telemedizin2

Medizinische Telematik und eGK
Im Spannungsverhältnis zwischen Funktionalität und Datenschutz

Thilo Weichert

I. Die grundsätzliche Diskussion

Die Diskussion um die elektronische Gesundheitsakte (eGK) und die medizinische Telematik wird stark bestimmt von zwei Fragen: 1. Lässt sich mit der eGK der medizinische Datenschutz und das mit dem hippokratischen Eid vor über 2000 Jahren normierte Patientengeheimnis gewährleisten? 2. Können unter Achtung des Patientengeheimnisses die Abläufe der automatisierten Verarbeitung von Daten so gestaltet werden, dass den medizinischen Leistungserbringern keine zusätzlichen Lasten aufgebürdet werden, ja dass sich gar Erleichterungen und Verbesserungen ergeben? Zusammengefasst in einer Frage: Wie lassen sich Datenschutz und Funktionalität beim Einsatz der eGK bzw. von medizinischer Telematik zugleich verwirklichen?

Dass der Datenschutz bei der Einführung der eGK nicht mehr gewährleistet wäre bzw. werden könne, war das zentrale Argument vieler ärztlicher, aber auch der sonstiger Gegner der eGK (1). Diesem Argument wurde mit dem Hinweis auf die hohen datenschutzrechtlichen Standards gekontert, die von der gesetzlichen Regelung des § 291a SGB V vorgegeben werden und die in der Praxis durch standardisierte Vorgaben der Gematik umgesetzt werden. Diese Vorgaben lassen sich - zunächst vereinfacht - wie folgt beschreiben: Die Verarbeitung von Patientendaten wird doppelt gesichert: Es erfolgt die Authentisierung durch einen medizinischen Heilberufler und die Autorisierung durch den Patienten. Die Authentisierung des Heilberuflers, also etwa des Arztes, erfolgt durch den Heilberufsausweis (HBA), auch Health Professional Card (HPC) genannt. Die Autorisierung des Patienten erfolgt durch die eGK. Um die jeweilige Berechtigung der Kartennutzer sicherzustellen, genügt der Besitz der HBA bzw. der eGK in der Regel nicht. Vielmehr wird zusätzlich zum Besitz das Wissen des Berechtigten in Form einer Personal Identification Number (PIN) verlangt. Diese PIN ist bisher als sechsstellige Kombination von Buchstaben und Ziffern angelegt (2).

Tatsächlich kann dieses Sicherheitsinstrumentarium als ausreichend zur Sicherung des Datenschutzes angesehen werden, ja sogar als vorbildlich. Besonders bestechend ist bei der Konzeption, dass die sensiblen Medizindaten verschlüsselt abgelegt werden und das Lesen dieser Daten technisch nur mit Hilfe eines auf der eGK befindlichen privaten Schlüssels möglich ist. Diese Konstruktion bedeutet, dass - technisch - die Verfügungshoheit über die Medizindaten tatsächlich beim Patienten liegt. Dieses Konzept ist durch die gesetzliche Regelung vorgegeben: Abgesehen von der Nutzung der eGK als Identifzierungskarte und zur Übermittlung von elektronischen Rezepten sollen sämtlichen Anwendungen bzw. Funktionalitäten für den Patienten freiwillig sein. D.h. der Patient soll - durch Bereitstellung der Karte und Eingabe der PIN - selbst entscheiden, wer seine Daten auf die Karte schreiben und wer sie lesen darf (3).

