

Chancen und Risiken zentralisierter Patienten – Datenbestände

Zentraler Datenpool der Krankenversicherung

Elektronischer Patientenpass und zentraler Rechner

Vortrag anlässlich des 11. Hessischen Datenschutzforums am 19. September 2002 in

Wiesbaden

Reinhard Vetter, Bayer. Landesbeauftragter für den Datenschutz

(Anrede)

lassen sie mich zunächst auf einige **Grundsätze** eingehen:

Was bedeutet Datenschutz?

- Datenschutz bedeutet in erster Linie Schutz des Rechtes des Menschen, grundsätzlich selbst zu entscheiden, wer was über ihn weiß und was er mit diesem Wissen anfängt.

Dieses Recht ergibt sich nach dem Volkszählungsurteil des Bundesverfassungsgerichts aus den Grundrechten der Menschenwürde und der Handlungsfreiheit des Menschen.

- In dieses Recht darf nur auf der Grundlage eines Gesetzes im überwiegenden Allgemeininteresse eingegriffen werden.

- Ein Eingriff liegt nicht vor, wenn der Betroffene in voller Kenntnis der beabsichtigten Datenverarbeitung ohne Zwang, d.h. freiwillig, einwilligt.

Von Freiwilligkeit kann nur die Rede sein, wenn der Betroffene Alternativen zur Einwilligung hat.

- Geschützt sind schließlich nur solche Informationen, die einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Anonymisierte Daten unterfallen daher nicht dem Datenschutz.

Datenschutz kann auch durch Pseudonymisierung, d.h. durch Codierung dergestalt realisiert werden, dass die Informationen zwar individualisiert bleiben, aber ohne Referenzangaben nicht mehr einer bestimmten Person zugeordnet werden können.

Welche Risiken ergeben sich nun aus einem zentralen Datenpool der gesetzlichen Krankenversicherungen?

Nach der **bisherigen Rechtslage** ^[VR1]– die allerdings für die **Disease – Management – Programme** bereits wesentlich **geändert** wurde - war es aus gutem Grund ausgeschlossen, dass die gesetzlichen Krankenkassen vollständige Krankheitskonten ihrer Versicherten aufbauten. Die Vorschrift des **§ 295 Abs. 2 SGB V** verhinderte die Übermittlung von Diagnosen niedergelassener Ärzte an die Krankenkassen^[VR2].

Dadurch wurde einmal dem Grundsatz Rechnung getragen, dass keine nicht erforderlichen Daten an die Krankenkassen gehen, zum anderen wurden dadurch die Risiken einer zentralen Speicherung sensibler Daten schon auf der Ebene der einzelnen Kasse vermieden.

Ein Datenpool für die Versicherten [VR3] aller gesetzlichen Krankenkassen, mit den vollständigen Krankheitsdaten von ca. 90 % Prozent der deutschen Bevölkerung, enthielte dagegen ein großes Gefährdungspotential [VR4].

Abgesehen davon, dass es der einzelne vielleicht gar nicht will, dass seine Krankenkasse alles medizinische über ihn weiß, noch weniger eine zentrale Organisation, würden durch einen solchen Datenbestand die Voraussetzungen für Risikoselektion geschaffen werden. Ich sage nicht, dass solche Absichten jetzt bestehen. Wenn aber einmal das Datenmaterial für solche Entscheidungen vorliegt, wird die Versuchung dafür doch größer.

Dieses personenbezogene Datenmaterial könnte durch Entscheidung des Gesetzgebers auch für weitere Zwecke nutzbar gemacht werden, z.B. für die Verwendung durch andere Versicherungen wie Lebensversicherungen, aber auch durch Banken oder Arbeitgeber. Ich sage nicht, dass solche Absichten jetzt bestehen, aber wiederum muss ich darauf hinweisen, dass solche Datenbestände große Begehrlichkeiten auslösen könnten und wahrscheinlich auch würden.

