik usw.) – müssen als sensibel eingestuft werden: Wenn sie für die Behandlung des Patienten nicht erheblich wären, würden und dürften sie nicht in der Krankenakte auftauchen.

Die Mitglieder der Datenschutzgruppe sind daher der Ansicht, dass sämtliche in medizinischen Unterlagen, elektronischen Patientenakten und EPA-Systemen enthaltenen bzw. gespeicherten Daten als "sensible personenbezogene Daten" zu gelten haben. Sie unterliegen damit nicht nur den allgemeinen Vorschriften der Richtlinie über den Schutz personenbezogener Daten, sondern auch den besonderen Datenschutzvorschriften über die Verarbeitung sensibler Daten in Artikel 8 der Richtlinie.

3. Generelles Verbot der Verarbeitung personenbezogener Daten betreffend die Gesundheit und Ausnahmen von dem Verbot

Artikel 8 Absatz 1 der Datenschutzrichtlinie 95/46/EG enthält ebenso wie Artikel 6 des Übereinkommens 108 des Europarates ein generelles Verbot der Verarbeitung personenbezogener Daten, die die Gesundheit betreffen. .

Dieser besondere Schutz, den Artikel 8 Absatz 1 gewährt, ergänzt die übrigen Bestimmungen der Richtlinie, insbesondere Artikel 6 über die Datenqualität und Artikel 7 über die Zulässigkeit der Datenverarbeitung.

Vom generellen Verbot der Verarbeitung medizinischer Daten werden jedoch Ausnahmen gemacht, da Informationen über einen Patienten für dessen richtige Behandlung unabdingbar sind.

Die Datenschutzrichtlinie enthält **zwingende Ausnahmeregelungen** (Artikel 8 Absätze 2 und 3) sowie eine **fakultative Befreiung** (Artikel 8 Absatz 4) vom Verarbeitungsverbot.

Alle diese Ausnahmebestimmungen sind eng **umgrenzt, erschöpfend** und **eng auszulegen**.

4. Artikel 8 Absatz 2 Buchstabe a „Ausdrückliche Einwilligung“

In Artikel 8 Absatz 2 Buchstabe a des EG-Vertrags heißt es:

> *Absatz 1 findet in folgenden Fällen keine Anwendung: a) Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvorschriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden“.*

a) Die **Einwilligung** des Betroffenen kann daher die Verarbeitung sensibler Daten rechtfertigen[10]. Wie schon in den Arbeitspapieren WP 12[11] und WP 114[12] ausgeführt, ist es gemäß Artikel 2 Buchstabe h der Richtlinie für die Gültigkeit der Einwilligung maßgeblich,

[10] Wer sich einer ärztlichen Behandlung unterzieht, willigt nicht automatisch im Sinne von Artikel 2 Buchstabe h in der Verarbeitung (vor allem nicht in die Offenlegung oder die Weitergabe) der bei der Behandlung erhobenen Daten ein.

[11] Arbeitspapier der Artikel 29-Datenschutzgruppe „Übermittlungen personenbezogener Daten an Drittländer: Anwendung der Artikel 25 und 26 der EU-Datenschutzrichtlinie (WP 12 vom 24. Juli 1998).

[12] „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995” der Artikel 29-Datenschutzgruppe (WP 114 vom 25. November 1995).

dass sie ungeachtet der jeweiligen Umstände "*ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage*" erfolgt ist.

aa) **Die Einwilligung muss ohne Zwang erfolgen**: ‚Ohne Zwang' bedeutet, dass sich eine Person aus freien Stücken und im Vollbesitz ihrer geistigen Kräfte ohne jeglichen sozialen, finanziellen, psychologischen oder sonstigen Druck von außen entscheiden kann. Erfolgt die Einwilligung nur, weil mit Nichtbehandlung oder einer schlechteren medizinischen Behandlung gedroht wird, kann von einer Einwilligung aus freien Stücken nicht die Rede sein. Die Einwilligung einer Person, die nicht die Möglichkeit hatte, eine echte Wahl zu treffen oder vor vollendete Tatsachen gestellt wurde, ist daher ungültig.

Wenn eine medizinische Fachkraft aus medizinisch indizierten Gründen in einer bestimmten Situation nicht anders kann als personenbezogene Daten in einer elektronischen Patientenakte zu verarbeiten, ist es nach Meinung der Datenschutzgruppe irreführend, wenn sie dazu die Einwilligung des Betreffenden einholt, um die Verarbeitung zu legitimieren. Eine Einwilligung sollte auf die Fälle beschränkt werden, in denen die betreffende Person tatsächlich frei entscheiden kann und anschließend die Einwilligung ohne irgendwelche Nachteile zurückziehen kann[13].

bb) Die Einwilligung muss einen konkreten Fall betreffen: Die Einwilligung ‚für den konkreten Fall' muss sich auf eine genau umrissene konkrete Situation beziehen, in der die Verarbeitung der medizinischen Daten erfolgen soll. Eine pauschale Zustimmung der betroffenen Person beispielsweise zur Erfassung ihrer medizinischen Daten in einer elektronischen Patientenakte und zur anschließenden Weitergabe früherer und aktueller Daten an in die Behandlung eingebundene medizinische Fachkräfte wäre keine Einwilligung im Sinne von Artikel 2 Buchstabe h der Richtlinie.

cc) Die Einwilligung muss in Kenntnis der Sachlage erfolgen: ‚In Kenntnis der Sachlage' bedeutet Einwilligung der betroffenen Person nach der bewussten Erfassung und Würdigung der Fakten und Auswirkungen einer Handlung. Sie muss in klarer und verständlicher Form genau und umfassend über alle relevanten Aspekte, insbesondere die in den Artikeln 10 und 11 genannten wie Art und Zweckbestimmung der verarbeiteten Daten, Personen, an die die Daten möglicherweise weitergegeben werden, und ihre Rechte, aufgeklärt werden. Hierzu gehört auch die Aufklärung über die möglichen Folgen bei Verweigerung der Einwilligung zu der jeweiligen Verarbeitung.

b) Bei sensiblen personenbezogenen Daten und damit auch bei für die elektronische Patientenakte bestimmten Daten muss die Einwilligung im Gegensatz zu den Bestimmungen in Artikel 7 der Richtlinie **ausdrücklich** erfolgen. Opt-out-Lösungen, bei denen die Einwilligung vorausgesetzt wird, wenn keine ausdrückliche Ablehnung erfolgt, genügen nicht dem Erfordernis der „ausdrücklichen" Einwilligung. Gemäß der allgemeinen Definition, wonach die Einwilligung eine Willensbekundung voraussetzt, muss sich die Einwilligung ausdrücklich auf den **sensiblen Daten** beziehen. Die betroffene Person muss sich darüber im

13 Stellungnahme 8/2001 der Datenschutzgruppe zur Verarbeitung personenbezogener Daten von Beschäftigten (WP 84, Punkt 10).

Klaren sein, dass sie auf den besonderen Schutz ihrer Daten verzichtet. Eine schriftliche Einwilligung ist allerdings nicht erforderlich.

c) Die Datenschutzgruppe hat festgestellt, dass es aus praktischen Gründen bisweilen schwierig sein kann, die Einwilligung zu erhalten, insbesondere dann, wenn es keine direkte Verbindung zwischen dem für die Verarbeitung Verantwortlichen und den betroffenen Personen gibt. Ungeachtet aller Schwierigkeiten muss **der für die Verarbeitung Verantwortliche** jedoch in jedem einzelnen Fall nachweisen können, dass er erstens die ausdrückliche Einwilligung der betroffenen Person erhalten hat und dass zweitens die ausdrückliche Einwilligung nach hinreichend genauer Aufklärung gegeben wurde.

d) Anders als in Artikel 7 wird in Artikel 8 Absatz 2 Buchstabe a dem Umstand Rechnung getragen, dass es Fälle geben kann, in denen das Verbot der Verarbeitung sensibler Daten **selbst durch ausdrückliche Einwilligung nicht** aufgehoben werden kann. Die Mitgliedstaaten können selbst entscheiden, ob und wie sie diese Fälle im Einzelnen regeln.

5. Artikel 8 Absatz 2 Buchstabe c: „lebenswichtige Interessen der betroffenen Person“

Die Verarbeitung sensibler personenbezogener Daten lässt sich mit dem Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten rechtfertigen, wenn die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.

