Wolfgang Linder **September 2013**

Die elektronische Gesundheitskarte (eGK) – Einfallstor für Ausspähung und vielfältige Nutzung von Patientendaten?

Derzeit sind die gesetzlichen Krankenkassen bemüht, möglichst viele ihrer Versicherten zu veranlassen, ihre Fotos einzusenden, um diese auf den neuen eGK`s aufzubringen. Statt - wozu sie durch § 291a Abs.2 Satz 3 SGB V verpflichtet wären – ihre Versicherten umfassend über die Funktionen der eGK und die mit ihrer Hilfe beabsichtigte Datenverarbeitung aufzuklären, wird diesen vorgespiegelt, Fotos und neue Karte sollten vorrangig den Missbrauch der bisherigen Krankenversichertenkarten durch Unbefugte verhindern und die Sicherheit der gespeicherten Daten erhöhen. Die Höhe der durch missbräuchliche Kartenverwendung entstandenen Schäden ist nie belegt worden. Überdies wird datenschutzwidrig nicht überprüft, ob die eingesandten Fotos tatsächlich die der Karteninhaber sind[1]. Es besteht daher Anlass zu der Annahme, dass die eigentlichen mit der Ausgabe der neuen Karten verfolgten Ziele ganz andere sind.

Auf Betreiben der Krankenkassen wurde in das Aufgabenprogramm der eGK nachträglich das Versichertenstammdatenmanagement (VSDM) aufgenommen. Bereits in den Arztpraxen sollen die auf den Karten gespeicherten administrativen Daten aktualisiert werden. Obgleich dies nicht die Öffnung der EDV-Systeme, mit deren Hilfe die Ärzte die Behandlung ihrer Patienten dokumentieren, voraussetzt, wurden den Ärzten durch finanzielle Anreize für den Erwerb hierfür geeigneter Lesegeräte genau dieses schmackhaft gemacht. Dies legt den Verdacht nahe, dass über das VSDM hinausgehende Ziele gefördert werden sollten.

Weitere gesetzlich vorgesehene Funktionen der neuen Karte sind die Versendung elektronischer Rezepte und elektronischer Arztbriefe. Deren Sinnhaftigkeit soll hier nicht bestritten werden. Aber: Mit Hilfe dieser Instrumente sollen doch Ärzte mit anderen Ärzten bzw. mit Apothekern kommunizieren. Warum aber sehen die bekannt gewordenen Konzepte es vor, die zu versendenden Daten auf zentralen Servern zu speichern?

Es wird also ein zentrales System der Gesundheitstelematik (GT) aufgebaut, ohne dass dieses für die Nutzung der eGK selbst, der VSDM, des elektronischen Rezepts oder des elektronischen Arztbriefes erforderlich wäre. Diese sollen auch nicht die zentralen Bausteine der GT sein, sondern vielmehr die elektronische Patientenakten (ePA`s), in denen die Ärzte die Diagnosen und Therapien möglichst vieler ihrer Patienten möglichst umfassend auf zentralen Servern speichern sollen. Vor den Versicherten und der Öffentlichkeit wird mittels Feigenblatt eGK verborgen, dass es eigentlich um den Aufbau einer serverbasierten Telematikinfrastruktur zwecks Speicherung von medizinischen Daten geht (These 1).

Die serverbasierte GT bietet Angriffspunkte für illegale Zugriffe auf eine unübersehbare Vielzahl auch patientenbezogener Gesundheitsdaten (1. Teil der These 2).

Der Gesetzgeber hat in §§ 291 und 291a SGB V zur Sicherung der mit Hilfe der eGK gespeicherten Gesundheitsdaten vorgeschrieben,

- die eGK müsse technisch geeignet sein, Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen,
- technische Vorkehrungen müssten gewährleisten, dass Zugriffe nur durch Autorisierung der Versicherten und in Verbindung mit einem elektronischen Heilberufsausweis erfolgen können.

