

## **eGK Aktuell**

### **Infopost zur Einführung der elektronischen Gesundheitskarte – Ausgabe 1, Juli 2009 – Thema Datensicherheit –**

#### **Es geht los: Einführung der eGK ab 1. Oktober 2009**

Die Einführung der elektronischen Gesundheitskarte (eGK) nimmt Fahrt auf. Am 01. Oktober 2009 beginnt in der Region Nordrhein der sogenannte Basis-Rollout und die ersten Versicherten werden mit der elektronischen Gesundheitskarte ausgestattet. Viele Versicherte stehen der neuen Karte jedoch unsicher und skeptisch gegenüber. Sie fühlen sich unzureichend informiert. eGK Aktuell informiert Sie von nun an in regelmäßigen Abständen über die wichtigsten Aspekte rund um die neue elektronische Gesundheitskarte.

Mit dem so genannten Basis-Rollout beginnt am 1. Oktober 2009 in der Region Nordrhein die Ausgabe der elektronischen Gesundheitskarte (eGK) an die Versicherten. Alle Vorarbeiten seitens der gematik und der Industrie wurden geleistet, so dass ein breites Spektrum an zugelassenen Kartenlesegeräten zur Verfügung steht. Gemäß den gesetzlichen Vorschriften wurde auch eine Vereinbarung getroffen, nach der die Kosten für die Anschaffung der Kartenlesegeräte und die Installationskosten von den Krankenkassen zu tragen sind.

#### **Datenschutz und Datensicherheit haben oberste Priorität**

Noch immer gibt es allerdings Stimmen, die mit Hinweis auf vermeintliche Sicherheitsrisiken für eine Verzögerung der eGK-Einführung plädieren. Diese Befürchtungen sind unbegründet. Die deutsche eGK unterscheidet sich gerade dadurch von ähnlichen Projekten in anderen Ländern, dass Datenschutz und Datensicherheit konsequent am Anfang aller Überlegungen stehen. Eine Reihe ineinander greifender Sicherheitsprinzipien sorgen für höchst mögliche Sicherheit. Tatsächlich dürfte es weltweit kaum ein medizinisches IT-Projekt mit einem so umfassenden Sicherheitskonzept geben.



## Sicherheitsprinzipien

### 1. Der Patient entscheidet selbst

Egal, ob ein Versicherter mit einer Krankenversichertenkarte oder mit seiner Gesundheitskarte zum Arzt geht: an der Behandlung ändert das nichts. Bei der eGK werden jedoch die Zugriffsrechte in die Hände der Versicherten gelegt – im wahrsten Sinne des Wortes. Anwendungen, bei denen es um persönliche medizinische Daten geht – die Speicherung von Notfalldaten oder von Arzneimitteln – sind konsequent freiwillig. Und wenn der Versicherte sich zur Nutzung dieser Angebote entschließt, behält er dank eGK den Schlüssel zu seinen Daten in der Hand: Er und niemand sonst entscheidet, wem die Daten zugänglich gemacht werden.

### 2. Das Zwei-Karten-Prinzip

Auch hier das Wichtigste zuerst: Um behandelt zu werden, benötigt der Versicherte keine PIN. Wenn er später einmal zusätzliche, freiwillige Anwendungen nutzen will, dann benötigt er zusätzlich zu seiner Karte noch eine nur ihm bekannte Geheimzahl. Die Kombination aus Karte und PIN ist von ec-Karten und Mobiltelefonen bekannt und hat sich millionenfach bewährt. Um wirksam zu verhindern, dass Versicherungen oder Arbeitgeber einen Versicherten (illegalerweise) „überreden“, seine Daten offen zu legen, dürfen zudem nur Angehörige von Heilberufen (Ärzte, Zahnärzte, Psychotherapeuten, Apotheker) die Daten einsehen – mit einer eigenen Chipkarte, dem elektronischen Heilberufsausweis (HBA). Nur wenn beide Karten – die eGK des Versicherten und der HBA des behandelnden Arztes, Psychotherapeuten oder des Apothekers – im Lesegerät stecken, ist der Zugriff auf persönliche medizinische Daten möglich. Später wird es möglich sein, dass der Versicherte Zugriffsrechte vergibt und der Arzt damit auch in Abwesenheit des Versicherten auf die Daten zugreifen kann.