Die Verarbeitung muss wichtige persönliche Interessen der betroffenen Person oder eines Dritten betreffen und medizinisch als lebenserhaltende Maßnahme in einer Situation indiziert sein, in der die betroffene Person ihrem Willen selbst nicht mehr Ausdruck verleihen kann. Daher kann diese Ausnahmeregelung auch nur für einige wenige Fälle gelten und darf keinesfalls zur Rechtfertigung der Verarbeitung personenbezogener medizinischer Daten zu anderen Zwecken als der Behandlung der betroffenen Person herangezogen werden, etwa zu allgemeinen Forschungszwecken, die keine unmittelbar verwertbaren Ergebnisse hervorbringen[14].

> Beispiel: Angenommen, eine Person ist nach einen Unfall bewusstlos und kann ihre Einwilligung zu der erforderlichen Offenlegung bekannter Allergien nicht geben. In diesem Fall würde die Ausnahmeregelung die Einsichtnahme einer medizinischen Fachkraft in die im EPA-System gespeicherten Daten ermöglichen, um sich dadurch Informationen über bekannte Allergien der betroffenen Person zu beschaffen, da diese Daten für den weiteren Verlauf der Behandlung entscheidend sein könnten.

6. Artikel 8 Absatz 3: „Verarbeitung der (medizinischen) Daten durch ärztliches Personal“

Artikel 8 Absatz 3 erlaubt die Verarbeitung sensibler personenbezogener Daten, wenn drei Voraussetzungen erfüllt sind: Die Verarbeitung der Daten muss „*erforderlich*“ sein und „*zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten*“ erfolgen; sie muss durch „*ärztliches Personal*“ vorgenommen werden, „*das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt*“ oder „*durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen*“.

---

[14] Artikel 26 Absatz 1 Buchstabe e enthält eine ähnliche Bestimmung im Hinblick auf Übermittlungen von Daten in Drittländer; zur Auslegung dieser Bestimmung siehe „Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995**”** der Datenschutzgruppe (WP 114 vom 25. November 1995).

a) Diese Ausnahme gilt lediglich für die Verarbeitung personenbezogener Daten zu dem **speziellen Zweck** der Erbringung gesundheitsbezogener Dienstleistungen wie Vorsorge, Diagnostik, Therapie und Nachsorge sowie zu Verwaltungszwecken wie etwa Abrechnung, Buchführung oder Statistik.

Nicht erfasst ist hingegen jegliche Art der Weiterverarbeitung, die zur Erbringung dieser Leistungen nicht unmittelbar erforderlich ist, wie medizinische Forschung, nachträgliche Kostenerstattung durch die Krankenversicherung oder die Durchsetzung von Geldforderungen. Nicht unter Artikel 8 Absatz 3 fallen ferner eine Reihe sonstiger Verarbeitungsvorgänge im Bereich des öffentlichen Gesundheitswesens und der sozialen Sicherheit, beispielsweise zur Sicherung der Qualität und Kosteneffizienz der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen; sie sind im Erwägungsgrund 34 der Richtlinie als Beispiele für die Anwendung von Artikel 8 Absatz 4 erwähnt.

b) Die Verarbeitung personenbezogener Daten unter Berufung auf Artikel 8 Absatz 3 muss des Weiteren für die unter Buchstabe a) genannten Zwecke „**erforderlich**" sein. Im Hinblick auf die EPA bedeutet dies, dass jegliche Aufnahme personenbezogener Daten in eine EPA absolut gerechtfertigt sein muss; die bloße „Nützlichkeit" des Vorhandenseins derartiger Daten in einer EPA wäre somit nicht ausreichend.

c) Die dritte in Artikel 8 Absatz 3 genannte Voraussetzung ist, dass die Verarbeitung sensibler personenbezogener Daten durch ärztliches oder sonstiges Personal erfolgt, das dem **Berufsgeheimnis (ärztliche Schweigepflicht) oder einer entsprechenden Geheimhaltungspflicht** unterliegt.

> Die nach der ärztlichen Standesordnung bestehende Schweigepflicht kam erstmals im ‚Eid des Hippokrates'[15] zum Ausdruck und wurde anschließend vom Weltärztebund in seiner Deklaration von Genf (1948) bestätigt. Sie dient dem Schutz der von medizinischem Personal im Verlauf der Behandlung eines Patienten gesammelten Daten. Die Verwendung dieser Informationen ist nur innerhalb der Grenzen des Behandlungsvertrages gestattet. Zwischen Arzt und Patient besteht ein Vertrauensverhältnis, das Dritte, auch wenn es sich um ärztliches Personal handelt, ausnimmt, es sei denn, der Patient hat in die Weitergabe seiner Daten eingewilligt oder die Weitergabe ist vom Gesetz so gewollt.

Die Datenschutzgruppe weist darauf hin, dass die besondere Verpflichtung zur Wahrung des Berufsgeheimnisses in den Mitgliedstaaten entweder gesetzlich verankert oder aber von einer Berufsvereinigung, die befugt ist, verbindliche Vorschriften zu erlassen, festgelegt sein muss. Die diesbezüglichen nationalen Vorschriften müssen ferner wirkungsvolle Sanktionen für den Fall des Verstoßes gegen die Schweigepflicht vorsehen.

Für den Fall, dass nicht-medizinisches Personal gezwungen ist, diese sensiblen personenbezogenen Daten zu verarbeiten, muss es laut Richtlinie ebenfalls verbindlichen Regeln unterworfen werden, die mindestens ein vergleichbares Maß an Vertraulichkeit und Datenschutz gewährleisten. Die Vorschriften müssen insbesondere die Verpflichtung enthalten, dass die Daten ausschließlich zu einem der in Artikel 8 Absatz 3 genannten Zwecke verwendet werden.

Ärztliches Personal, das die unmittelbare Verantwortung für die Behandlung der Patienten trägt, ist im Allgemeinen gesetzlich dazu verpflichtet, die von ihnen vorgenommene ärztliche Behandlung (Untersuchungen, Verschreibungen usw.) in Patientenakten zu dokumentieren.

---

[15] „*Über alles, was ich während oder außerhalb der Behandlung im Leben der Menschen sehe oder höre und das man nicht nach draußen tragen darf, werde ich schweigen und es geheimhalten"* (Quelle: http://en.wikipedia.org/wiki/Hippocratic_Oath).

Zahlreiche gesetzliche Vorschriften zur ärztlichen Schweigepflicht beschränken von jeher die Vorhaltung und Verwendung von Patientendaten auf das direkte zweiseitige Verhältnis zwischen dem Patienten und der von ihm konsultierten ärztlichen Fachkraft bzw. medizinischen Einrichtung.

d) Da Artikel 8 Absatz 3 der Richtlinie eine Ausnahme vom allgemeinen Verbot der Verarbeitung sensibler Daten darstellt, ist die Bestimmung eng auszulegen.

e) Die Frage, ob Artikel 8 Absatz 3 der Richtlinie als *alleinige* Rechtsgrundlage für die Verarbeitung personenbezogener in einem EPA-System dienen kann, ist nach Ansicht der Datenschutzgruppe zu verneinen; nach ihrem Verständnis bezieht sich Artikel 8 Absatz 3 ausschließlich auf die Verarbeitung medizinischer Daten für die dort genannten medizinischen und kurativen Zwecke und greift auch nur dann, wenn die Verarbeitung „erforderlich" ist und von einer ärztlichen Fachkraft oder einer sonstigen Person vorgenommen wird, die dem Berufsgeheimnis oder einer entsprechenden Geheimhaltungspflicht unterliegt. Werden in einer EPA personenbezogene Daten für darüber hinaus gehende Zwecke verarbeitet oder sind die dort genannten Voraussetzungen nicht erfüllt, kann Artikel 8 Absatz 3 nicht als alleinige Rechtsgrundlage für die Verarbeitung personenbezogener Daten dieser Art herangezogen werden.