[1] zur Sicherheit oder richtiger Unsicherheit der zentral gespeicherten Gesundheitsdaten weiter unten im Text

Die Betreiber des Projekts eGK und GT, d.h. die Telematikindustrie, die Gematik[2] und die verantwortlichen Politiker, versichern, sie beabsichtigten, diese Vorgaben umzusetzen, dadurch sei der Missbrauch dieser Daten ausgeschlossen. Allerdings ist aufschlussreich, dass sich auf der FAQ-Liste der Gematik zu der Frage „Wie werden Datenschutz und Datensicherheit gewährleistet?“ relativierende Formulierungen befinden wie jene, „dass die Speicherung sensibler Patientendaten so sicher wie möglich erfolgt“ oder jene, dass man sich um „ein Höchstmaß an Sicherheit“ bemühe[3].

Warum aber drückt die Gematik sich so vorsichtig aus? Vielleicht tut sie ja gut daran:

1. Die Angehörigen von Heilberufen dürfen mit Hilfe ihrer elektronischen Heilberufsausweise unter bestimmten Voraussetzungen – vor allem Autorisierung durch den betroffenen Patienten per eGK – auf dessen zentral gespeicherte medizinische Daten zugreifen. Es ist wichtig zu wissen, dass es sich um etwa 2 Millionen potentiell Zugriffsberechtigter handelt: Ärzte, Zahnärzte, Apotheker, Apothekerassistenten, Pharmazieingenieure, Apothekenassistenten, Personen, die bei den Vorgenannten oder in einem Krankenhaus als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind, sonstige Erbringer ärztlich verordneter Leistungen und Psychotherapeuten.[4] „Wer glaubt, dass er bei rund 2 Millionen Zugangsberechtigten ...einen Missbrauch der Daten ausschließen kann, handelt naiv, fahrlässig oder will absichtsvoll täuschen“.[5] Die Gematik jedenfalls scheint sich über das Gefahrenpotential im klaren zu sein.

2. Die renommierte „Gesellschaft für Informatik (GI)“ jedenfalls „lehnt eine Speicherung von Gesundheitsdaten im Internet nachdrücklich ab. Angesichts der Vielzahl Zugriffsberechtigter von etwa 80 Millionen[6] dürfte hinreichend sichere Zugriffskontrolle überhaupt nicht machbar sein. Dies wird spätestens dann in einem Missbrauchsfall offenkundig werden, wenn jedermann mit vorgefertigten, im Internet erhältlichen Tools die Daten seiner Nachbarn, seiner Bekannten, seines Abgeordneten oder anderer Politiker wie Landes- und Bundesminister etc. lesen kann“.[7] Ganz zu schweigen von den Aussichten für die Geheimdienste[8]

3. In der kritischen Literatur zum Projekt der eGK werden einige technische Schwachpunkte von deren Sicherheitsarchitektur angeführt, so die Speicherung der medizinischen Daten zwecks Back-up verloren gegangener Daten und die Öffnung des Servers bei berechtigten Abrufen. Bei Tests hat sich herausgestellt, dass sowohl Patienten als auch Angehörige von Heilberufen dazu neigen, ihre Passwörter vergessen zu haben. Dies hat den Vorschlag angeregt, der Patient könne doch sein Passwort in der Arztpraxis hinterlegen, was unberechtigte Zugriffe unter Umgehung des Patientenwillens geradezu provozieren dürfte. Hinzukommt, dass in der Hektik und dem Stress des Alltags in Arztpraxen die wiederholte Eingabe von Passwörtern häufig als unzumutbare Belastung empfunden werden dürfte.

---

2 vgl. Whitepaper von Aporil 2008, im Netz unter gematik_white_paper_sicherheit(2).pdf und gematik_GA_Gesamtarchitektut_VI_3_0.pdf. Nach § 291a Abs. 7 SGB V nehmen die Akteure der „gesundheitlichen Selbstverwaltung“ (vor allem Kassen, Ärzte, Krankenhäuser und Apotheker) in der „Gesellschaft der Telematik“, kurz Gematik, nach Maßgabe des § 291b SGB V unter Fachaufsicht des Bundesministeriums für Gesundheit die Aufgabe des Aufbaus der GT wahr.

