

Sebastian Jekutsch

Mythen und Missverständnisse über die eCard eGK

Nachdem die Agenturen früh von einem „Moratorium für die elektronische Gesundheitskarte“ schrieben, im Koalitionsvertrag aber ziemlich unklar ein „Überprüfen der Strukturen“ gefordert wurde, hat sich der neue Gesundheitsminister inzwischen dafür ausgesprochen, dass der im Oktober begonnene Rollout der ersten Version weitergehen soll. Die bisherigen Funktionen, so das Argument, entsprächen der altbekannten Krankenversicherungskarte und die sei ja unkritisch. Neu geprüft werden sollen also vor allem die neuen Funktionen der Karte, Patientenakte, Notfallausweis, eRezept, Arztbrief, sowohl aus Anwendersicht – siehe Probleme mit der PIN und der Langsamkeit, die FfF-Kommunikation berichtete – als auch aus Datenschutzsicht. Vielleicht ist es also an der Zeit, über ein paar Mythen und Missverständnisse aufzuklären, wobei wir mal so tun, als seien alle versprochenen bzw. angedrohten Funktionen schon Realität.

Mythos: Meine Gesundheitsdaten stehen auf der Karte

Oft wird von „auf die Karte speichern“ geschrieben, aber es kommt nur wenig auf die Karte, sie hat auch nur wenig Speicherplatz. Direkt auf der Karte stehen nur die üblichen Versicherten-daten und – wenn gewünscht – die Notfalldaten. Der Rest sind lediglich Verweise auf Daten, die verschlüsselt in großen Rechenzentren irgendwo im Land gespeichert sind. Dazu braucht es zwei wichtige Datensätze ebenfalls auf der Karte: Den Schlüssel zum Ver- und Entschlüsseln und ein Logbuch der Zugriffe auf die Karte und damit indirekt auf die Daten.

Missverständnis: Meine Gesundheitsdaten sind im Internet gespeichert

So hat es sogar die Gesellschaft für Informatik in einer Stellungnahme aus dem Jahr 2005 formuliert. „Im Internet gespeichert“ ist natürlich ähnlich simpel gedacht wie „das Internet ausdrucken“. Wahr ist, dass kein neues physikalisches Netz aufgebaut wurde für die Gesundheits-Telematik, das wäre viel zu teuer geworden, genutzt werden daher genau die Wege, die auch ein Internetzugang nutzt. Die Kommunikation findet aber nicht mit den üblichen Internetanwendungsprotokollen (http, ftp) statt, auch wenn die Kommunikationsbasis in der Tat TCP/IP ist. Realisieren tut das der *Konnektor* beim Arzt, der zwischen Lesegerät und Internetzugang geschaltet wird, sobald die Karte Online-Funktionen haben wird. Dass man sich später die Gesundheitsdaten des Nachbarn er-google-n können wird, ist ein Märchen.

Ungenau: Die Daten liegen auf einem zentralen Server

Das ist fast richtig. Oben wurde schon erwähnt, dass fast nichts auf der Karte selbst steht. Verteilt werden die anderen Daten auf verschiedene Server, die eRezepte zum Beispiel woanders als die Patientenakten. Im Grunde macht es auch keinen Unterschied, wo etwas gespeichert ist, wichtig ist, ob es einen von allen Stel-



len aus einheitlichen Zugriff auf die Daten gibt. So sind all die Webseiten auf der Welt auf wer weiß wie vielen Servern verteilt, die Infrastruktur erlaubt es aber, dass ich mit http einen homogenen Zugriff auf alle Seiten habe. Das ist quasi zentral, und die Kritik daran greift: Eingebrochen wird auf Datenbanken ja auch nicht, indem man die Festplatten klagt, sondern man schafft sich Zugriff von außen über die Datenleitungen.