II. Praktische Probleme

Dieser Ansatz, der eine fast ideale Realisierung der medizinischen und der informationellen Selbstbestimmung des Patienten zum Ziel hat, erfordert von diesem eine gewisse intellektuelle Kompetenz bei der Nutzung der eGK: Der Patient muss zunächst in der Lage sein, die komplexen Vorgänge der elektronischen Verarbeitung seiner Medizindaten mit der eGK in Kombination mit der Telematik-Infrastruktur, also der Hintergrundsysteme in Form des Netzes, der Rechner und Systeme der medizinischen Leistungserbringer sowie der Dienstleister zu verstehen. Dann muss der Patient bewusst entscheiden können, welche Verarbeitungsoptionen er wünscht und welche nicht. Hierfür ist es nötig zu verstehen, welche indirekten positiven und negativen Konsequenzen eine Verarbeitung hat bzw. haben kann. Beispiele: Erlaubt der Patient die Aufnahme einer Blutinfektion in den Basis- bzw. Notfalldatensatz, so können im Fall einer Behandlung die Heilberufler zu besonderer Vorsicht z.B. bei Blutkontakt angehalten und dadurch geschützt werden. Zugleich droht mit der Information eine für den Betroffenen wenig kalkulierbare Diskriminierung. Die Aufnahme umfassender gynäkologischer Daten ermöglicht einer Frauenärztin, sich ein umfassendes Bild von ihrer Patientin zu machen. Zugleich muss die Patientin aber darüber bestimmen, ob sie diese Informationen bei einem Hausarztbesuch, bei einem arbeitsärztlichen Gesundheitscheck oder bei einer Behandlung einer Erkältung während eines Besuchs eines fremden Arztes im Urlaub freischalten möchte.

Derartige Entscheidungen dürften derzeit viele Patienten überfordern, da die damit verbundenen Interessenlagen sehr komplex sein können und die Patienten bisher derartige Handlungsoptionen nicht kennen. Ein gewisser Lerneffekt wird sich bei vielen Patienten mittelfristig einstellen. Dennoch wird die Fähigkeit zur Inanspruchnahme des Rechts auf medizinische und informationelle Selbstbestimmung von Patient zu Patient immer sehr unterschiedlich sein. Dies hat eine direkte Auswirkung auf das Arzt-Patienten-Verhältnis: Dieser hat bisher die Funktion eines Gesundheitslotsen für den Patienten. Künftig wird ihm zusätzlich die Funktion eines Lotsen über die Gesundheitsdaten zukommen. Diese Aufgabe wiederum kann auch den Arzt überfordern, der eine Medizin-, nicht aber eine Informatikausbildung genossen hat. Fehlen dem Patienten und oder dem Arzt die nötigen Medienkompetenzen, so besteht die Gefahr des Fehlgebrauchs des Systems, auch die Gefahr des bewussten Missbrauchs durch Dritten sowie die Gefahr der Schädigung (4).

Bei der Erprobung in Flensburg scheiterte die Nutzung der eGK, die noch gar nicht umfassende Funktionalitäten vorweist, an viel banaleren Problemen: Viele der Patienten sahen sich schon von der Notwendigkeit überfordert, die Nutzung der eGK durch den Arzt zu autorisieren, indem sie ihre PIN verwenden. Gerade die typische Patientenklientel zeigte sich aus den unterschiedlichsten Gründen oft nicht in der Lage, innerhalb der vorgegebenen Zeit die sechsstellige PIN auf der Tastatur einzugeben. Viele konnten sich die Nummer nicht merken; viele schafften es nicht, sie in der Kürze der Zeit zu übertragen; manche waren zur Eingabe aus körperlichen Gründen nicht in der Lage (5). Die Reaktion der Ärzte auf diese praktischen Probleme ist so verständlich, wie inkonsequent. Sie forderten faktisch den Verzicht auf die PIN-Eingabe und setzten, da dies kurzfristig nicht umgesetzt werden konnte, den Testversuch aus. Inkonsequent ist dies, weil die Ärzte ansonsten - zu Recht - darauf pochen, dass das

Patientengeheimnis gewahrt wird, ihnen aber ein ungehinderter Praxisablauf wichtiger war: Die geforderte Komfort-PIN, z.B. sechsmal die Null, sowie andere "Lösungen" wie das Aufschreiben der PIN auf die Karte (Edding-Lösung) oder die Nutzung des Geburtsdatums als PIN hätten jeweils zur Folge, dass das Geheimnis "PIN" kein Geheimnis mehr wäre.