Doch selbst wenn alle genannten Voraussetzungen erfüllt sind, darf nicht übersehen werden, dass EPA-Systeme ein neues Gefahrenpotenzial bergen, und um dem entgegenzuwirken, bedarf es neuer, zusätzlicher Schutzmaßnahmen: EPA-Systeme ermöglichen den direkten Zugang zu einem Bündel von Unterlagen verschiedenen Ursprungs (Krankenhäuser, Ärzte usw.) über die medizinische Behandlung, die eine bestimmte Person im Verlauf ihres Lebens erhält. EPA-Systeme überschreiten daher die traditionellen Grenzen, die die Beziehungen zwischen einem einzelnen Patienten und einer medizinischen Fachkraft oder Einrichtung kennzeichnen: Die Vorhaltung medizinischer Daten in einer elektronischen Patientenakte geht über das herkömmliche Maß der Vorhaltung und Nutzung von Krankenunterlagen hinaus. Durch die vielen Zugriffspunkte in einem offenen Netz wie dem Internet wird die Gefahr des unberechtigten Abfangens von Patientendaten größer. Wenn elektronische Patientenakten erst einmal ins Netz gestellt sind, kann sich das bisherige gesetzlich vorgeschriebene Maß an Vertraulichkeit, das noch von herkömmlichen Papierakten ausging, als unzureichend erweisen, um die privaten Interessen eines Patienten zu schützen. Voll ausgereifte EPA-Systeme neigen dazu, den Zugang zu medizinischen Informationen und sensiblen personenbezogenen Daten zu erleichtern und sie größeren Kreisen zugänglich zu machen. Vor diesem Hintergrund ist es nicht leicht sicherzustellen, dass tatsächlich nur das entsprechende ärztliche Personal Zugang zu den Informationen erhält, und auch nur zu Zwecken, die mit der medizinischen Versorgung der betreffenden Person in Zusammenhang stehen. Die Verarbeitung sensibler personenbezogener Daten ist bei EPA-Systemen sehr viel komplexer und hat direkte Auswirkungen auf die Rechte des Einzelnen. Folglich müssen EPA-Systeme als neues potenzielles Risiko für den Schutz sensibler personenbezogener Daten betrachtet werden.

Neben der Zweckgebundenheit und dem Erforderlichkeitskriterium greift Artikel 8 Absatz 3 auf die Verpflichtung der medizinischen Fachkräfte, die Daten ihrer Patienten vertraulich zu behandeln, als dem zentralen und traditionellen Schutzmechanismus zurück. Mit Einführung der EPA gilt dies jedoch möglicherweise nur noch beschränkt, da der Zweck der EPA unter anderem darin besteht, für Behandlungszwecke gerade solchen Fachkräften Zugang zu Krankenakten zu verschaffen, die an der in der Akte dokumentierten früheren Behandlung nicht beteiligt waren.

Die Datenschutzgruppe ist sich daher keineswegs sicher, dass, selbst wenn die Verarbeitung mit Artikel 8 Absatz 3 gerechtfertigt wird, die ärztliche Schweigepflicht allein den nötigen

Schutz in einem EPA-Kontext bietet. Neues Risikopotenzial erfordert zusätzliche und möglicherweise auch neue Sicherheitsvorkehrungen, die über die in Artikel 8 Absatz 3 vorgesehenen Mechanismen hinausgehen, um einen angemessenen Schutz der personenbezogenen Daten in EPA-Systemen zu gewährleisten.

7. Artikel 8 Absatz 4: Ausnahme vom Verarbeitungsverbot aufgrund eines wichtigen öffentlichen Interesses

Einige Vorschriften der Richtlinie lassen den Mitgliedstaaten relativ viel Spielraum, um das rechte Maß zwischen dem Schutz der Rechte der betroffenen Person einerseits und den legitimen Interessen der für die Verarbeitung Verantwortlichen oder Dritter oder etwaigen öffentlichen Interessen andererseits zu finden.

Artikel 8 Absatz 4 gestattet den Mitgliedstaaten weitere Abweichungen vom Verarbeitungsverbot:

> *„Die Mitgliedstaaten können vorbehaltlich angemessener Garantien aus Gründen eines wichtigen öffentlichen Interesses entweder im Wege einer nationalen Rechtsvorschrift oder im Wege einer Entscheidung der Kontrollstelle andere als die in Absatz 2 genannten Ausnahmen vorsehen.“*
>
> Im Erwägungsgrund 34 heißt es:
>
> *„(34) Die Mitgliedstaaten können, wenn dies durch ein wichtiges öffentliches Interesse gerechtfertigt ist, Ausnahmen vom Verbot der Verarbeitung sensibler Datenkategorien vorsehen in Bereichen wie dem öffentlichen Gesundheitswesen und der sozialen Sicherheit - insbesondere hinsichtlich der Sicherung von Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen -, der wissenschaftlichen Forschung und der öffentlichen Statistik. Die Mitgliedstaaten müssen jedoch geeignete besondere Garantien zum Schutz der Grundrechte und der Privatsphäre von Personen vorsehen.“*

a) Sollte ein Mitgliedstaat von dieser Möglichkeit Gebrauch machen wollen, so muss die Ausnahme folglich in einer Rechtsvorschrift oder einer Entscheidung der Kontrollstelle geregelt werden (**besondere Rechtsgrundlage**).

b) Die Verarbeitung der sensiblen personenbezogenen Daten muss aufgrund eines **wichtigen öffentlichen Interesses** gerechtfertigt sein. Im Erwägungsgrund 34 der Richtlinie werden Beispiele für Bereiche angeführt, in denen ein solch wichtiges öffentliches Interesse gegeben sein könnte. Hierzu gehören insbesondere das öffentliche Gesundheitswesen und die soziale Sicherheit, wenn es darum geht, die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechung von Leistungen in den Krankenversicherungssystemen sicherzustellen.

Das wichtige öffentliche Interesse ist von den Mitgliedstaaten in jedem Einzelfall für den gesamten Umfang der ausgenommenen Verarbeitungen darzulegen; außerdem muss die Verarbeitung im Hinblick auf dieses wichtige öffentliche Interesse erforderlich sein. Jede Maßnahme dieser Art muss verhältnismäßig sein, d.h. es darf keine weniger einschneidende Alternativen geben.

Um rechtmäßig zu sein, was etwaige Eingriffe in das Privat- und Familienleben betrifft, muss sie sich ferner im Einklang mit Artikel 8 der Europäischen Menschenrechtskonvention in der Auslegung des Straßburger Gerichtshofs für Menschenrechte befinden: Sie muss „*in Übereinstimmungen mit den Gesetzen*“ erfolgen und „*in einer demokratischen Gesellschaft*“

aus Gründen des öffentlichen Interesses erforderlich sein. Der Gerichtshof hat wiederholt entschieden, dass in der Eingriffsnorm der Umfang des den zuständigen Behörden eingeräumten Ermessens und die Art und Weise, wie dieses Ermessen ausgeübt wird, unter Berücksichtigung des rechtmäßigen Ziels der betreffenden Maßnahme hinreichend klar ausgeführt sein müssen, damit der Einzelne vor willkürlichen Eingriffen angemessen geschützt ist.

c) Die Mitgliedstaaten müssen dabei **geeignete besondere Garantien** zum Schutz der Grundrechte und der Privatsphäre von Personen vorsehen.

d) Macht ein Mitgliedstaat von Artikel 8 Absatz 4 Gebrauch, ist gemäß Artikel 8 Absatz 6 die Kommission davon in Kenntnis zu setzen.

In Bezug auf die elektronische Patientenakte stellt die Datenschutzgruppe fest, dass die Argumente zur Einführung von EPA-Systemen (vgl. Punkt I) unter Umständen „ein wichtiges öffentliches Interesse“ erkennen lassen. In einigen Mitgliedstaaten ist in der Verfassung ein 'Recht auf Schutz der Gesundheit' verankert, die zeigen, wie wichtig geeignete Maßnahmen zur Sicherung des „Gesundheitsschutzes“ genommen werden. In einem solchen rechtlichen Kontext würde ein EPA-System sicherlich mit einem „wichtigen öffentlichen Interesse“ begründet, da es sich dabei um ein Instrument handelt, das ja speziell dazu gedacht ist sicherzustellen, dass der Patient medizinisch angemessen versorgt wird.

Artikel 8 Absatz 4 der Richtlinie könnte daher als Rechtsgrundlage für ein EPA-System herangezogen werden, sofern es alle darin genannten Voraussetzungen erfüllt. Wichtig ist vor allem, dass es geeignete Garantien zum Schutz der dort gespeicherten personenbezogenen Daten bietet.

Im folgenden Abschnitt möchte die Datenschutzgruppe daher die Frage möglicher Garantien und eines geeigneten Rechtsrahmens für EPA-Systeme diskutieren.

III. Überlegungen zu einem geeigneten Rechtsrahmen für EPA-Systeme

Die Datenschutzgruppe beschäftigt sich nachstehend mit einigen Themenkomplexen, bei denen im Rahmen von EPA-Systemen besonderer Handlungsbedarf besteht, wenn die Rechte der Patienten in Bezug auf den Schutz ihrer Daten gewährleistet werden sollen[16]. Wegen der weitreichenden Folgen von EPA-Systemen und der besonderen Transparenz, die derartige Systeme erfordern, sollten die Garantien vorzugsweise in einem umfassenden gesonderten Rechtsrahmen festgelegt werden.