3 so Prof. Dr. Hartmut Pohl, Informatiker, zitiert in der Internetzeitung „schattenblick“ vom 22.04.2012 unter „Das System e-Card – Optimierter Zugriff auf die Ressource Mensch, S.5, im Netz unter Sb 120422_schattenbl#B2D1.pdf, mit Hinweis auf www.gematik.de/cms/de/header_navigation/faq/faq_1.jsp

4Wiedergabe der Aufzählung in § 291a Abs.4 SGB V

5 So wiederum Pohl s.o. Fußnote 3

6 Hier sind alle gesetzlich Krankenversicherten selbst, die auf ihre eigenen Daten zugreifen können, und die Angehörigen der Heilberufe eingerechnet

7 Gi-thesen-gesundheit#59B3D1.pdf

8 dazu unten auf S. 3 unter Punkt 7

4. Über den Konnektor, der die Praxissoftware mit dem Internet verbindet, wird ein Einfallstor in deren Struktur geschaffen, z.B. können Administratoren sich per Fernzugriff auf die Rechner von Ärzten etc. draufschalten[9]

5. Da der Verfasser kein Informatiker ist, macht er sich nicht anheischig, das Ausmaß der Missbrauchsgefahr real beurteilen zu können. Eins jedoch glaubt er beurteilen zu können: Bei 80 bzw. 2 Millionen Zugriffsberechtigter[10] ist nie auszuschließen, dass immer wieder Einzelne unter ihnen dem Druck oder der Versuchung erliegen.

6. Nun wird häufig damit argumentiert, die bisherige dezentrale Datenhaltung in Krankenhäusern, Arztpraxen etc. sei deutlich unsicherer. Dass es auch bisher um die Sicherheit unserer Gesundheitsdaten nicht immer zum besten bestellt ist, soll nicht bestritten werden. Aber: Abgesehen davon, dass ein Teil der immensen finanziellen Mittel für das Projekt der zentralen Datenhaltung ausreichen würde, hier Abhilfe zu schaffen, so ist doch eines klar: Die Gematik selbst schätzt in einem Whitepaper die Menge aller zu speichernden Patientendaten auf mehrere Dutzend Terabyte (1 TB = 1024 GB).[11] Um wieviel größer sind da Versuchung und Schaden unberechtigter Zugriffe, als wenn es lediglich um die in einer Klinik oder gar nur in einer Arztpraxis gespeicherten Behandlungsdaten ginge?

7. Immer neue in den vergangenen Jahren aufgedeckte Datenschutzskandale haben den Verdacht bestärkt, dass illegale Datennutzung weit verbreitet ist. Zudem ist von kompetenter Seite wiederholt dargelegt worden, dass elektronische Daten, deren Speichermedien in Verbindung mit dem Internet stehen, selbst durch Firewalls oder Verschlüsselung nicht absolut sicher sind. Staatliche Programme wie PRISM, TEMPORA und XKEYSCORE dürften den letzten vertrauensvollen Bürger davon überzeugt haben[12]. Die Bundesregierung hat bisher keine Veranlassung zu der Annahme gegeben, als sei sie bereit und in der Lage, daran etwas zu ändern. Zwar haben die Datenschutzbeauftragten (DSB`s) von Bund und Ländern in ihrer Entschließung vom 05.09.13[13] Konsequenzen gefordert. Aber die Forderung, Projekte wie das der eGK mit seiner zentralen Struktur sollten überdacht oder gar aufgegeben werden, fehlt. Dies verwundert nicht. Stehen die DSB`s doch von Anfang an mit dem Projekt „im regelmäßigen Dialog“.[14] Wie der DSB des Bundes es in einem Schreiben vom 22.09.11 an das Komitee für Grundrechte und Demokratie formulierte, sehen sie sich in das Projekt eingebunden. Da mag es schwer fallen, das eigene Verhalten kritisch zu hinterfragen und zu korrigieren.

Die GT bietet die optionale Grundlage für umfassende Auswertungen der Gesundheitsdaten aller Patienten (2. Teil der These 2).

