Gründe, um eine zugeschickte eGK OHNE Bild zurückzuschicken.

Diese Begründung darf und soll hemmungslos weitergegeben werden.

S t a n d : März 2 0 1 5

Bitte verwenden Sie einfach, was auf SIE zutrifft.

Absender

An die
Krankenkasse...
Postfach
Ort

Ort, Datum

eGk zurück – Vers.-Nr.: ….

Sehr geehrte Damen und Herren,

zunächst möchte ich meine Zufriedenheit mit den Leistungen der …...Krankenkasse äußern. Mein Schreiben richtet sich also nicht gegen die …...Krankenkasse, sondern gegen das Vorhaben der Bundesregierung, angestoßen mit dem GMG Gesundheitsmodernisierungsgesetz von 2005, eine Datenbasis mit allen relevanten Patientendaten zu schaffen, also ALLE Patientendaten zentral zu speichern. Das ist ein weiterer Schritt zum gläsernen Bürger und bedeutet die Abschaffung der ärztlichen Schweigepflicht. Beides bin ich nicht bereit mitzutragen.

Aus 2 Gründen muß ich Ihnen heute meine eGK zurückschicken:

1. Die Karte ist ungültig, da gesetzliche Vorgaben nicht erfüllt sind.
2. Der Datenschutz im Zusammenhang mit der eGk existiert NICHT und kann auch niemals existieren.

Zu 1. – ungültige Karte:

Sie haben mir eine ungültige eGK geschickt:

1. sie entspricht nicht den gesetzlichen Vorgaben.
2. sie enthält ein **verfassungswidriges** und damit **unzulässiges Personenkennzeichen,** nämlich die lebenslang gültige Krankenversicherungsnummer

Im § 291, Abs. 2 SGB V hat der Gesetzgeber festgelegt, daß nur noch Krankenversicherungskarten MIT Lichtbild ausgestellt werden dürfen. Daran hat sich bis heute nichts geändert.

Die mir zugeschickte eGK verstößt durch das fehlende Lichtbild also gegen :

1. § 291a Abs. 2 und 3 i. V. m. § 291 Abs. 2 und 2a SGB V
2. § 3 Abs. 1 der Anlage 4 a zum BMV-Ä
3. Anhang 1, Abs. 1.2 der Anlage 4 a zum BMV-Ä.

Sie werden sicher nachvollziehen können, daß ich nicht die Abschaffung der ärztlichen Schweigepflicht durch Annahme einer (ungültigen) eGK unterstütze, denn nichts anderes bedeutet der derzeitige Aufbau der Telematik-Infrastruktur zur eGK, u. a. mit geplanten Anwendungen, die mit der eGK gar nichts zu tun haben – s. u. Begründung 2, e-health-Gesetzentwurf.

Der Titel "Elektronische Gesundheitskarte" ist übrigens eine Irreführung. In Wirklichkeit geht es nicht um die Karte, sondern der Kern des Projektes ist ein gigantisches, deutschlandweites IT-Netzwerk mit zentralen (bzw. funktionell zentralen) Großcomputern zur Patientendatenspeicherung. Wo diese Server stehen, wird bis heute verschwiegen. Diese könnten in Deutschland, aber auch in den USA oder anderen Ländern stehen.

Tatsächlich, im neuen System liegen Patientendaten nicht mehr im geschützten Raum Hausarztpraxis, sondern irgendwo auf einem **Zentralrechner,** auf den 120.000 Arztpraxen, 60.000 Zahnarztpraxen und Psychotherapiepraxen, 3.000 Krankenhäuser, 300 Krankenkassen und 22.000 Apotheken und deren Mitarbeiter Tag und Nacht potentiellen Zugriff haben müssen. Dazu kommen eine unbekannte Anzahl von EDV-Wartungsfirmen und die Betreiber der Server. (NSA und GCHQ sind übrigens schon „drin" – später mehr dazu)

Selbst eine eGK *mit* Foto wäre rechtswidrig, da auch sie den gesetzlichen Anforderungen nicht entspricht, weil keine identitätsgeprüften Fotos verwendet wurden und werden, obwohl der § 291, Abs. 2 SGB V verlangt, dass auf der Krankenversichertenkarte u. a. „*Unterschrift und Lichtbild des Versicherten"* aufgebracht werden.