Auch darüber hinaus würde ein solcher Riesenbestand sensibler Daten ein großes **Missbrauchsrisiko** beinhalten: Ungetreue Mitarbeiter könnten Informationen nach draußen geben, die für den Einzelnen größten Schaden bedeuten können, z.B. an Versicherungen, an Arbeitgeber, bei entsprechendem Interesse auch an die Öffentlichkeit. Hacker könnten von außen eindringen, Schäden verursachen und Daten missbrauchen.

Damit wir uns richtig verstehen, ich will hier nichts unterstellen. Ich will aber darauf hinweisen, dass mit der Größe solcher Datenbestände und mit der Sensibilität solcher Daten auch die Risiken für den Missbrauch wachsen.

Absichten der Politik, zur Verbesserung der "Daten-Transparenz im Gesundheitswesen" einen Pool mit Patientendaten [VR5] zu schaffen, müssen deshalb kritisch hinterfragt werden. Kritisch hinterfragt zum einen, ob das wirklich erforderlich ist.

Die Kassenzahnärztliche Bundesvereinigung verneint dies dezidiert.

Als Datenschutzbeauftragter muss ich aber auch Argumente vorbehaltlos überprüfen, die für **ein überwiegendes Interesse** der Allgemeinheit an einem solchen Datenpool sprechen.

Hier ist die Haltung **des Bundesgesundheitsministeriums nicht von der Hand** zu weisen:

Danach ist ein Pool von Leistungsdaten der medizinischen Versorgung für die **Weiterentwicklung der gesetzlichen Krankenversicherung erforderlich.** Mit der Analyse von Behandlungsabläufen sollen die **Wirtschaftlichkeit und Qualität verbessert, Über-, Unter- und Fehlversorgung korrigiert und schließlich die Krankenhausversorgung optimiert werden können.**

Ich muss anerkennen, dass die derzeitige **Aufsplitterung der Abrechnungen auf verschiedene Leistungssektoren und auf eine Vielzahl von Kassenärztlichen Vereinigungen und Krankenkassen eine valide Datenbasis für sektor- und kassenartenübergreifende Auswertungen verhindert.** Die Notwendigkeit einer solchen validen Datenbasis erscheint plausibel.

Ich frage aber, ist dafür tatsächlich die Vollerhebung und Speicherung notwendig? Reicht dafür nicht auch eine **genügend große Stichprobenerhebung**^[VR6]?

Auf keinen Fall müssen für die genannten Zwecke die einzelnen Krankheiten von **Herrn Mustermann, Wiesbaden, Königstraße 10**, bekannt sein.

Ich begrüße es deswegen, halte es aber auch für **zwingend notwendig**,

- dass **nur pseudonymisierte Daten** ^[VR7]vorgesehen sind,
- dass eine **Depseudonymisierung verfahrensmäßig ausgeschlossen** ^[VR8]sein soll,
- dass **Pseudonymisierung getrennt** ^[VR9]von der Krankenkasse erfolgen soll.

Dies alles muss aber **gesetzlich konkretisiert und abgesichert** ^[VR10]werden, nur dann ist Missbrauch weitestgehend ausgeschlossen.

Die **wichtigsten Forderungen der Datenschutzbeauftragten** sind deshalb:

- **Gesetzliche Regelung der einzelnen Aufbereitungszwecke**^[VR11]. Es darf nicht so sein, dass zunächst der Datenpool geschaffen wird, erst dann wird überlegt, was man alles damit machen kann.
- **Öffentl. Rechtsform und Konzeption als Träger des Sozialgeheimnisses** für ^[VR12]Vertrauensstelle und den "Datenpool"

- **Trennung** dieser Stellen von Krankenkassen, Kassenärztlichen Vereinigungen und ihrer Verbände [VR13]
- **Pseudonymisierung** auch der **Leistungserbringerdaten** [VR14].
- Technische und rechtliche **Absicherung des absoluten Re-Identifikationsverbots** durch Einwegpseudonyme und Gesetz [VR15].
- Zulassung **nur aggregierter Auswertungen**.