1. Wahrung des Selbstbestimmungsrechts

Auch wenn ein EPA-System nicht ausschließlich auf der Einwilligung der betroffenen Person (Artikel 8 Absatz 2) als alleiniger Rechtsgrundlage beruht, sollte die Selbstbestimmung des Patienten über Zeitpunkt und Art der Verwendung seiner Daten als Schutzmechanismus eine große Rolle spielen[17].

---

[16] Die allgemeinen Anforderungen der Richtlinie 95/46/EG an die rechtmäßige Verarbeitung personenbezogener Daten werden an diese Stelle nicht noch einmal wiederholt, da sie sowieso gelten. Hier geht es nur um die besonderen zusätzlichen Anforderungen an die Verarbeitung medizinischer Daten in EPA-Systemen, die notwendig erscheinen, um das besondere Risiko, das EPA-Systeme für den Schutz der Privatsphäre darstellen, auszugleichen.

[17] In einigen Rechtsräumen existiert nicht nur ein Grundrecht auf Datenschutz, sondern auch ein verfassungsmäßiges Recht auf Schutz der Gesundheit: Die Verpflichtung zur Bereitstellung einer optimalen Behandlung hat einige Mitgliedstaaten dazu veranlasst vorzuschreiben, dass medizinische Fachkräfte Zugang zu

a) Die "Zustimmung" des Patienten ist, wenn ihr die Funktion einer geeigneten Garantie zukommt, nicht mit der „Einwilligung“ gemäß Artikel 8 Absatz 2 der Richtlinie gleichzusetzen und muss somit auch nicht alle Voraussetzungen des Artikels 8 Absatz 2 erfüllen: Während die **Einwilligung als Rechtsgrundlage** für die Verarbeitung von Krankendaten stets „ausdrücklich“ gegeben werden muss, braucht die **Zustimmung als eine Form der Garantie** nicht unbedingt im Voraus (Opt-in) erfolgen – die Möglichkeit, von seinem Selbstbestimmungsrecht Gebrauch zu machen könnte - je nach Lage der Dinge – auch die Form einer ausdrückliche Ablehnung (Opt-out-Lösung) annehmen.

b) Da die verschiedenen Arten von Krankendaten unterschiedlich schwerwiegende Konsequenzen haben können, sollte zwischen verschiedenen Verwendungsmöglichkeiten mit **abgestuften Arten der Ausübung des Selbstbestimmungsrechts** unterschieden werden:

So sollten die Rechtsvorschriften über die Einführung eines EPA-Systems für die Eingabe von Daten in eine elektronische Patientenakte oder den Zugang zu diesen Daten ein graduelles System vorsehen, das zum Teil die Einwilligung (Opt-in-Verfahren), vor allem wenn es um die Verarbeitung von Daten mit besonders schwerwiegenden potenziellen Folgen geht wie Abtreibungsdaten, psychiatrische Daten usw.[18]) und bei weniger kompromittierenden Daten die ausdrückliche Ablehnung (Opt-out-Verfahren) vorschreibt[19]. Dieses System hätte den Vorteil, dass es zum einen das nötige Maß an Schutz bietet und zum anderen praktikabel und flexibel ist.

c) Ein Patient sollte grundsätzlich **die Möglichkeit haben, die Weitergabe** seiner medizinischen Daten, die von einer medizinischen Fachkraft während der Behandlung registriert wurden, an anderes medizinisches Personal **zu verhindern**.

Ferner stellt sich die Frage, wie zu verfahren ist, wenn der Zugang zu Informationen in einer EPA verwehrt wird: Soll die Zugangsverweigerung so erfolgen, dass sie für den Betreffenden gar nicht sichtbar wird, oder sollte sie – eventuell beschränkt auf bestimmte Fälle – mit einer Nachricht verbunden werden, dass zusätzliche Informationen zwar vorhanden, aber nur unter bestimmten Voraussetzungen zugänglich sind.

d) Ausgehend von der Annahme, dass niemand gezwungen werden kann, sich an einem EPA-System zu beteiligen, müssen die Rechtsvorschriften über die Einführung eines EPA-Systems auch die Möglichkeit eines kompletten Ausstiegs aus dem System in Betracht ziehen. Es muss geregelt werden, ob dies eine Verpflichtung zur vollständigen Löschung der Daten beinhaltet oder ob lediglich der weitere Zugang zu den EPA-Daten verhindert wird; dabei kann die Entscheidung auch den betroffenen Personen überlassen werden.

2. Identifizierung und Authentisierung von Patienten und medizinischem Personal

a) In EPA-Systemen müssen Patienten **absolut zweifelsfrei identifizierbar[20]** sein. Würden aufgrund von Fehlern bei der Patientenidentifikation irrtümlicherweise Daten einer anderen Person verwendet, hätte dies in vielen Fällen fatale Folgen.

---

den im EPA-System gespeicherten Daten haben sollen. Dies ist in Ordnung, solange es ein Gegengewicht gibt in Form von ausführlichen Vorschriften, die die Einzelheiten des rechtmäßigen Zugangs oder die –gravierenden – Folgen im Fall des Missbrauchs der Zugangsrechte u.a. regeln.

[18] Es könnten besondere Anwendungen wie etwa "versiegelte Umschläge" eingeführt werden, die sich ohne Zutun der betroffenen Person nicht öffnen lassen.

[19] Damit die Opt-out-Lösungen wirklich eine angemessene Garantie darstellen, muss der Patient allerdings entsprechend informiert werden.

[20] „Identifizierbar“ bedeutet, dass eine Person durch Identifikationsmerkmale wie Name, Geburtsdatum, Anschrift usw. beschrieben wird; im vorliegenden Fall wird es nötig sein, dass die Richtigkeit der Beschreibung durch amtliche Bescheinigungen wie Geburtsurkunde, Pass oder Sozialversicherungskarte u.ä. bestätigt wird.

Eine elektronische Gesundheitskarte in Form einer Chipkarte könnte die elektronische Identifizierung von Patienten und auch ihre **Authentisierung[21] für den Fall, dass die Patienten ihre Akte selbst einsehen wollen**, erheblich erleichtern.
b) Wegen der besonderen Sensibilität der Krankendaten muss außerdem verhindert werden, dass sich Unbefugte Zugang zu den Daten verschaffen können. Voraussetzung für eine zuverlässige Zugangskontrolle sind eine zweifelsfreie Identifizierung[22] und Authentisierung. Benutzer müssen deshalb **eindeutig identifizierbar und zudem ordentlich authentifizierbar** sein. [23]

Da einer der Hauptvorteile von EPA-Systemen in der Möglichkeit des Zugriffs mittels elektronischer Kommunikationsmittel unabhängig von Zeit und Ort besteht, müssen Routinen für eine zweifelsfreie Identifizierung und Authentisierung eingerichtet werden. Um die mit der Authentisierung mittels Kennwort verbundenen Risiken zu umgehen, sollte zumindest längerfristig die Authentisierung mit Hilfe der elektronischen Signatur angestrebt werden, die den Nutzern zusammen mit einer ordentlichen amtlichen Kennung - beispielsweise auf besonderen Chipkarten - zugeteilt wird.

Für medizinisches Personal muss ein Erkennungs- und Authentisierungssystem entwickelt werden, bei dem eine medizinische Fachkraft nicht nur seine Identität nachweisen muss, sondern auch die **Funktion, in der sie elektronisch tätig wird**, z.B. als Psychiater oder Krankenschwester.

3. EPA-Zugangsberechtigung zu Eingabe- und Konsultationszwecken

a) Allgemeine Zugangskontrollsysteme:

Die Daten in EPA-Systemen sind vertrauliche medizinische Aufzeichnungen. Für den Zugang zu einer elektronischen Patientenakte muss daher der **Grundsatz** gelten, dass - abgesehen vom Patienten selbst – **nur** jene **medizinischen Fachkräfte** oder Mitarbeiter von Gesundheitseinrichtungen **zugangsberechtigt sein dürfen**, **die an der Behandlung** des Patienten **mitwirken**. Es muss somit eine akute Behandlungssituation zwischen dem Patienten und der medizinischen Fachkraft vorliegen, die auf die EPA-Daten zugreifen möchte.