### 3. Verschlüsselung und ständige Anpassung

Sensible Patientendaten werden bei der Verwendung der eGK mit modernster Sicherheitstechnik verschlüsselt („Kryptographie“). Die Entschlüsselung der Daten ist nur mit Hilfe der eGK des jeweiligen Patienten möglich. Wichtig: Mit der Weiterentwicklung der Computertechnik werden diese und andere technische Sicherheitsmaßnahmen immer wieder dem aktuellen Stand der

Sicherheitstechnik angepasst. Dabei handelt es sich um eine der wichtigsten Aufgaben der gematik. Das Bundesamt für Sicherheit in der Informationstechnik veröffentlicht dazu jährlich verbindliche Vorgaben („technische Richtlinie TR-03116“) zur Sicherheit von kryptographischen Verfahren.

#### **4. Sichere Transportwege**

Dank verschlüsselter Speicherung der Gesundheitsdaten ist das Sicherheitsniveau bei der eGK so hoch, dass die besten Rechner schätzungsweise mehrere Milliarden Jahre arbeiten müssten, um sie zu entschlüsseln. Mit dem Aufbau der eGK-Infrastruktur entsteht erstmals im deutschen Gesundheitswesen ein nach allen Seiten abgesichertes Kommunikationsnetz, das die Daten zusätzlich zur Verschlüsselung nach außen abschirmt. Um an dieses Netz angeschlossen zu werden, muss eine medizinische Einrichtung zertifizierte und registrierte Geräte („Konnektoren“) einsetzen und darf ausschließlich über verschlüsselte Kanäle („virtuelle private Netzwerke“, VPN) kommunizieren. Dieses System geht auf Grund des Schutzbedarfes der personenbezogenen medizinischen Daten um ein Vielfaches über die Sicherheitsanforderungen bspw. von Internetplattformen für Onlinebanking hinaus – von der Übertragung von Patientendaten per Fax oder E-Mail gar nicht zu reden.

#### **5. Kontrolle durch den Versicherten**

Bei der eGK werden nicht nur alle technischen Register gezogen, um sensible Daten zu schützen. Der Versicherte kann auch jederzeit kontrollieren, wer auf seine Daten zugegriffen hat. Dazu wird ein so genannter Protokoll-Dienst („Audit“) eingerichtet, der Zugriffe auf die Daten penibel protokolliert. An Patientenkiosken können die Versicherten zukünftig jederzeit nachvollziehen, wer wann auf ihre Daten zugegriffen hat.



## Nachgefragt: Die häufigsten Bedenken

### **„Patientendaten können von Megaservern entwendet werden“**

Bei der eGK werden keine zentralen „Megaserver“ aufgebaut, die sämtliche Patientendaten enthalten. Stattdessen ist ein verteiltes System vorgesehen, bei dem die Daten an unterschiedlichen Orten gespeichert und verarbeitet werden. Sensible Patientendaten sind zudem verschlüsselt, sodass sie auch dann nicht einsehbar wären, wenn ein Rechenzentrum „geknackt“ würde. Bei Pflichtdaten wie etwa den Rezeptdaten wird mit Pseudonymen gearbeitet, um diese Daten besonders zu schützen.

### **„Es gibt keine unabhängige Evaluation der Sicherheit“**

Das ist falsch. Das Fraunhofer Institut FOKUS hat der gematik im Jahr 2008 bescheinigt, dass die getroffenen Sicherheitsmaßnahmen einen bestmöglichen Zugriffsschutz auf die Patientendaten bieten. Als Reaktion auf den 111. Deutschen Ärztetag wurde zudem ein weiteres Sicherheitsgutachten in Auftrag gegeben, dessen Ergebnisse Ende des Jahres vorliegen werden. Unabhängig davon werden sicherheitsrelevante Komponenten der eGK-Infrastruktur vom Bundesamt für Sicherheit in der Informationstechnik (BSI), der obersten deutschen Behörde in Sachen IT-Sicherheit, zertifiziert.