Das Thema "zentraler Rechner" ist auch für den **elektronischen Patientenpass bzw. die elektronische Gesundheitskarte** relevant. Zu diesem Komplex gibt es zahlreiche Modelle, auch schon einzelne Anwendungen in der Praxis für begrenzte Bereiche.

Ich gehe vom **Eckpunktepapier** des Bundesgesundheitsministeriums vom 12. März 2002 und von der "**Gemeinsamen Erklärung** des BMG und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen" vom 03. Mai 2002 aus [VR16].

Nach dem Eckpunktepapier sollen auf die **Krankenversichertenkarte zusätzlich weitere Funktionen** integriert werden. Von der bisherigen **Ausweisfunktion der KVK** sollen sie **informationstechnisch getrennt** werden.

Diese **Trennung** ist aus der Sicht des Datenschutzes eine **conditio sine qua non**. Sie ist unbedingt notwendig, da der Versicherte die Krankenversichertenkarte beim Arztbesuch vorlegen muss. Ohne die Trennung wäre von dieser Vorlagepflicht auch der übrige Inhalt der Karte umfasst, die Karte würde auch insoweit zur **Pflichtkarte**. Das wäre aber strikt abzulehnen, da damit der Patient seine **Hoheit über seine Gesundheitsdaten verlöre** [VR17].

Die Eckpunkte und die gemeinsame Erklärung enthalten darüber hinaus **wichtige Ansatzpunkte**, die aus der Sicht des Datenschutzes ebenfalls erforderlich sind.

Insbesondere besagt die gemeinsamen Erklärung ausdrücklich, dass mit dem Ausbau der KVK zu einer **Gesundheitskarte keine zentralen Patientendatensammlungen** [VR18]entstehen sollen.

Diese würden ein **hohes Gefährdungspotential** bedingen: Durch unbefugtes Eindringen auf den Server könnten größte Schäden entstehen, die Sammlung sensibelster Gesundheit- bzw. Krankheitsdaten könnte Begehrlichkeiten der verschiedensten Art auslösen, auf die ich oben bereits hingewiesen habe. Auch das Missbrauchsrisiko würde durch eine zentrale Speicherung vervielfacht.

Eine zentrale Speicherung müßte auch gewährleisten, dass Daten jeweils nur durch den explizit hierzu Berechtigten eingegeben und ausgelesen werden können. Dies wird technisch sicher darstellbar sein.

Ein interessanter zusätzlicher Aspekt darf dabei aber nicht übersehen werden: Für die klare Abgrenzung der Daten der verschiedenen Personen zueinander wird aus technischen Gründen ein **eindeutiges Ordnungsmerkmal** für die bestimmte Person erforderlich sein.

Dieses könnte sich als **Personenkennzeichen** erweisen. Eine weite Verbreitung solcher Gesundheitskarten mit zentraler Datenspeicherung hätte damit die Auswirkung, dass für einen großen Teil der Bevölkerung jedenfalls für einen solchen einzelnen Anwendungsbereich eine Art Personenkennzeichen entstünde.

Ich hielte es nicht für ausgeschlossen, dass sich daran von Seiten der **Politik Überlegungen** anschließen könnten, dieses Kennzeichen dann auch für andere Anwendungen nutzbar zu machen. Damit wäre der Schritt zur Einführung eines **allgemeinen Personenkennzeichens** getan, das nach der Rechtsprechung des Bundesverfassungsgerichts unzulässig wäre.

Schließlich wäre bei einer zentralen Speicherung der Krankheitsdaten bei einem **externen Dienstleister** der zwingend notwendige **strafrechtliche und strafprozessuale Schutz der Krankheitsdaten nicht gewährleistet**^[VR19]: Das Zeugnisverweigerungsrecht gilt nur für den behandelnden Arzt und seine ärztlichen Gehilfen, der Beschlagnahmeschutz besteht nur für die Daten, die sich im Gewahrsam des behandelnden Arztes oder einer Krankenanstalt befinden.

Fraglich ist, ob diese Nachteile zentraler Speicherung nicht durch eine ausreichende **Verschlüsselung der Daten abgemildert** oder ausgeschlossen werden könnten.