Regelungsbedarf dürfte auch bei der Frage bestehen, welche Arten von medizinischen Fachkräften/Einrichtungen auf welcher Ebene Zugang zu EPA-Daten erhalten sollen (praktizierende Ärzte, Krankenhausärzte, Apotheker, Krankenschwestern, Chiropraktiker?, Psychologen?, Familientherapeuten? usw.).

Der Datenschutz könnte außerdem durch **modulare Zugangsrechte** erhöht werden, d.h. die medizinischen Daten in einer elektronischen Patientenakte werden in bestimmte Kategorien eingeteilt, auf die jeweils nur bestimmte medizinische Fachkräfte/Einrichtungen zugreifen dürfen[24]. Die Vorteile einer modularen EPA werden ausführlicher unter Ziffer 6 erörtert.

---

[21] „Authentisierung“ bedeutet, dass eine Person den Nachweis erbringt, dass sie tatsächlich die ist, für die sie sich ausgibt. Dies geschieht in der Regel durch Vorlage eines amtlichen Ausweispapiers mit Foto (z.B. Pass) oder – im elektronischen Bereich – mit Hilfe der elektronischen Signatur.

[22] Die „zweifelsfreie Identifizierung“ sollte nicht mit Hilfe von Kennziffern vorgenommen werden, die in anderen Zusammenhängen oft benutzt werden, wenn nicht besondere Garantien eingebaut werden, um die Möglichkeit der Herstellung von Querverbindungen auszuschließen (vgl. Artikel 8 Absatz 7 der Richtlinie).

[23] In Frankreich soll ein erster Test mit einer elektronischen Patientenakte anlaufen, bei dem mit einer speziellen Kennung gearbeitet wird; es steht jedoch noch nicht fest, ob dieses System bei der endgültigen Version des EPA beibehalten wird.

[24] So könnte beispielsweise der Zugang zu Daten über eine psychiatrische Behandlung zunächst nur für Psychiater erlaubt sein oder es könnte ein spezielles Medikationsmedul eingerichtet werden, auf das Apotheker zugreifen können, ohne dass sie die übrigen Teile der elektronischen Patientenakte einsehen können.

b) Besondere Zugangskontrollen unter Mitwirkung des Patienten:

Wann immer in der Praxis durchführbar, d.h. sofern der Patient präsent und handlungsfähig ist, sollte ihm die **Möglichkeit** gegeben werden, **den Zugang zu seinen EPA-Daten zu verweigern, wenn er es denn so will**. Hierzu muss er im Vorfeld wissen, wer wann warum auf seine Daten zugreifen will und welche Folgen eine Zugangsverweigerung haben könnte. Für die Einwilligung in die Abfrage der Daten müssen Verfahren entwickelt werden, die keinen unzumutbaren psychologischen Druck auf den Patienten ausüben.

Wo ein **Nachweis** erforderlich ist, dass der Patient dem Zugriff auf seine EPA-Daten zugestimmt hat, muss es auch zuverlässige Instrumente geben, die einen solchen Nachweis liefern, wie z.B. die elektronische Überprüfung der Kennung des Patienten oder – wenn solche Instrumente bereits generelle Anwendung finden – die elektronische Signatur o.ä.. Die Vorlage eines solchen Nachweises muss elektronisch dokumentiert werden, um später überprüft werden zu können.

Ferner sollte geregelt werden, ob die betroffene Person das Recht haben soll zu verlangen, dass bestimmte Daten nicht in ihre elektronische Akte aufgenommen werden. Eine mögliche Lösung dieses Problems könnten "versiegelte Umschläge" sein, die sich ohne Zutun der betroffenen Person nicht öffnen lassen.

c) Zugriff der betroffenen Personen auf die Daten in ihrer elektronischen Patientenakte:

Ob die Patienten einen **direkten (elektronischen) Zugriff** auf ihre EPA zu Konsultationszwecken erhalten sollen, ist eine Frage der medizinischen Machbarkeit. Das den Betroffenen nach Datenschutzgrundsätzen zustehende Auskunftsrecht (z.B. gemäß Artikel 12 der Richtlinie 95/46/EG) muss nicht zwangsläufig mit einem Recht auf *Direkt*zugang verbunden sein. Ein direkter Zugang kann jedoch das Vertrauen in ein EPA-System erheblich stärken. Aus Sicht des Datenschutzes wäre die Vorbedingung für die Gewährung eines direkten Zugangs eine sichere elektronische Personenidentifizierung und –Authentisierung, um zu verhindern, dass sich Unbefugte Zugang zu den Daten verschaffen können.

Die Frage, ob Patienten selber die Daten in ihre elektronische Patientenakte eingeben sollen oder ob die medizinische Fachkraft dies für sie übernehmen soll, muss ebenfalls in den Vorschriften zum EPA-System geregelt werden. Eine angemessene Transparenz im Hinblick auf die Protokoll-Routinen, die den Urheber der Einträge in eine EPA kenntlich machen, würde mögliche Probleme hinsichtlich der Verlässlichkeit der Daten höchstwahrscheinlich ausräumen. Ebenso wäre es denkbar, den Zugang zu Eingabezwecken auf ein bestimmtes Modul in einer EPA zu beschränken.

In diesem Zusammenhang müssen ebenfalls das Leistungsvermögen und die besonderen Bedürfnisse von chronisch Kranken, älteren Menschen und Behinderten berücksichtigt werden.

4. Verwendung der EPA für andere Zwecke

Die Akzeptanz der EPA-Systeme in der Bevölkerung wird von ihrem **Vertrauen in die Vertraulichkeit des Systems** abhängen.

Die Begründung für einen rechtmäßigen Zugang zu Daten in einer elektronischen Patientenakte sollte die gleiche sein, mit der Zweck des EPA-Systems im Wesentlichen begründet wird, nämlich erfolgreiche medizinische Behandlung durch verbesserte Information. **Die Datenschutzgruppe ist der Ansicht, dass der Zugang zu medizinischen Daten in einer elektronischen Patientenakte für andere Zwecke als die in Artikel 8 Absatz 3 genannten grundsätzlich verboten sein sollte.**

Dies würde beispielsweise den EPA-Zugang von praktischen Ärzten, die als Sachverständige für Dritte arbeiten, z.B. für private Versicherungsunternehmen, bei Gericht, für Arbeitgeber usw., ausschließen. Außerdem sollte die Standesordnung für medizinische Fachkräfte so beschaffen sein, dass Zuwiderhandlungen wirksam bekämpft werden.

Durch spezielle Maßnahmen sollte auf jeden Fall verhindert werden, dass Patienten widerrechtlich dazu veranlasst werden, ihre EPA-Daten offenzulegen, z.B. auf Aufforderung eines möglichen künftigen Arbeitgebers oder einer Versicherungsgesellschaft. Um zu verhindern, dass sie derartigen Aufforderungen nachgeben, die nach den datenschutzrechtlichen Bestimmungen unzulässig sind, ist es wichtig, die Patienten über ihre Rechte aufzuklären. Eventuell müssen auch technische Mittel zum Einsatz kommen, z.B. besondere Anforderungen an einen Komplettausdruck der EPA.

Die Verarbeitung von EPA-Daten zum Zwecke der **medizinischen Forschung und der Erstellung von Statistiken** im öffentlichen Auftrag könnte ausnahmsweise gestattet werden, wenn die Ausnahmen mit den Bestimmungen der Richtlinie im Einklang stehen (vgl. Artikel 8 Absatz 4 mit dem dazu gehörigen Erwägungsgrund 34): Sie müssen somit vom Gesetzgeber für bestimmte, im voraus festgelegte Zwecke vorgesehen werden, wobei zum Schutz der Grundrechte und der Privatsphäre des Einzelnen der Grundsatz der Verhältnismäßigkeit gewahrt sein muss („geeignete besondere Garantien").

Wann immer möglich, sollten Daten aus EPA-Systemen für andere Zwecke (Statistik, Qualitätsbewertung) nur in anonymisierter oder zumindest in pseudonomysierter Form[25] verwendet werden.