Vorgetragen wurde die Forderung nach der "Komfort-PIN" mit dem rechtlichen Argument der Selbstbestimmung: Es stünde den Patienten frei, ihre PIN zu wählen und sie auch völlig frei zu geben. Mit einer entsprechenden Einwilligung werde dem Datenschutz genügt. Diese Erwägungen sind nicht tragfähig: Wer - aus welchen Gründen auch immer - nicht in der Lage ist, seine PIN zu nutzen, aber faktisch gezwungen ist, seine eGK zu verwenden, der entscheidet sich nicht nach freien Stücken für den PIN-Verzicht. Die Bereitschaft zum Verzicht auf eine sichere PIN wäre gerade dort besonders hoch, wo auch der Schutzbedarf der Daten besonders hoch ist: bei älteren Menschen mit vielen und sehr sensiblen Medizindaten, bei denen die Gefahr des Missbrauchs und der Diskriminierung besonders hoch ist, zumal bei diesen auch die Gefahr des Kartenverlustes bzw. des unberechtigten Kartengebrauchs erhöht ist. Die Erwägung, es gebe ja noch die weitere Sicherung der Autorisierung durch den HBA, ist nicht zielführend: HBAs wird es in einer deutschen Telematik-Infrastruktur hunderttausende geben. Die Gefahr eines Kartenverlustes einschließlich Kompromittierung der PIN oder einer unberechtigten Nutzung der HBA ist hoch. Die Missbrauchzahlen von EC-Karten, bei denen auch Wissen und Besitz des Berechtigten zusammen kommen müssen, lassen dies vermuten. Wildfremde Ärzte sind nicht qua Beruf vertrauenswürdig, schon gar nicht, wenn sie für bestimmte interessierte Stellen arbeiten, etwa ein Pharmaunternehmen, eine private Versicherung, eine Krankenkasse, einen Arbeitgeber oder eine Behörde.

III. Die Infrastrukturverantwortung des Staates

Der Staat kann es nicht zulassen, dass er eine technische Infrastruktur schafft, die den Bürgern keine ausreichende Sicherheit bietet. Diese Feststellung erhielt jüngst durch ein Urteil des Bundesverfassungsgerichtes die besondere Weihe eines Grundrechtes. Danach hat bei komplexen IT-Systemen jeder Mensch ein Recht auf Gewährleistung der Vertraulichkeit und der Integrität solcher Systeme (6). Übersetzt auf die Telematik-Infrastruktur: Bei der Gestaltung der informationstechnischen Abläufe müssen Rahmenbedingungen gefunden und realisiert werden, die systemseitig nicht nur funktionieren, sondern zugleich den Datenschutz strukturell gewährleisten. Der Missbrauch kann und muss auch nicht vollständig ausgeschlossen werden. Wohl aber muss alles Vertretbare für die Sicherheit getan werden; unkalkulierbare Risiken darf es nicht geben.

Wie die geforderte Synthese von Sicherheit und Funktionalität aussieht, lässt sich nicht am Reißbrett und auch nicht in Entscheidungsgremien vorab festlegen. Vielmehr bedarf es der Erfahrungen der Praxis, an denen die Planungen gemessen werden und die ein Nachjustieren sowohl bei den Maßnahmen, evtl. sogar bei den Zielen, notwendig machen. Bei der eGK ist dieser Konflikt besonders delikat: Ohne die überzeugte Mitarbeit von Ärzteschaft und Patienten lässt sich die eGK nicht realisieren. Schon allein dies setzt nicht nur Vertraulichkeit und Integrität der Daten, sondern auch

Anwendungsfreundlichkeit und Funktionalität voraus. Anwendungen und Funktionen sind bei der Telematik-Infrastruktur nicht einfach, sondern hochtechnisch und komplex. Diese lassen sich, so die Botschaft der Informatiker, menschlich beherrschen. Die sie aber beherrschen sollen, sind keine Informatiker. Es bedarf so nicht nur des Lernens durch Versuch und Irrtum. Es bedarf auch des Dialogs zwischen Informatikern und Sicherheitstechnikern einerseits und teilweise technisch völlig ungebildeten Laien aus der Patienten- und der Ärzteschaft auf der anderen Seite.