Theoretisch wäre das möglich unter der Voraussetzung, dass die Ver- und Entschlüsselung entweder ausschließlich durch den jeweils Berechtigten erfolgt bzw. angestoßen wird. Das würde bedeuten, dass entweder eine Vielzahl von Berechtigten die Verschlüsselung jeweils zuverlässig mit starken Verschlüsselungswerkzeugen bei sich lokal durchführen müßte.

Weiter wären die verschlüsselten Daten in die zentrale Datenbank zu übertragen.

Alternativ wäre auch ein Datenbanksystem denkbar, das über die erforderliche komplexe Funktionalität für den Schlüssel verfügt, der im jeweiligen Fall auf die einzelnen Daten anzuwenden wäre. Ob es solche Systeme derzeit gibt, entzieht sich meiner Kenntnis.

In jedem Fall wäre ein aufwendiges Schlüsselmanagement erforderlich.

Ich habe **starke Zweifel**, ob sich das alles mit der notwendigen hohen **Zuverlässigkeit** auf Dauer realisieren ließe.

Eine zentrale einheitliche **Verschlüsselung** der Daten durch den **Serverbetreiber** wäre auf jeden Fall **abzulehnen**, da er dann Zugriff auf die Daten nehmen könnte und Missbräuche nicht auszuschließen wären.

Im übrigen zeigen die "Eckpunkte" und noch mehr die gemeinsame Erklärung begrüßenswerte **Ansatzpunkte für eine datenschutzfreundliche Ausgestaltung**.

Das gilt besonders für das klare **Bekennnis zur Freiwilligkeit**^[VR20]. Ich halte das für die **zentrale Frage**. Das Recht, grundsätzlich selber über die Verwendung seiner personenbezogenen Daten zu bestimmen, wäre in seinem innersten Kern betroffen, wenn Gesundheits- bzw. Krankheitsdaten ohne eigene Entscheidungsmöglichkeit offen gelegt werden müßten

An dieser Frage entscheidet sich deshalb die Vereinbarkeit einer solchen Karte mit dem Recht auf informationelle Selbstbestimmung.

Ich sehe angesichts der besonderen Sensibilität von medizinischen Daten auch **keine "überwiegenden Interessen der Allgemeinheit"**, die eine solche gesetzliche Verpflichtung rechtfertigen würden.

Für eine effektive Realisierung der Entscheidungsmöglichkeiten des Bürgers in der Verwendung der Karte ist weiter die **Entscheidungsmöglichkeit** notwendig, ob und wie die

Karte im Einzelfall verwendet wird. Das Konzept des BMG enthält hier bereits Ansatzpunkte. Es sieht verschiedene Felder vor, die gesonderte Eintragungen des Bürgers ermöglichen. Es soll auch ein Feld für solche Medikationen vorgesehen werden, die nicht dem allgemeinen Lesezugriff für die Berechtigten geöffnet werden sollen [VR21].

Das reicht aber nicht aus. Der Bürger und die Bürgerin muss auch zumindest die Möglichkeit haben, die Karte im **Einzelfall nicht vorzulegen** [VR22]. Die Bürger und Bürgerinnen sollen sich im Einzelfall auch dagegen entscheiden können, dass ein bestimmter Eintrag auf der Karte vorgenommen oder dass ein besonders sensibler Inhalt ausgelesen wird [VR23]. Hätten sie diese Möglichkeit nicht, reduzierte sich ihre Entscheidungsfreiheit über die Verwendung seiner Krankheitsdaten ganz erheblich. Sie wären dann auf ein "Alles oder nichts" beschränkt.

Von ärztlicher Seite wird nun eingewandt, dass diese Möglichkeiten für den Bürger schwer handlebar seien.

Beide Einwände sind nicht von der Hand zu weisen.

Auf der anderen Seite hatten Bürger und Bürgerin auch bisher die Freiheit, nicht jedem Arzt alles zu sagen.