5. Organisationsstruktur eines EPA-Systems

Bei der Diskussion über die verschiedenen organisatorischen Möglichkeiten der Speicherung von Daten in einer elektronischen Patientenakte werden in der Regel folgende Alternativen genannt:

- EPA als System, bei dem der Zugang zu den medizinischen Aufzeichnungen über die medizinische Fachkraft erfolgt, der zur Speicherung der Behandlungsdaten seiner Patienten verpflichtet wird – auch oft als „**dezentrale Speicherung**" bezeichnet, oder
- EPA als einheitliches Speichersystem, an das die medizinischen Fachkräfte ihre Unterlagen weitergeben müssen – gemeinhin auch als „**zentrale Speicherung**" bezeichnet oder
- als dritte Alternative ein System, bei dem der Patient „Herr" über seine Krankenakte bleibt, indem die **Eingabe der medizinischen Daten des Patienten unter dessen Aufsicht über einen speziellen elektronischen Dienst** erfolgt, und bei dem ihm eventuell sogar das Recht eingeräumt wird zu entscheiden, welche Daten in die Akte aufgenommen werden und welche nicht[26].

a) Die dritte Möglichkeit (**Speicherung unter Aufsicht des Patienten**) ist im Hinblick auf das Selbstbestimmungsrecht des Patienten sicherlich die beste Lösung; was die Qualität – sprich die Richtigkeit und Vollständigkeit - der Aufzeichnungen betrifft, könnte es allerdings

[25] Pseudonymisierung bedeutet, dass ein Identifikationsmerkmal (Name, Geburtsdatum usw.) durch eine neue Bezeichnung ersetzt wird, vorzugsweise durch Verschlüsselung, sodass der Empfänger der Information die betreffende Person nicht identifizieren kann.

[26] Dies ist das französische Modell, das derzeit gerade eingerichtet wird. Die Dienstleister heißen „hébergeurs"; ihre Stellung regelt ein Dekret, das zuvor der französischen Datenschutzkommission (Commission Nationale de l'Informatique et des Libertés – CNIL) zur Stellungnahme vorgelegt wurde. Das Dekret geht ausführlich auf Fragen der Zulassung dieser Dienstleister und der Sicherheit des Systems ein.

Probleme geben, wenn der Patient allein – ohne das Korrektiv einer medizinischen Fachkraft - entscheidet, welche Daten in seiner EPA vorgehalten werden.

b) Beim "**dezentralen Speichersystem**", das überhaupt erst durch die Einrichtung entsprechender Suchpfade zu einem System wird, bliebe die bisherige Struktur der Dokumentation von Krankendaten bei den verschiedenen Anbietern medizinischer Leistungen unangetastet. Inwieweit die Patientendaten in einem solchen System auffindbar sind, hängt von der Qualität des Suchsystems ab.

Bei diesem Organisationsmodell **behält die medizinische Fachkraft/Einrichtung die Kontrolle** über die Patientenakte (bzw. genauer gesagt über den von ihr angelegten Teil der EPA). Wegen der komplexen Architektur dieses Systems müsste eventuell eine zentrale Stelle eingerichtet werden, die die Lenkung und Überwachung des gesamten Systems übernimmt und auch für die datenschutzrechtliche Konformität des Betriebs des Systems sorgt. Nützlich wäre möglicherweise auch die Einrichtung einer zentralen Meldestelle für Datenschutzprobleme, an die sich die Patienten wenden könnten, anstatt unter einer Vielzahl von für die Verarbeitung verantwortlichen Personen oder Einrichtungen die richtige finden zu müssen.

c) Der Hauptvorteil eines sogenannten **zentralen Speichersystems** wäre wahrscheinlich die geringere Anfälligkeit für technische Probleme und die Rund-um-die-Uhr-Verfügbarkeit, die bei einem unterhalb der Krankenhausebene angesiedelten EPA-System nicht so ohne weiteres gewährleistet wäre. Es gäbe für das gesamte System einen einzigen Datenverarbeiter, der die Daten von den medizinischen Fachkräften/Einrichtungen entgegennimmt, die ihre Dokumentation (einzelnen oder als Paket) an das Zentralsystem schicken.

Gegen ein solches zentrales Speichersystem könnte aus datenschutzrechtlicher Sicht das höhere Missbrauchsrisiko sprechen. Man könnte jedoch besondere Sicherheitsvorkehrungen treffen (z.B. verschlüsselte Speicherung), um die Sicherheitsrisiken zentral vorgehaltener Daten zumindest bis zu einem gewissen Grad in Grenzen zu halten. Damit wird jedoch die Verantwortung dafür, dass die in dem System gespeicherten Daten vertraulich behandelt werden, dem medizinischen Personal aus den Händen genommen, was sich auf die Vertrauenswürdigkeit des Systems für die Patienten negativ auswirken könnte.

Inwieweit die Patienten Inhalt und Weitergabe ihrer elektronischen Patientenakte beeinflussen können, hängt in beiden Fällen – beim dezentralen und beim zentralen System – von der Architektur des Systems ab (siehe Punkt 3 b).

6. In EPA gespeicherte Datenkategorien und Art ihrer Präsentation

Der eigentliche Sinn und Zweck eines EPA-Systems besteht darin, sämtliche die Gesundheit betreffenden Daten einer bestimmten Person zu erfassen, die für ihren langfristigen Gesundheitszustand aller Voraussicht nach von Belang sind, damit im Falle einer etwaigen späteren Behandlung umfassende sachdienliche Informationen zur Verfügung stehen, durch die die Chancen einer erfolgreichen Behandlung der Patienten steigen.

Für die Datenschutzgruppe ist ein solches System hauptsächlich mit folgenden Problemen behaftet:

a) Die „**Vollständigkeit" einer Patientenakte** ist praktisch unmöglich und auch nicht wünschenswert: **In die Akte sollen ausschließlich *erhebliche* Informationen aufgenommen werden**. Eine der schwierigsten Fragen, die es beim Aufbau eines EPA-Systems zu beantworten gilt, ist daher, welche Arten medizinischer Daten in eine elektronische Patientenakte aufgenommen werden und wie lange sie darin gespeichert bleiben sollen[27].

[27] Es gibt Datenkategorien, die für den Rest des Lebens eines Patienten wichtig sind (z.B. Allergien), aber

Auch wenn diese Frage in erster Linie von Fachleuten auf dem Gebiet der Medizin zu beantworten ist, so hat sie doch auch eine datenschutzrechtliche Dimension: Gemäß den Grundsätzen der Erheblichkeit und Verhältnismäßigkeit der Datenerfassung, muss sich die Sammlung von Daten auf jene Daten beschränken, die für den Verarbeitungszweck erheblich sind, und sie darf auch nicht darüber hinaus gehen (Artikel 6 Absatz 1 Buchstabe c der Richtlinie). Die Rechtmäßigkeit von EPA-Systemen wird daher davon abhängen, ob eine angemessene Lösung bei der Wahl der 'richtigen' Datenkategorien und der 'richtigen' Zeitspanne für die Speicherung der Informationen in einer EPA gefunden wird.

b) Präsentation der Daten in der EPA: Da sich die Gesundheitsdaten in verschiedene Kategorien einteilen lassen, die ein recht unterschiedliches Maß an Vertraulichkeit erfordern, würde es sich im Grunde anbieten, innerhalb eines EPA-Systems verschiedene **Datenmodule** mit unterschiedlichen Zugangsvoraussetzungen einzurichten: Ein „Impfmodul“ zum Beispiel sollte für die betroffene Person jederzeit zugänglich sein und könnte auch einem größeren Kreis von Mitarbeitern im Gesundheitsdienst zugänglich gemacht werden. Für Apotheker könnte ein „Medikationsmodul“ eingerichtet werden, auf das mit Zustimmung des Patienten zugegriffen werden kann[28]. Für den Zugang zu einem „Notfallmodul“ könnte es eine spezielle technische Lösung geben. Sinnvoll wäre auch die Einrichtung von speziellen „Benachrichtigungssystemen“, die den Patienten automatisch auf anstehende Impfungen, routinemäßige Überprüfungen des Gesundheitszustandes oder Nachuntersuchungen aufmerksam machen würden.

Besonders sensible Daten könnten durch Speicherung in speziellen Modulen mit besonders strengen Zugangsvoraussetzungen besser geschützt werden. Beispiele hierfür wären Daten über eine psychiatrische Behandlung oder Abtreibung. Anstatt solche Daten aus der elektronischen Patientenakte herauszunehmen – was sich negativ auf künftige Behandlungen auswirken könnte, sollten besondere Zugangsbeschränkungen in das System eingebaut werden, wozu unter anderem auch die ausdrückliche Einwilligung des Patienten sowie besondere technische Schranken (z.B. „versiegelte Umschläge“) gehören.

c) Bei der strukturellen Gestaltung der EPAs sollten auch spezielle Auskunftsersuchen, die von Zeit zu Zeit anfallen können, mit berücksichtigt werden. Ein Beispiel: Nach nationalem Recht können private Versicherungsunternehmen (bis zu einem gewissen Grad) Anspruch auf Auskunft über Krankendaten haben, wenn sie diese Daten für die Erfüllung ihrer vertraglichen Verpflichtungen gegenüber dem Versicherungsnehmer benötigen. Dass private Versicherungsunternehmen Zugang zu einer elektronischen Patientenakte erhalten, dürfte wohl ausgeschlossen sein. Eine mögliche Lösung wäre daher die Erstellung einer speziellen „Standarddokumentation“, die gegebenenfalls den legitimen Informationsinteressen des Versicherers gerecht wird und den privaten Versicherungsunternehmen mit Zustimmung des Patienten elektronisch übermittelt werden könnte.