Die Lösung der Probleme ist noch nicht gefunden, doch der Weg zur Lösung ist erkennbar: Es ist oft nicht möglich, maximale Sicherheitsziele beizubehalten, es müssen dann Kompromisse zwischen Sicherheit und Funktionalität gefunden werden. Diese möglichen Lösungen müssen in einem transparenten Dialog von den Betroffenen und Beteiligten diskutiert und deren Umsetzung letztlich demokratisch legitimiert entschieden werden. Orientieren kann man sich hierbei oft an der konventionellen Welt, in der - oft leidlich - Vertraulichkeit und Funktionalität gegeben sind. Verschlechterungen dieser gegenüber sollte es und darf es nicht geben.

IV. Erwägungen für praktische Lösungen

Hinsichtlich der PIN-Problematik wurde vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) eine Treuhänderlösung vorgeschlagen (7): Der Arzt sollte bei Patienten, die ihre PIN nicht handhaben können, für diese die Aufgabe übernehmen. Wird die PIN in der Patientenakte oder im Arztsystem geschützt gespeichert und nur im Beisein des Patienten, ausgewiesen durch die Vorlage der eGK, genutzt, so entsteht gegenüber der konventionellen Bearbeitung der Patientendaten kein Nachteil. Der Patient, der bisher seine Gesundheit und seine Gesundheitsdaten seinem Arzt anvertraute, muss nun auch der verantwortungsbewussten PIN-Nutzung vertrauen, die zusätzliche Möglichkeiten der Medizindatenverarbeitung eröffnet. Durch Protokollierung kann und muss die treuhänderische Tätigkeit überprüfbar bleiben.

Das Stecken von HBA und eGK sowie die PIN-Eingabe bzw. -Nutzung bei Arzt wie beim Patienten dürfen nicht zum Ritual und nicht zur lästigen Übung werden. Dies setzt neue Praxisabläufe voraus, bei denen die Arztpraxis-Software eine wichtige Rolle spielt. Die Hoffnung, man könne die Telematik-Infrastruktur von der Arztpraxis-Software weitgehend abschotten, dürften sich als unrealistisch erweisen. Es ist richtig, zunächst die Infrastruktur nach den höchsten Standards abzusichern. Die Schnittstellen zu externen Systemen, also z.B. zum Arzt- oder Krankenhausrechner, können über eine sichere Voreinstellung des Konnektors weitgehend in den Griff gebracht werden. Es dürfte aber schon mittelfristig kein Weg daran vorbeiführen, teilweise auf die Sicherheit der externen Systeme vertrauen zu müssen, so wie dies heute generell der Fall ist. Dies gilt z.B., wenn den Patienten die Möglichkeit der Nutzung bestimmter Funktionalitäten über das Internet eingeräumt werden soll (In der Diskussion steht ein sog. PIN@home-Verfahren.). Bewegt sich diese Sicherheit nicht mehr in der staatlichen Verfügungsmacht, so kann sie doch hergestellt werden, z.B. über die - staatlich geregelte - Auditierung bzw. Zertifizierung der eingesetzten Verfahren oder Komponenten.

Es dürfte sinnvoll sein, dass das Stecken der eGK beim Arztbesuch nur einmal bei der

Anmeldung stattfindet und die weitere Nutzung der Karte dem Behandlungsablauf des Patienten folgt, bis dieser die Praxis wieder verlässt und die eGK wieder zurückerhält. Da jedoch dem Kartenbesitz eine hohe Bedeutung beigemessen werden muss, insbesondere wenn Dritte (die Ärzte) über die PIN Verfügungsmacht erhalten, sind an die Regelung des Verbleibs der Karte während des Praxisaufenthalts klare und hohe Anforderungen zu stellen.