Nach geltender gesetzlicher Regelung darf auf patientenbezogene medizinische Daten nur
- mit der Zustimmung der betroffenen Patienten, d.h. Autorisierung mittels eGK (Ausnahme: elektronisches Rezept),
- durch Inhaber von Heilberufsausweisen,
- nur für die § 291a Abs.3 SGB V abschließend aufgeführten Funktionen und
- soweit es zur Versorgung der Patienten erforderlich ist,

[9] it-ler-analysiert-die-egk (www.ocmts.de/egk/)
[10] nur Angehörige von Heilberufen oder zuzüglich der Patienten selbst, vgl. Fußnoten 4 und 6
[11] gematik_white_paper_sicherheit.pdf sowie gematik_GA_Gesamtarchitektur_VI_3_0.pdf
[12] zu den Gefahren: Silke Lüder in „Gesundheitswirtschaft“, 09/13, S. 42
[13] www.bfdi.bund.de
[14] so E-HEALTH-COM News vom 14.05.13

zugegriffen werden, vgl. § 291a Abs. 4,5 SGB V. Diese seinerzeit in 2003 durch die DSB`s von Bund und Ländern durchgesetzten Schranken werden stets angeführt, wenn es gilt, Befürchtungen vor umfassenden Auswertungen zu begegnen.

Ob aber diese strikten Regelungen Bestand haben, ist die Frage: Allein die Existenz des zentralen Datenpools steht im Widerspruch dazu. Sie fordert geradezu relationale Auswertungen heraus[15]. Immer wieder ist auch von „Mehrwertdiensten" die Rede, von Funktionen jenseits der gesetzlich Vorgesehenen. Die GT könnte eine Art Werbeplattform für gewerbliche Anbieter im Wellness-Bereich werden. Überhaupt heißt es: "Um möglichst viele Anwendungen für Patienten auf die Telematik-Plattform zu portieren, müssen medizinische Geräte und zentrale Software Services integriert werden. So können Anbieter einzelner Teilprodukte die Dienste der Telematikinfrastruktur nutzen, um hybride Mehrwertdienste modellieren und anbieten zu können". [16] IBM will „eine skalierbare Plattform mit einer Auswahl möglicher Mehrwertdienste bieten". Man hole sich hierfür verschiedene Industrie-Partner ins Boot.[17]

Die medizinische Forschung verspricht sich einen bislang unbekannten Vorrat an Daten für ihre Projekte[18]. Im Rahmen des Projekts „Electronic Health Records for Clinical Research" (EHR4CR), gefördert durch die EU im Rahmen der „Innovative Medicines Initiative 2011-2014) mit 7 Millionen Euro, bauen Forschung und Industrie eine europaweite Technologieplattform auf, die die Sekundärnutzung von Daten aus elektronischen Patientenakten für die medizinische Forschung ermöglichen soll. Vor allem könnten geeignete Studienpatienten besser identifiziert werden. Ziel sei es, über die Plattform elektronische Patientenakten nahtlos in bestehende Forschungsplattformen und Netzwerke des Gesundheitswesens zu integrieren. Derzeit wichen die gesetzlichen Bestimmungen und die Rechtspraxis zum Datenschutz und zum Schutz der Privatsphäre in den Mitgliedsstaaten der EU stark voneinander ab. U.A. sollten deshalb die Rechtssituation analysiert und Empfehlungen dafür erarbeitet werden, wie für die klinische Forschung Rechtssicherheit geschaffen werden könne, d.h. doch das als strikt betrachtete deutsche Datenschutzrecht aufgeweicht werden könne[19]

Es liegt auch nahe, die gespeicherten elektronischen Patientenakten „nahtlos" mit den durch die im Rahmen der „nationalen Kohorte" gespeicherten Daten und Bioproben von 200.000 Bundesbürgern, einer nationalen Forschungsplattform im Aufbau[20], zu verknüpfen. Zu bedenken ist insbesondere, dass bei Längsschnittuntersuchungen über längere Zeiträume wiederholt die Verknüpfung der genutzten Daten mit bestimmten Patienten erforderlich ist. Auch in andere Datenpools könnten die ePA`s „nahtlos" überführt werden, etwa in Projekte ähnlich dem auf der letzten CEBIT durch das „cloud4health"- Konsortium (Industrie, Forschung, Kliniken) vorgestellten Projekt, Patientendaten mittels „Cloud-Computing" für „Kostensenkungen bei klinischen Studien, „cloudbasiertes Wirkstoffscreening" oder „automatisierte Plausibilitäts- und Wirtschaftlichkeitsprüfungen medizinischer Behandlungen" zu nutzen.[21]