Sie werden dies auf Fälle beschränkt haben, wo sie dafür gute Gründe gesehen haben. So kann es für die Einholung einer **unbeeinflussten Zweitmeinung** zweckmäßig erscheinen, die Erstdiagnose dem zweiten Arzt nicht zu offenbaren.

Auch wird es durchaus Fälle geben, in denen der Patient oder die Patientin dem **Orthopäden**, der ein Knie behandelt, nicht den Besuch bei **Fachärzten für bestimmte sensible Krankheiten** offenbaren will.

All diese Möglichkeiten haben Bürger und Bürgerinnen bis jetzt. Diese dürfen ihnen auch mit der Verwendung der Gesundheitskarte nicht genommen werden.

Auf jeden Fall muss es möglich sein, einzelne **ärztliche Fachbereiche vom allgemeinen Zugriff** auszuschließen.

Für die Frage der "Handlebarkeit" vertraue ich auf die Phantasie der Informatiker.

Ich begrüße es deshalb sehr, dass in der "**gemeinsamen Erklärung**" ausdrücklich hervorgehoben wird,

- dass Patienten entscheiden können (sollen), **welche ihrer Gesundheitsdaten aufgenommen** und welche gelöscht werden,
- dass Patienten entscheiden können (sollen), **ob und welche Daten sie einem Leistungserbringer** zugänglich machen^[VR24].

In der gemeinsamen Erklärung steht auch der begrüßenswerte Satz,

dass "**Modellversuche** nur unter strenger Beachtung des Datenschutzes und des Selbstbestimmungsrechtes der Patienten durchgeführt werden"

Wenn ich die Novelle der **Modellklausel in § 63 Abs.3 SGB V** betrachte, muss ich da leider **leicht skeptisch** sein:

Nach dieser Bestimmung soll es möglich sein, für Modellvorhaben u.a.

"von den Vorschriften des 10. Kapitels dieses Buches" abzuweichen.

Diese Vorschriften stellen nun gerade die **Datenverarbeitungsbefugnisse** für die gesetzlichen Krankenversicherungen dar und damit auch deren **Grenzen**. Natürlich soll ein Abweichen nur mit Zustimmung des Versicherten möglich sein, nur im für den Modellversuch erforderlichen Umfang und nur nach ausführlicher Aufklärung des Versicherten über Sinn und Zweck des Versuchs und der damit erfolgenden Datenverarbeitung.

Trotzdem frage ich mich, ob wirklich eine derart **pauschale Freistellungsklausel erforderlich war?** Ich frage mich auch, warum der Forderung des Bundesbeauftragten für den Datenschutz, die Entscheidungsfreiheit des Versicherten über die Kartenverwendung im Einzelfall aufzunehmen, erst in die Begründung eines Änderungsantrags für die Ausschussberatungen aufgenommen wurde.

Diese Modellklausel steht für mich deshalb in einem **merkwürdigen Widerspruch** zu der fast gleichzeitig herausgegebenen "Gemeinsamen Erklärung" und zu der dortigen Forderung, dass

"Modellversuche nur unter strengster Beachtung des Selbstbestimmungsrechtes des Patienten durchgeführt werden"

Die Modellversuche und vor allem eine später folgende breite Einführung von Gesundheitskarte und elektronischer Patientenakte **müssen von den Gedanken der "Gemeinsamen Erklärung"** getragen werden. Sie müssen von dem Bestreben getragen werden, den Bürgern und Bürgerinnen auch mit der elektronischen Gesundheitskarte ein Höchstmaß von Entscheidungsfreiheit zu ermöglichen.

Das ist meine Hoffnung als Datenschutzbeauftragter.

Seite: 2

[VR1] Rechtsstand September 2002; inzwischen wurden durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung – Gesundheitsmodernisierungsgesetz (GMG)- wesentliche Änderungen in das Sozialgesetzbuch V eingefügt; unter anderem sollen jetzt für die Abrechnung auch allgemein u.a. die Krankenversicherungsnummer übermittelt werden. Die Abrechnung erfolgt deswegen jetzt generell nicht mehr nur fallbezogen sondern versichertenbezogen.