Der Arzt ist nach der **Anlage 4a des BMV-Ä, Anhang 1, Ziffer 1.2 verpflichtet die Identität des Versicherten zu prüfen.** Eine solche Identitätsprüfung durch den Arzt ist aber nur möglich, wenn bereits bei der Herstellung der eGK ein identitätsgeprüftes Lichtbild verwendet worden ist, was bis heute definitiv NICHT der Fall ist.

Der Arzt kann also die Identität gar nicht überprüfen und macht sich somit evtl. strafbar nach § 203 StGB (Ärztliche Schweigepflicht), wenn er sich auf die Daten der eGK verläßt und vielleicht auch noch Patientendaten per Internet überträgt (Versichertenstammdatenmanagement).

Die hier vertretene Rechtsauffassung wurde durch das 2014 bekannt gewordene Gutachten der Kassenärztlichen Bundesvereinigung (KBV) bestätigt.

Zu 2. – nicht existierender Datenschutz der eGK:

Begründung 1)

Nach der heutigen Sachlage muß davon ausgegangen werden, daß die versprochene Datensicherheit

1. nicht existiert und
2. niemals existieren kann

Dies hat der **GKV-Spitzenverband** am 20. 1. 2015 in der ZDF-Sendung **Frontal 21** zum Thema Datenschutz bei der eGK selbst zugegeben.

Antwort des GKV-Verbandsprechers, Florian Lenz zur obigen Frage: (Ab Minute 8.30)
„Wir wissen, daß in der Vergangenheit Fehler gemacht worden sind, daß nicht korrekt mit Daten umgegangen worden ist...

Und weiter...(ab Minute 8.50)
„Wir können nicht völlig ausschließen, daß an irgendeiner Stelle irgendwo jemand aus Versehen oder mit Absicht etwas mit Daten falsch macht."

Quellen:
http://www.stoppt-die-e-card.de/exit.php?url_id=706&entry_id=288 und
https://www.youtube.com/watch?v=WlEpaP-TY9g

Wie leichtfertig die Krankenkassen mit Patientendaten heute schon umgehen, belegen der telefonische und der Online-Service. Beim Telefonat reichen auch schon der Name und das Geburtsdatum. So ist schon eine ECHTE *eGK mit dem Bild des „Krümelmonsters“* aus der Sesamstraße ausgestellt worden.

Der Verlust der KV-Karte kann also recht einfach zum Datenmißbrauch genutzt werden – und ist es auch schon, ein Telefonat genügt. Sollte also jemand an meine persönlichen Gesundheitsdaten, bzw. heutzutage einfach nur an meine Versicherungsnummer gelangen, kommt das einem **Identitätsdiebstahl** gleich. Das kann bei kriminellem Ausnutzen existenzvernichtende Folgen haben.

Begründung 2)

Gemalto und Giesecke & Devrient, beide führend bei der Ausgabe der eGK, gelten seit 2010 als gehackt: *(Warum Verschlüsselung knacken, wenn man den Schlüssel hat?!)*

Meldung vom 20. Februar 2015: (netzpolitik.org)
Schon im Gründungsjahr von MHET, 2010, verkündete GCHQ stolz seinen Erfolg in einer Präsentation:

> **„GEMALTO – Erfolgreich mehrere Maschinen verwanzt und wir glauben, dass wir ihr gesamtes Netzwerk haben.“**

Seit Jahren kopieren also NSA und GCHQ bei den Herstellern von SIM-Karten und Smart Cards die zugehörigen Schlüssel ab. Damit können sie die übertragenen Informationen mitlesen und manipulieren.

Übrigens manipulieren die Schnüffler auch die Abrechnungs-Server der Netzbetreiber. So können sie Daten und SMS zu und von fremden Endgeräten übermitteln, OHNE dass es in den Rechnungsdaten erscheint.

Auch Gemaltos deutscher Mitbewerber Giesecke & Devrient (eGK) wird als Angriffsziel erwähnt, und es darf angenommen werden, dass in den vergangenen Jahren noch andere Hersteller dazugekommen sind.

Quelle:
https://netzpolitik.org/2015/verschluesselung-knacken-wenn-man-den-schluessel-haben-kann-wie-nsa-und-gchq-sim-karten-keys-stehlen/

Der Einbruch in ein System der höchsten Sicherheitsstufe ist also gelungen.... und seit 2010 bis Februar 2015 völlig unentdeckt !!!