Die Autorisierung der einzelnen Datenverarbeitungen lässt sich über die PIN-Eingabe vornehmen und durch den Patienten steuern; sie muss nicht für jedem Arbeitsschritt, wohl aber bei allen relevanten Prozessen gefordert werden. Dies sind die jeweiligen Funktionen der eGK, also die jeweilige Nutzung z.B. des Arztbriefes, des eRezeptes oder der Eintragung in die Patientenakte. Eine einmalige Autorisierung pro Funktion dürfte in der Regel genügen.

Für einzelne Schritte sind aus praktischen Gründen Vereinfachungen vorzusehen. So ist es naheliegend und gesetzlich so vorgesehen, dass es für die Abfrage des Notfalldatensatzes keiner Eingabe der Patienten-PIN bedarf. Für das Schreiben des e-Rezeptes ist die Autorisierung durch den Patienten ebenfalls nicht nötig, da die weitere Verfügung hierüber ohnehin beim Patienten liegt. Bei den sonstigen Anwendungen ist dagegen zumindest eine einmalige Freigabe nötig; beim Arztbrief ist es evtl. angesagt, im Interesse der Transparenz für den Patienten jede einzelne Übermittlung der Daten an einen anderen Arzt vom Patienten bestätigen zu lassen.

Unterschieden werden muss und kann zwischen Lese- und Schreibbefugnissen. Für das Schreiben, nicht nur des Rezeptes, muss es keine übermäßigen Anforderungen geben, ebenso wie bei der bisherigen ärztlichen Dokumentation, die ohne Einschaltung des Patienten erfolgt. Hier kommt es auf die Authentisierung des Arztes durch seine digitale Signatur an. Insofern könnten dem Arzt sogar zeitversetzte Schreibmöglichkeiten gegeben werden, dass er also nicht sofort während des Arztbesuchs, sondern in einem definierten Zeitkorridor oder nach einem definierten Verfahren auch danach Arztbriefe verfassen oder Eintragungen in die elektronische Patientenakte vornehmen kann.

Erfolgt eine Bevollmächtigung des Arztes durch den Patienten zur Eingabe der PIN, so bedarf es nicht nur eines geordneten Verfahrens bei der Erteilung, sondern auch eines solchen beim Entzug der Vollmacht. Diese Frage ist von Relevanz auch für die PIN-Änderung, die z.B. auch dadurch nötig werden kann, dass das PIN-Geheimnis in der Arztpraxis kompromittiert wurde. Da der Vorgang der PIN-Änderung mehrere bevollmächtigte Ärzte tangieren kann und da davon auszugehen ist, dass dieser nur selten stattfindet, können und müssen hier höhere Anforderungen gestellt werden, bei denen eine ~~höhere~~ Einbindung des Patienten ~~erfolgt~~.

Für die problematische Eingabe der Patienten-PIN ist die Bindung dieser PIN an die Nutzung eines oder mehrerer vertrauenswürdiger Ärzte denkbar. Im Interesse hinreichender Transparenz und Wahlfreiheit sollte die Autorisierung des Arztes zur Patienten-PIN-Eingabe in einem standardisierten Formularverfahren schriftlich erfolgen. Die weitere Umsetzung kann dagegen wohl vollautomatisiert stattfinden, also dadurch dass vom Arztsystem die verschlüsselt abgelegte Patienten-PIN über die HBA freigeschaltet wird, wenn die eGK gesteckt ist. Natürlich muss systemseitig

sichergestellt sein, dass der Arzt erkennt, wenn er eine Patienten-PIN setzt, und dass er hierüber eine bewusste Entscheidung trifft. Die - konventionelle - Unterrichtung des Patienten kann über eine Verhaltensregel gesichert werden.