7. Übermittlung medizinischer Daten in Drittländer

Die elektronische Verfügbarkeit medizinischer Daten in EPA-Systemen kann zu einer deutlichen Verbesserung der Diagnose- und Behandlungsmöglichkeiten führen, weil auf diese Weise medizinischer Sachverstand, der nur in einer medizinischen Einrichtung außerhalb der EU vorhanden ist, in Anspruch genommen werden kann. Bei der Hinzuziehung ausländischer Sachverständiger zu Diagnosezwecken muss die Identität des Patienten nicht unbedingt offen gelegt werden. Deshalb sollten Daten in Länder außerhalb der Europäischen Union/des Europäischen Wirtschaftsraums nur in **anonymisierter oder zumindest pseudonomysierter**

---

auch solche, die nur kurzfristig von Bedeutung sind, z.B. die Unvereinbarkeit bestimmter Behandlungen.

[28] Ein Medikationsmodul in einer EPA hätte außerdem den Vorteil, dass sich der behandelnde Arzt ebenfalls einen Überblick über die gesamte Medikationsgeschichte eines Patienten verschaffen könnte.

Form weitergeleitet werden. Fehlt die ausdrückliche Einwilligung der betroffenen Person in die Übermittlung der personenbezogenen Daten[29], könnte so das Problem der Einholung der Erlaubnis für den Datentransfer umgangen werden, da die Identität für den Adressaten unbekannt bleibt.

Wegen des hohen Risikos, dem personenbezogene Daten in einem EPA-System in einer Umgebung ohne angemessenen Schutz ausgesetzt sind, weist die Datenschutzgruppe nachdrücklich darauf hin, dass jede Verarbeitung – vor allem die Speicherung – von EPA-Daten in Rechtsräumen stattfinden muss, die die EU-Datenschutzrichtlinie oder andere angemessene Rechtsvorschriften anwenden.

Ein besonderes Problem sind die grenzüberschreitenden Datenströme im Verlauf klinischer Studien: Es kann sein, dass die Wissenschaftler, die direkt mit den Patienten zu tun haben, gelegentlich Zugang zu den EPA-Daten in ihrer personalisierten Form benötigen. Mindestvoraussetzung für jeden Transfer von aus klinischen Studien hervorgegangenen Daten an die Auftraggeber oder an sonstige rechtmäßig beteiligte Einrichtungen muss jedoch eine einwandfreie Pseudonomysierung sein, besonders dann, wenn sich die Auftraggeber in Ländern ohne angemessenes Schutzniveau befinden.

Aspekten der Datensicherheit sollte in diesem Zusammenhang stets ganz besondere Aufmerksamkeit geschenkt werden, um der Gefahr der unzulässigen Weitergabe an Umgebungen, die vom Standpunkt des Datenschutzes aus unter Umständen nicht sicher sind, aus dem Weg zu gehen.

8. Datensicherheit

Die Akzeptanz eines mit extrem hohen Risiken behafteten Datenverarbeitungssystems hängt davon ab, ob ein entsprechend hohes Maß an Datensicherheit für sämtliche Aspekte des Systems gewährleistet ist. Der **Zugriff durch Unbefugte muss faktisch unmöglich sein** und von vornherein unterbunden werden, wenn das System aus Sicht des Datenschutzes annehmbar sein soll. Für Befugte muss das System dagegen praktisch unbegrenzt zugänglich sein, sobald ein echter Informationsbedarf besteht, wenn die Vorteile, die man sich von dem System für die medizinische Versorgung der Patienten erhofft, tatsächlich eintreten sollen.

Der ordnungspolitische Rahmen für die Einführung eines EPA-Systems müsste eine Reihe von Maßnahmen technischer und organisatorischer Natur vorsehen, mit denen der Verlust oder die Veränderung und Verarbeitung der Daten in einem EPA-System durch Unbefugte sowie der unberechtigte Zugriff auf die Daten verhindert werden können. Die Sicherheit des Systems muss mit Hilfe des aktuellen Wissenstands und der neuesten Techniken im Bereich der Informatik und Informationstechnik gewährleistet werden.

Soweit irgend möglich, sollten daher **datenschutzfreundliche Technologien (Privacy Enhancing Technologies - PETs)**[30], zum Einsatz kommen. Die Verschlüsselungstechnik sollte nicht nur für den Transfer, sondern auch zur Speicherung der Daten in EPA-Systemen verwendet werden. Alle getroffenen Sicherheitsvorkehrungen sollten benutzerfreundlich sein, damit sie möglichst breite Anwendung finden. Die dadurch verursachten Kosten sollten als Investition in die Vereinbarkeit von EPA-Systemen mit den Grundrechten betrachtet werden, denn dies wird eine der wichtigsten Vorbedingungen für den Erfolg der Systeme sein.

---

[29] In Situationen, in denen der Patient physisch nicht in der Lage ist, seine Einwilligung zu geben (z.B. weil er im Koma liegt), könnten seine Daten dennoch gemäß Artikel 26 Absatz 1 Buchstabe e in Drittländer ohne angemessenes Datenschutzniveau weitergegeben werden, wenn lebenswichtige Interessen des Patienten dies erfordern. .

[30] Zu PETs siehe Ziffer 4.3 des Berichts der Kommission - Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46), KOM(2003) 265 endg.

Auch wenn viele der vorstehend erörterten Schutzvorrichtungen bereits Datensicherungselemente enthalten, ist es wichtig, dass der ordnungspolitische Rahmen zum Zwecke des Datenschutzes folgende besondere Maßnahmen vorsieht:

- die Entwicklung eines zuverlässigen, effektiven elektronischen Identifizierungs- und Authentisierungssystems und von laufend aktualisierten Registern, anhand deren sich nachprüfen lässt, ob die Personen, die Zugang zum EPA-System haben oder beantragen, tatsächlich hierzu befugt sind;
- ausführliche Protokollierung und Dokumentierung sämtlicher Verarbeitungsschritte, die im System stattgefunden haben, vor allem bei Anträgen auf Zugang zu Konsultations- oder Eingabezwecken, in Verbindung mit regelmäßigen internen Überprüfungen der Berechtigungen und den entsprechenden Folgemaßnahmen;
- wirksame Vorrichtungen zur Sicherung und Wiederherstellung des Inhalts der EPA-Systeme,
- Verhinderung des Zugriffs auf EPA-Daten oder der Änderung der Daten durch unberechtigte Personen zum Zeitpunkt ihres Transfers oder ihrer Speicherung zu Sicherungszwecken, z.B. durch kryptographische Algorithmen,
- klare, genau festgelegte Anweisungen für alle zugangsberechtigte Personen, in denen dargelegt wird, wie von den EPA-Systemen ordnungsgemäß Gebrauch gemacht wird und wie Sicherheitsrisiken und Verstöße gegen die Sicherheitsvorschriften vermieden werden können,
- klare Abgrenzung der Funktionen und Befugnisse der Personen, die für das System verantwortlich sind oder zumindest daran mitwirken, im Hinblick auf Haftungsfragen bei Unzulänglichkeiten,
- regelmäßiges internes und externes Datenschutz-Audit.

9. Transparenz

Eine elektronische Patientenakte verbessert zweifellos die Möglichkeiten der medizinischen Versorgung, bietet aber gleichzeitig auch viel Raum für Missbrauch, wenn sich Unbefugte Zugang zu dem System verschaffen. Um Vertrauen in das System haben zu können, werden die öffentliche Meinung und der einzelne Nutzer daher **in Bezug auf Inhalt und Funktionsweise eines EPA-Systems ein besonders hohes Maß an Transparenz** einfordern. Der oder die für das System Verantwortlichen müssen daher den Datenschutzbehörden ihre Verarbeitungen **melden** und außerdem **spezielle Informationen** bereitstellen, die **leicht zugänglich und allgemein verständlich** sind. Um die nötige Transparenz hinsichtlich der nationalen EPA-Systeme herzustellen, bietet es sich an, die Vorteile des Internet für die Informationsverbreitung zu nutzen.