Vor ein paar Tagen noch komplett ahnungslos - und jetzt ist sich Gemalto sicher, dass nichts gestohlen wurde – für wie glaubwürdig halten Sie diese Aussage?

Wenn bis heute dieses jahrelange Datenleck den Betreibern der Firma nicht aufgefallen ist, bedeutet das, dass interne Kontrollen völlig versagt haben müssen. Es gibt also KEINE Sicherheit mit den jetzt ausgegebenen elektronischen Karten.

Begründung 3)

Aus internen Mails der **CSC Deutschland Solutions GmbH** geht hervor, daß die Firma an allen großen IT-Vorhaben der Bundesregierung beteiligt ist. Die Mutterfirma **CSC** (USA) **ist einer der wichtigsten IT-Dienstleister des US-Geheimdienstes NSA** (praktisch die *„EDV-Abteilung der*

NSA“), **u. a. an der Entwicklung von Spähprogramen des US-Nachrichtendienstes beteiligt.**

Philipp Müller, Public Affairs Director von CSC, hat telefonisch indirekt die Echtheit der E-Mails bestätigt:

> *„Wir finden, es gehört nicht zum guten Ton, interne E-Mails zu veröffentlichen.“*
>
> (Allein in den vergangenen vier Jahren der letzten Regierung unter Angela Merkel zwischen 2009 und 2013 bekam die CSC Deutschland genau 100 Aufträge von zehn unterschiedlichen Ministerien und dem Bundeskanzleramt.)

Nach den Bestimmungen des PATRIOT Act sind auch ausländische (US) Töchterfirmen nach dem US-Gesetz verpflichtet, Zugriff auf ihre Server zu gewähren; selbst dann, wenn lokale Gesetze dies untersagen.

Die Firma *CSC Deutschland Solutions GmbH* ist bereits mehrfach durch ungefilterte illegale Datenweitergabe unangenehm aufgefallen und steht heftig in der Kritik.

Dieser Firma wird Zugang zu praktisch allen großen IT-Vorhaben der Bundesregierung gewährt?!

Quelle:
https://netzpolitik.org/2014/interne-e-mails-csc-freut-sich-ueber-neue-vertraege-mit-behoerden-trotz-no-spy-erlass-und-medialen-anschuldigungen/

Selbst so hochspezialisierte Firmen wie Google, Microsoft oder Sony konnten Datenklau nicht verhindern. Für wie hoch halten Sie die Wahrscheinlichkeit, daß dies einem halbstaatlichen Unternehmen mit ca. 2 Mill. offiziell Zugriffsberechtigten und eine unbekannten Zahl nicht offiziell Zugriffsberechtigter gelingt?

Im **e-Health-Gesetzentwurf** ist derzeit folgendes zu lesen: (März 2015)

Der Austausch von Gesundheitsdaten – auch mit nicht-ärztlichen Leistungserbringern – soll so gestärkt werden. […] Die bisherige Regelung, wonach in der Telematikinfrastruktur der eGK gespeicherte Gesundheitsdaten ausschließlich zum Zweck der Versorgung der Patienten genutzt werden dürfen, würde durch die Hintertür abgeschafft.

Im Klartext:
Durch das geplante **e-Health-Gesetz** werden die (zentral gespeicherten) Patientendaten an Versicherungen, Pharmaindustrie, Behörden, Forschungs- und Entwicklungsprojekte, etc. weitergeleitet. (sämtliche Arbeitgeber dürften an den Daten brennend interessiert sein). Spätestens jetzt dürfte klar sein, daß der Datenschutz bei der eGk durch das e-Healt-Gesetz aufgehoben und der **gläserne Patient** Wirklichkeit wird.

In diesem Zusammenhang ist die Äußerung des **Geschäftsführers der Gematik**, Arno Elmer sehr interessant. Elmer überraschte Anfang 2013 in einer Diskussion betr. eGK mit der skeptischen Sichtweise: **"Wir bauen nur die Autobahn. Wenn der Gesetzgeber die Daten haben will, dann ändert er die Gesetze und holt sie sich."** Klingelt's ?!

Es dürfte wohl klar sein, worum es bei der eGK wirklich geht, oder?!

Ich meine, dass ich nun deutlich genug gemacht habe, dass sich mein Schreiben nicht gegen die …..Krankenkasse richtet und ebenso, daß ein Datenschutz bei der eGK nicht existiert.

Freundliche Grüße nach Hamburg