Seite: 2

[VR2] § 295 Abs. 2 SGB V geändert w.o.

Seite: 3

[VR3] Die Gefahr wurde durch die obigen Änderungen verstärkt. Die obigen personenbezogenen Daten dürfen allerdings nur für Abrechnungszwecke verwendet werden. Für die Bildung sektor- und quartalsübergreifender Untersuchungen wurde ein Pseudonymisierungsverfahren eingeführt, das die nachstehenden Forderungen weitgehend berücksichtigt §§ 303 a ff SGB V i.F.GMG, dazu siehe unten

Seite: 3

[VR4] Dieses Gefährdungspotential wurde durch das GMG vergrößert

Seite: 4

[VR5] Inzwischen wurden die gesetzlichen Voraussetzungen für einen Pool mit pseudonymisierten Daten durch die §§ 303 a ff GMG geschaffen

Seite: 5

[VR6] Forderung aufgenommen: In § 303 e Abs. 1 Satz 2 SGB V i.F.GMG wird ein Stichprobenverfahren ausdrücklich vorbehalten

Seite: 5

[VR7] Jetzt § 303 c aaO

Seite: 5

[VR8] Jetzt § 303 c Abs. 1 Satz 2 aaO

Seite: 5

[VR9] Jetzt § 303 c Abs. 3 Satz 1 aaO

Seite: 5

[VR10] Ist erfolgt; s.o.

Seite: 5

[VR11] Erfüllt: § 303 f Abs. 2 aaO.

Seite: 5

[VR12] Erfüllt: §§ 303 c Abs. 3 Satz 2, 303 d Abs. 2 Satz 2 aaO.

Seite: 6

[VR13] Erfüllt: §§ 303 c Abs. 3 Satz 1, 303 d Abs. 2 Satz 1 aaO.

Seite: 6

[VR14] Erfüllt: § 303 c Abs. 1 Satz 1 aaO.

Seite: 6

[VR15] Erfüllt: § 303 c Abs. 1 Satz 2 und Abs. 2 aaO.

Seite: 6

[VR16] Inzwischen liegt mit § 291a SGB V in der Fassung des GMG eine gesetzliche Regelung der elektronischen Gesundheitskarte vor, die einen wesentlichen Teil der nachstehenden Forderungen aufgenommen hat Die Gesundheitskarte in dieser Form soll bis zum 1. Januar 2006 eingeführt werden.

Seite: 6

[VR17] § 291 a aaO. setzt die Trennung voraus, da der Zugriff auf die Gesundheitsdaten die ausdrückliche Einwilligung des Betroffenen vorsieht § 291 a Abs. 3 Satz 3 aaO.

Seite: 7

[VR18] In § 291 a aaO keine ausdrückliche Regelung. Vielmehr läßt aaO die Frage „Server“- oder Kartenlösung“ offen (Begründung zu lit. c aaO.). Auch bei Serverlösung ist dezentrale Lösung möglich.

Seite: 8

[VR19] Hier wesentliche Neuregelung: Nach § 91 Abs. 2 Satz 1 StPO i.d.F. von Art. 30 GMG wird der strafprozessuale Schutz von Patientendaten auf die Gesundheitskarte im Besitz des Patienten und nach Satz 2 aaO. auf Dienstleister erweitert, der für die in § 91 StPO geschützten Personen und Einrichtungen Daten verarbeitet. Dieses Argument gegen externe Verarbeitungen ist damit entfallen.

Seite: 9

[VR20] So jetzt § 291 Abs. 3 Satz 3 a aaO

Seite: 10

[VR21] Siehe dazu jetzt § 291 a Abs. 3 Satz 1 Nr. 5 aaO.

Seite: 10

[VR22] So § 291 a Abs. 3 Satz 4 2. H.S. aaO.

Seite: 10

[VR23] w.vor

Seite: 11

[VR24] Diese Möglichkeiten bestehen nach der Regelung des § 291 a aaO.