Wichtig für die Entlastung der ärztlichen Tätigkeit und deren Beschränkung auf das Wesentliche ist, dass viele routinemäßige Praxisabläufe mit Bezug zur eGK nicht vom Arzt, sondern vom Hilfspersonal ausgeübt werden können. Hierzu müssen die einzelnen Prozesse beim Arzt bzw. beim Krankenhaus präzise analysiert werden im Hinblick auf die dort auftretenden Risiken und die sich daraus ergebenden technischen bzw. organisatorischen Sicherungen. Gerade hier kann man sich an bewährte Praktiken bei konventionellen Abläufen orientieren. Nach verbindlicher Festlegung und Abschichtung der Befugnisse von Personal und Ärzteschaft, natürlich unter deren Beteiligung, wird diesen mehr Sicherheit und Klarheit gegeben, als bisher besteht.

V. Schlusserwägung

Denk- und Diskussionsblockaden sollten, wenn die Realisierung der medizinischen Telematik-Infrastruktur mit einer eGK ernsthaft gewünscht wird, vermieden werden. Der Beschluss der Versammlung der Bundesärztekammer macht hierfür den Weg frei (8). Sensibilität und Offenheit ist auch auf behördlicher Seite, also sowohl beim zuständigen Ministerium wie bei den beteiligten Datenschutzbeauftragten oder dem Bundesamt für die Sicherheit in der Informationstechnik, gefordert. Klar muss allen sein, dass eine Telematik-Infrastruktur ohne Datenschutz nicht geht. Ebenso klar muss aber sein, dass diese auch funktionieren muss.

(1) Vgl. z.B. die Presseerklärung des Arbeitskreises Vorratsdatenspeicherung vom 18.05.2008, http://www.vorratsdatenspeicherung.de/content/view/221/135/lang,de/; vgl. z.B. aber z.B. www.heise.de vom 07.04.2008: „Die Ängste der Kritiker".
(2) § 291a Abs. 5 S. 2 1.HS: „Durch technische Vorkehrungen ist zu gewährleisten, dass in den Fällen des Absatzes 3 S. 1 Nr. 2 bis 6 der Zugriff nur durch Autorisierung der Versicherten möglich ist. Der Zugriff auf Daten sowohl nach Absatz 2 S. 1 Nr. 1 als auch nach Absatz 3 S. 1 mittels der elektronischen Gesundheitskarte darf nur in Verbindung mit einem elektronischen Heilberufsausweis, im Falle des Absatzes 2 S. 1 Nr. 1 auch in Verbindung mit einem entsprechenden Berufsausweis, erfolgen, die jeweils über eine qualifizierte elektronische Signatur verfügen."
(3) Gesellschaft für Telematikanwendungen der Gesundheitskarte (gematik) GmbH, Die elektronische Gesundheitskarte, whitepaper Sicherheit, Wie werden Gesundheitsdaten in Zukunft geschützt, April 2008.
(4) Thilo Weichert, Medizinische Telematik und Datenschutz, Beitrag zum 111. Deutschen Ärztetag am 22.05.2008 in Ulm, https://www.datenschutzzentrum.de/medizin/gesundheitskarte/20080522-weichert-medizinische-telematik.html.
(5) Vgl. Artikel bei http://www.heise.de 08.04.2008, 11.04., 14.04. und 22.05.2008.
(6) BVerfG, U.v. 27.02.2008, NJW 2008, 822 = MMR 2008, 315 = DVBl 2008, 582
(7) Unabhängiges Landeszentrum für Datenschutz, PIN-Management bei der elektronischen Gesundheitskarte (eGK) v. 17.04.2008.
(8) Beschlussprotokoll unter http://www.baek.de/page.asp?his=0.2.20.5711.6205.6312; vgl. Heike E. Krüger-Brand: Holpriger Weg zum Basiskonsens, Deutsches Ärzteblatt

30.05.2008, A 1164.

Dr. Thilo Weichert ist Landesbeauftragter für Datenschutz Schleswig-Holstein und damit Leiter des Unabhängigen Landeszentrums für Datenschutz in Kiel