---

[15] Relationale Datenbanken erlauben vielfältige Auswertungen, mittel derer die gespeicherten Daten beliebig miteinander verknüpft werden können, auch „data-warehouse" genannt

[16] „Konzepte patientenorientierter Gesundheitstelematik. Mehrwertdienste für die Deutsche Gesundheitstelemnatik", (www.uni-kassel.de/fb7/ibwl/leimeister/pub/JML_143_b.pdf), zitiert wiederum nach Pohl aaO

[17] Ärztezeitung vom 18.12.12: „Keine Angst vor Online-Diensten", www.aerztezeitung.de/extras/druckansicht/?sid=82795...

[18] Hier ist mit dem Einwand zu rechnen, dass Forschung grundsätzlich positiv zu bewerten ist und überdies ebenso wie die Privatsphäre Grundrechtsschutz genießt . Dem ist entgegenzuhalten, dass in Zeiten drittmittel -, d.h. industriefinanzierter Forschung und profitorientierter Gesundheitswirtschaft gerade medizinische Forschung kritisch auf ihren Nutzen für Patienten zu hinterfragen ist.

[19] www.ehr4cr.eu, vgl. Deutsches Ärzteblatt Jg. 109, Heft 7 vom 17.02.12

[20] www-nationale-kohorte.de und Görlitzer „BIOSKOP", 09/12, S. 3

[21] Görlitzer „Patientendaten in der Wolke" in „BIOSKOP", 03/13, S. 8

Nun baut die derzeit geltende Gesetzeslage recht hohe Hürden auf, die zu überwinden sind, damit die ePA`s vollständige und zuverlässige Datengrundlagen für all diese denkbaren Auswertungen darstellen. § 291a Abs.3 Sätze 4,5 SGB V bestimmt, dass die Versicherten vor der Speicherung ihrer Daten in einer ePA gegenüber einem zugriffsberechtigten Arzt, Zahnarzt, Psychotherapeuten oder Apotheker ihre Einwilligung erklärt haben müssen. Diese ist auf der eGK zu dokumentieren und ist jederzeit widerruflich. Zudem darf nach § 291a Abs.5 Sätze 1-3 SGB V in jedem Einzelfall die Verarbeitung von Daten im Rahmen einer ePA nur mit dem Einverständnis des Versicherten möglich sein.

Aber: Gesetze können geändert werden. Wie schnell und reibungslos und ohne großes öffentliches Aufsehen das geht, habe ich in meinem Beitrag zu der Veröffentlichung „Digitalisierte Patienten – Verkaufte Krankheiten“ des Komitees für Grundrechte und Demokratie[22] versucht, anschaulich zu machen.[23] Kurz vor der abschließenden Lesung eines Artikelgesetzes mit gänzlich anderen im Fokus der öffentlichen Debatten stehenden Inhalten bringen die Mehrheitsfraktionen einen Änderungsantrag ein, der möglichst ohne Begründung und ohne Diskussion verabschiedet wird. Und die eben dargestellten Regelungen werden – so meine Voraussage – dieses Schicksal erleiden, wenn eine kritische Öffentlichkeit dies nicht verhindert und wenn die Logik und die immensen Kosten der serverbasierten GT dies verlangen, s.u. unter These 3. Von Dr. Arno Elmer, dem Geschäftsführer der Gematik, ist folgende Aussage überliefert: „Wir bauen nur die Datenautobahn, wenn der Gesetzgeber sich die Daten holen will, dann holt er sie sich“ .[24] Durch wen und zu mit welchen Zielen wiederum auf den Gesetzgeber einwirkt wird, lässt sich wohl denken.