Durch kostenlose, leicht zu handhabende und dennoch sichere Zugangspunkte, über die sich die betroffenen Personen über Inhalt und Weitergabe ihrer EPA informieren können, ließen sich die Transparenz und damit das Vertrauen in das System ebenfalls erhöhen.

10. Haftung

Ein EPA-System muss auch die Gewähr bieten, dass **etwaige Verletzungen der Privatsphäre** infolge der Speicherung und Bereitstellung von Krankendaten in einem EPA-System durch einen **Anspruch auf Ersatz des** beispielsweise durch falsche oder unzulässige Nutzung der EPA-Daten entstandenen **Schadens** in angemessener Weise wiedergutgemacht werden.

Im Rahmen einer Analyse der mit EPA-Systemen verbundenen datenschutzrechtlichen Probleme können Fragen der Haftung bei falschem Gebrauch eines EPA-Systems nur gestreift werden. Nach Ansicht der Datenschutzgruppe sollte ein Mitgliedstaat, der ein EPA-System einführen möchte, vorher eine sorgfältige Analyse der zivil- und arztrechtlichen Aspekte und Folgen eines solchen Vorhabens vornehmen lassen, um zu klären, welche neuen Haftungsfragen hieraus möglicherweise erwachsen, z.B. die Frage der Haftung für die Richtigkeit und Vollständigkeit der EPA-Einträge, die Frage, wie ausführlich eine medizinische Fachkraft, die einen Patienten behandelt, die EPA studieren muss oder die haftungsrechtlichen Folgen für den Fall, dass aus technischen Gründen nicht auf das System zugegriffen werden kann usw.

11. Kontrollmechanismen für die Verarbeitung von EPA-Daten

Da die Einführung von EPA-Systemen mit **besonderen Risiken** verbunden ist, bedarf es **effizienter Kontrollmechanismen** zur Bewertung der bestehenden Schutzvorrichtungen. Augrund der Komplexität der Informationen in einer elektronischen Patientenakte und der Vielzahl der potenziellen Nutzer besteht möglicherweise Bedarf an neuen Verfahren im Zusammenhang mit den Zugangsrechten der betroffenen Personen:

a) Für Streitigkeiten über die korrekte Nutzung der Daten in einem EPA-System sollte ein **besonderes Schiedsverfahren** eingeführt werden. Das Verfahren sollte für die betroffenen Personen unkompliziert und gebührenfrei sein. Da in der Regel ärztlicher Sachverstand benötigt wird, um zu beurteilen, ob Informationen in einem EPA-System falsch oder unnötigerweise verarbeitet wurden, dürfte die Datenschutzbehörde nicht die beste Wahl sein, um sich mit solchen Beanstandungen zu befassen, zumindest nicht in erster Instanz. Öffentliche „Patientenanwälte“ könnten sich dort, wo es sie bereits gibt, dieser Aufgabe annehmen.

b) Ein EPA-System muss gewährleisten, dass die betroffene Person ihre Auskunftsrecht ohne größere Schwierigkeiten ausüben kann. Grundsätzlich ist die für die Verarbeitung verantwortliche Person diejenige, die Auskunft geben muss. **EPA-Systeme sind** jedoch **Systeme, in denen die Informationen** vieler verschiedener Datenverarbeiter **zusammenfließen**. In diesen Systemen, an denen viele für die Verarbeitung verantwortliche Personen mitwirken, müssen die betroffenen Personen eine **einzige spezielle Stelle** als Ansprechpartner haben, **die für die ordentliche Bearbeitung der Anträge zuständig ist**. Da eine elektronische Patientenakte, wenn denn ihre Möglichkeiten erst einmal voll genutzt werden, ein äußerst komplexes Gebilde ist und da die Patienten Vertrauen in das System haben müssen, ist es wichtig, dass die Patienten, dessen Daten in einem EPA-System verarbeitet werden, wissen, wie sie einen zuständigen Ansprechpartner erreichen, mit dem sie mögliche Unzulänglichkeiten des Systems besprechen können. In Rechtsvorschriften über EPA-Systeme muss es hierzu daher eine spezielle Regelung geben.

c) Als vertrauensbildende Maßnahme könnte eine spezielle Routine eingeführt werden, mit der die betroffene Person darüber unterrichtet wird, wann wer auf ihre elektronische Patientenakte zugegriffen hat. Wenn die betroffenen Personen in regelmäßigen Abständen ein Protokoll mit einer Liste der Personen oder Einrichtungen erhielten, die sich Zugang zu ihrer Datei verschafft haben, könnten sie sich sicher sein, dass sie wissen, was mit ihren Daten in dem EPA-System geschieht.

d) Es muss ein regelmäßiges internes und externes Audit von Zugangsprotokollen durch Datenschutzbeauftragte durchgeführt werden. Das bereits genannte jährliche Protokoll für die betroffenen Personen wäre eine zusätzliche effektive Maßnahme zur Überprüfung der rechtmäßigen Verwendung von EPA-Daten. Wenn es in Krankenhäusern, die an das EPA-

System angeschlossen sind, Datenschutzbeauftragte gäbe, würde sich die Wahrscheinlichkeit der korrekten Verwendung der Daten in diesen Systemen sicherlich erhöhen.

IV. FAZIT

Jeder Bürger und jeder Patient hat ein Recht auf Schutz seiner Privatsphäre und darf somit zu Recht erwarten, dass die Vertraulichkeit und der Schutz seiner persönlichen Daten von allen medizinischen Fachkräften konsequent gewahrt wird. Dies gilt auch für die Systeme zur elektronischen Speicherung von Patientendaten (EPA).

Die Artikel 29-Datenschutzgruppe will mit dieser Arbeitsunterlage eine Interpretationshilfe zu den auf EPA-Systeme (elektronische Patientenakten – EPA) anwendbaren Datenschutzbestimmungen geben und einige allgemeine Grundprinzipien formulieren. Außerdem soll abgeklärt werden, welche Vorbedingungen bei der Einrichtung von EPA-Systemen erfüllt sein und welche Schutzgarantien diese Systeme bieten müssen, und es soll damit überdies ein Beitrag zur einheitlichen Anwendung der nach Maßgabe der Richtlinie 95/46/EG erlassenen einzelstaatlichen Maßnahmen geleistet werden.

Die Datenschutzgruppe weist nachdrücklich darauf hin, dass die Einrichtung und der Betrieb von EPA-Systemen in völliger Übereinstimmung mit den Grundsätzen des Datenschutzes, wie sie in der Richtlinie 95/46/EG verankert sind, erfolgen muss. Sie ist der Auffassung, dass die Einhaltung dieser Grundsätze den beteiligten Personen und Einrichtungen dabei hilft, das ordentliche Funktionieren derartiger Systeme sicherzustellen. Außerdem ist es ihrer Ansicht nach unabdingbar, dass EPA-Systeme ungeachtet ihrer Rechtsgrundlage vor dem Hintergrund solider, gesetzlich verankerter Datenschutzgarantien eingerichtet und betrieben werden.

Die Artikel 29-Datenschutzgruppe fordert die Ärzteschaft und Angehörigen der Heilberufe sowie alle sonstigen Mitarbeiter und Einrichtungen, die medizinische Dienstleistungen erbringen, und die breite Öffentlichkeit auf, sich zu dem vorliegenden Arbeitspapier zu äußern[31].

Da die Entwicklung in diesem Bereich stetig voranschreitet, ist nicht auszuschließen, dass die Datenschutzgruppe weitere Kommentare abgibt oder sonstige Folgemaßnahmen ergreift.

Brüssel, den 15. Februar 2007

Für die Datenschutzgruppe
Der Vorsitzende

---

[31] Ihre Kommentare zu dem Arbeitspapier richten Sie bitte an folgende Anschrift: Sekretariat der Artikel-29-Datenschutzgruppe

Europäische Kommission, Generaldirektion Justiz, Freiheit und Sicherheit

Referat C.5 - Datenschutz

Büro: LX 46 1/43

B-1049 Brüssel

E-Mail-Adresse: Amanda.JOYCE-VENNARD@ec.europa.eu ; Fax: +32-2-299 80 94
Sofern nicht ausdrücklich um vertrauliche Behandlung gebeten wird, werden alle Stellungnahmen, ob von öffentlicher oder privater Seite, auf der Website der Datenschutzgruppe veröffentlicht.

Peter SCHAAR