Mythos: Wenn der zentrale Server gehackt wird, sind die Daten aller Patienten bekannt

Das geht nicht, weil auf den Servern praktisch nur Datenmüll steht. Die Gesundheitsdaten sind nämlich verschlüsselt – und jeder Patient hat einen eigenen Schlüssel. Selbst der kritischste Informatiker wird nicht behaupten, dass man einen dieser Schlüssel knacken könnte, geschweige denn alle. Man muss pro Patient also an den Schlüssel ran. Der Schlüssel ist nur auf der Karte des Patienten. (Genauer steht es beim nächsten Mythos.) Er verlässt auch nie die Karte, denn die Karte verschlüsselt die Daten selbst, sie ist ein kleiner Computer. Somit ist zwingende Vor-

aussetzung für das Entschlüsseln der Daten eines Patienten der zumindest kurzfristige Besitz seiner Karte. Die anderen Voraussetzungen sind: PIN, Lesegerät plus Konnektor und der Heilberuferausweis.

Mythos: Wenn ich die Karte verliere, sind meine Daten weg

Die reine Lehre der IT-Sicherheit sagt: Ja, natürlich! Denn die Daten auf den Servern sind zwar nicht weg, aber mit der Karte ist die einzige Stelle weg, auf der der Schlüssel zum Entschlüsseln gespeichert ist. Die Realität ist leider anders: Das eGK-Gesetz schreibt vor, dass die Daten wiederherstellbar sein müssen. Das heißt, die Schlüssel aller Patienten müssen noch woanders gespeichert sein; dies ist sicherlich die größte Sicherheitslücke der elektronischen Gesundheitskarte. Wenn die Karte weg ist, sollen Daten damit umgeschlüsselt werden können, d.h. der Patient bekommt eine neue Karte mit neuem Schlüssel. Die alt-verschlüsselten Daten müssen dann vorher mit einem zentralen Dienst passend neu verschlüsselt worden sein.

Dabei ist diese Sicherheitslücke eigentlich gar nicht nötig, denn die Gesundheitsdaten sind noch woanders gespeichert: Bei den Ärzten. Die schaffen ihre Akten und ihre Praxis-IT nämlich nicht ab, dort bleibt alles wie es war. Verliert man seine Daten, könnte man sie sich also bei den Ärzten wieder zusammensuchen, die eRezepte eingeschlossen. Weg wären dann nur die Notfalldaten, die evtl. speziell gesetzten Zugriffsrechte für die Daten und die Daten, die Patienten selbst auf der Karte gespeichert haben.

Missverständnis: Die PIN ist der Schlüssel

Die PIN ist ein weiteres Sicherheitsmerkmal. Man kennt das von der EC-Karte: Wenn man die Karte verliert oder sie geklaut wird, dann hilft das dem Dieb erstmal nicht, denn die Server rücken die Daten nur raus, wenn eine passende PIN mitgeschickt wird. Die Daten kommen weiterhin verschlüsselt in der Arztpraxis an und werden erst in der Karte entschlüsselt, weil auf dieser der Schlüssel steht. Die PIN steht selbstredend nicht auf der Karte. PIN und Schlüssel haben rein gar nichts miteinander zu tun.

Mythos: Die Krankenkasse kann meine Daten lesen

Das stimmt nicht. Mit Ausnahme der so genannten Versichertenstammdaten (also etwa der Daten, die auch jetzt schon auf der Krankenversichertenkarte stehen), die die Kasse selbst auf die Karte schreiben lässt, kann die Krankenkasse nichts lesen, wenn der Patient es nicht will. Die Kassen haben nicht einmal einen Heilberuferausweis, geschweige denn, dass sie die Schlüssel zu den Daten ihrer Kunden hätten. Die Kasse bekommt aber

dennoch wegen der Abrechnungsnotwendigkeit mit dem Arzt ziemlich viel von den Patienten mit. Das ist heute auch schon so.

Mit dem Gesetz, das auch die Karte einführt, ist die Möglichkeit neu entstanden, dass die Kassen bessere Statistiken über ihre Patienten führen können. Dazu werden einige der Gesundheitsdaten pseudonymisiert, d.h. ein Patient taucht nur noch als Geschlecht + Alter + Wohngegend +... auf. Die endgültige Festlegung dieses Pseudonyms steht noch aus, die bisherigen Ideen geben aber einigen Anlass zur Kritik. Dies sollten wir kritisch beobachten.