Gematik und Politik halten sich mit Aussagen zu den voraussichtlichen Kosten des Projekts zurück. Lediglich eine Schätzung auf ca. 2 Mrd. Euro wurde ganz zu Anfang genannt. Von anderer Seite aber wurden auch Kosten in Höhe von 14 Mrd. Euro genannt. Verifizieren lässt sich wohl beides nicht. Man weiß, was man von derartigen Zahlen halten darf. Die Unternehmensberatung Booz, Allen, Hamilton jedenfalls kam in einem von der Gematik in Auftrag gegebenen, aber durch den Chaos Computer Club veröffentlichten[25] Gutachten zu dem Ergebnis, dass sich die eGK erst rechnet, wenn sie für die ePA genutzt wird. Und, so könnte man fortfahren, wenn Ärzte und ihre Patienten nahezu vollzählig mitmachen und, könnte man weiter fortfahren, wenn die in den ePA`s vollzählig gespeicherten medizinischen Daten umfassend und vielfältig ausgewertet werden.

Aufschlussreich ist auch, dass zwar die Höhe der Verwaltungsausgaben der Krankenkassen nach Maßgabe des § 4 SGB V SGB V begrenzt ist, dass aber § 291a Abs. 7 Satz 7 SGB V die Ausgaben für eGK und GT ausdrücklich davon ausnimmt. Als rechne man mit ständig steigenden Kosten und als sei man bereit, sie unbegrenzt zu akzeptieren, gegenfinanziert durch die Beiträge der Versicherten und durch Einsparungen bei den Leistungen für ihre gesundheitliche Versorgung. Von Abstrichen an dem Projekt selbst war bislang nichts zu vernehmen. Dem steht sicher u.a. entgegen, dass bei den Mitgliedsorganisationen der Gematik, bei der Gematik selbst und in der Telematikindustrie eine Vielzahl von Arbeitsplätzen und beruflichen Karrieren von diesem Projekt abhängen. Wer spart sich schon gern selbst ein.

---

[22] Köln 2011, siehe www.grundrechtekomitee/de/node/388

[23] s.o. Fußnote 17 S. 123ff „Die elektronische Gesundheitskarte – Baustein der zentralen Telematikinfrastruktur in der Gesundheitsökonomie oder: Fünf Lehrstücke, wie Bürokratie und Lobby ihre Interessen durchsetzen – oder wie leichtfertig und willfährig der Deutsche Bundestag Gesetze beschließt und verändert“

[24] auf dem gesundheitspolitischen Kongress der Piraten am 04.02.13, vgl. www.heise.de/newsticker/meldung/Piratenpartei-diskuti....

[25] httpc//dasalte.ccc.de/crd/whistleblowerdocs/20060731-Gesundheitstelematik.pdf?language=de

Gegenwehr und Alternativen

Abschließend sei erwähnt, dass die Gegenwehr gegen das Projekt immer stärker wird.[26] Auf der Großdemonstration „Freiheit statt Überwachung“ am 07.09.13 in Berlin haben Redner und Demonstranten die Forderung nach einem Stopp des Projekts „eGK“ erhoben, zu recht in diesem Zusammenhang. Wenn die Geheimdienste schon Aufwand, Mittel und Rechtsbrüche nicht scheuen, um Kommunikations- und Kontodaten auszuspionieren, so werden sie erst recht nicht Gesundheitsdaten unbehelligt lassen, die ihnen auf dem Präsentierteller der GT dargeboten werden.

Werden aber die Politiker ihrer Verantwortung nicht gerecht, wird es darauf ankommen, dass Patienten, Versicherte, Ärzte dem Druck bzw. der Versuchung widerstehen, daran mitzuwirken, dass in den ePA`s sämtliche medizinische Daten aller Patienten gespeichert werden - und, dass öffentlicher Druck einen gedankenlosen oder willfährigen Gesetzgeber daran hindert, durch Gesetzesänderungen den nicht genehmen Willen von Patienten, Versicherten, Ärzten ins Leere laufen zu lassen.

Als Alternative bieten sich dezentrale GT-Strukturen an, die die medizinische Versorgung durch die Verbesserung der elektronischen Kommunikation der Angehörigen von Heilberufen untereinander verbessern, aber die dargestellten Kosten und Risiken erheblich verringern.

[26] vgl. etwa www.stoppt-die-e-card.de und www.grundrechtekomitee.de