Missverständnis: Die Krankenkasse bekommt jedesmal sofort mit, wenn ich beim Arzt bin

Dieses Gerücht basiert auf der Tatsache, dass bei jedem Einstecken der Gesundheitskarte in das Lesegerät eines Arztes oder Apothekers die oben erwähnten Versichertenstammdaten geprüft werden. Es könnte nämlich sein, dass die Karte gesperrt ist oder dass der Zuzahlungsstatus sich geändert hat oder einfach nur die Adresse des Patienten. Deshalb werden die Daten auf der Karte von zentraler Stelle aus aktualisiert. Die aktuellen Daten stellen in der Tat die Krankenkassen zur Verfügung, nicht aber die Anwendung und den Server, die dieses Update übernehmen.

Diese Überprüfung der Stammdaten ist übrigens nicht Teil des derzeitigen Rollouts. Die erste Version der Gesundheitskarte kommt noch komplett ohne Netzzugang aus.

Unsinn: Meine Gesundheitsdaten sind sicher

Nur nicht existierende Daten sind sicher vor Missbrauch. Das klappt in unserem Fall jetzt und in Zukunft nur, wenn man nie zum Arzt geht.

Ungenau: Wenn meine Karte geklaut wird, hat der Dieb Zugriff auf meine Daten

Der Dieb braucht auch einen Heilberuferausweis, deren PIN, die dazu passenden Zugriffsrechte, Lesegerät plus Konnektor – all dies ist bei einem Arzt des Patienten – und die PIN der Gesundheitskarte. Aber dann kann es losgehen. Leichter wird ein Missbrauch, wenn die private Nutzung der Karte am heimischen PC oder an speziellen öffentlichen Terminals, so genannten Kiosken, ermöglicht werden sollte. Auch hier sind die Pläne noch nicht konkret genug, dass man sich ein klares Bild des Risikos machen könnte.



Sebastian Jekutsch

Sebastian Jekutsch ist FfF-Mitglied. Wenn noch Unklarheiten plagen, oder wer weitere Mythen vermutet, der nutze bitte den Kontakt: sj@fiff.de.

Unwahrscheinlich: Wenn ich nicht mitmache bei der Patientenakte und anderem, dann erhöht die Kasse zur Strafe die Beiträge

Laut Gesetz ist das verboten. Es wird oft als Argument benutzt, dass man Gesetze verändern kann, siehe Pläne mit den Mautdaten. Damit lässt sich natürlich jedes Gesetz diskreditieren. Wir sollten aufpassen, wen wir in die Legislative wählen.

Gefahr: Wenn das Internet zusammenbricht, bricht auch das Gesundheitssystem zusammen

Es soll stets einen konventionellen, papierbasierten Ersatzbetrieb geben. Allerdings ist wohl zu erwarten, dass sich früher oder später die Telematik-basierten Geschäftsprozesse derart verfestigen, dass eine Abhängigkeit entsteht. Das gilt jetzt schon für viele andere Bereiche.

Verwechslung: Die Abkürzung für die elektronische Gesundheitskarte ist e-Card

e-Card bezeichnet eigentlich eine Signaturkarte für die Bürger für eGovernment-Prozesse, d.h. eine Möglichkeit, Dokumente elektronisch zu unterschreiben und somit behördliche Vorgänge (z.B. Steuererklärungen) elektronisch und online erledigen zu können. Für die Gesundheits-Telematik ist eine solche Signaturfunktion lediglich bei den Heilberuferausweisen (HBA) vorgesehen (Arzt unterschreibt eRezepte u.ä.), nicht bei der eGK des Patienten. Sie soll laut Gesetz allerdings technisch dafür geeignet sein.

Die eGK kann also noch zur e-Card werden. Dann würde sie in Konkurrenz treten zum elektronischen Personalausweise (ePA) und der so genannten JobCard, die als elektronischer Sozialversicherungsausweis z. B. ALG-II-Anträge noch effizienter ablehnbar machen wird. Es gibt also noch viele Anlässe, der IT-Industrie staatlicherseits weitere Konjunkturpakete zu verschaffen.

*erschienen in der FfF-Kommunikation,
herausgegeben von FfF e.V. - ISSN 0938-3476
www.fiff.de*