### **„Andere politische Verhältnisse können die Sicherheit aufweichen“**

Auch dies ist ein Einwand, der vom 111. Deutschen Ärztetag formuliert wurde. Die eGK wurde so konzipiert, dass die Patientenrechte auch künftig nicht politischer Willkür unterworfen sind, sondern unabhängig kontrolliert werden können. Auch eine Veränderung politischer Gegebenheiten ist für den Versicherten nicht relevant: nur er kann seine Daten mit Hilfe seiner Gesundheitskarte entschlüsseln. Neben dem Bundesdatenschutzbeauftragten und dem BSI wachen auch unabhängige Institutionen im Beirat der gematik darüber, dass die Patientenrechte und die Interessen des Datenschutzes auch künftig gewahrt bleiben, zum Beispiel die Verbraucherzentrale Bundesverband und die Bundesarbeitsgemeinschaft Selbsthilfe.



## Das sagen die Experten

Der **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit** (BfDI), **Peter Schaar**, macht sich für die Einführung der eGK stark, weil diese dank ihrer Sicherheitsprinzipien den Datenschutz und die Datensicherheit im deutschen Gesundheitswesen verbessere. Bereits am 7. Juli 2005 äußerte er sich in einer Rede sehr positiv zum §291a, SGB V: *„Die [...] datenschutzrechtlichen Parameter finden Sie hier allesamt wieder, und deshalb halte ich diese Regelung für so gelungen.“*

In dem im Jahr 2007 vorgelegten 21. Tätigkeitsbericht geht der BfDI auf einige Grundprinzipien der eGK genauer ein: *„Das Zugriffs-konzept ist technisch so konzipiert, dass das Patientengeheimnis [...] gewahrt bleibt. [...] Auch die Grundprinzipien der Datenvermeidung und Datensparsamkeit werden eingehalten.“* Diese positive Grundhaltung zur eGK findet sich aktuell auch im 22. Tätigkeitsbericht des BfDI wieder, der am 21. April 2009 vorgestellt wurde.

In einem mit der Nachrichtenagentur AP geführten Gespräch ist Schaar im April explizit auf den Basis-Rollout der eGK eingegangen und hat sich **gegen weitere Verzögerungen ausgesprochen**: *„Ich sehe keinen Grund für die [von einigen Ärzten geforderte] Aussetzung“,* so Schaar. Das sei aus Sicht des Datenschutzes eher schädlich: *„Die derzeitige Versichertenkarte ist schlechter abgesichert als die elektronische Gesundheitskarte. Denn jetzt werden die Daten nicht verschlüsselt.“*

Auch **Stefan Etgeton, Bundesverbraucherschutzzentrale**, betonte in einem Interview im November 2008 die hohe Datensicherheit der eGK: *„Es empfiehlt sich aber in jedem Fall, bei der Einrichtung einer elektronischen Patientenakte auf die Angebote zurückzugreifen, die für die neue Gesundheitskarte zertifiziert wurden. Sie sind damit automatisch Teil einer gesicherten Telematikinfrastuktur, also eines Systems, das in etwa so sicher sein soll wie das der Geheimdienste.“*  
(Interview mit der TAZ am 24. November 2008)

## **Technisch überholt – Die alte Krankenkassenkarte hat ausgedient**

**Seit langem schon wird von Datenschützern die heute noch gültige Krankenversichertenkarte bemängelt.** Sie ist technisch längst überholt und ihre Sicherheitsvorkehrungen sind nicht mehr hinreichend. Sensible Versichertendaten wie z.B. Versicherten- und Sozialstatus sind nicht ausreichend vor Zugriffen unbefugter Dritter geschützt. Die alte Karte wird deshalb nur noch für einen Übergangszeitraum geduldet. Nach dem Willen der Datenschützer soll sie schnellstmöglich durch die neue elektronische Gesundheitskarte abgelöst werden. Denn im Gegensatz zur jetzigen Versichertenkarte ist der Schutz der Daten der Versicherten mit der eGK nachweislich gewährleistet:

1. Für die eGK kommen nur sicherheitsüberprüfte Komponenten (eGK, HBA, Lesegeräte, Konnektoren) zum Einsatz. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) überprüft die Komponenten hinsichtlich dieser Eigenschaften.
2. Die Daten werden bei jedem Versicherten individuell mit Hilfe der eGK und der PIN verschlüsselt. Niemand, der nicht vom Versicherten dazu berechtigt wurde kann diese Daten lesen.
3. Nur berechtigte Personen, also Angehörige der Heilberufe, haben Zugriff auf die Daten des Versicherten, nachdem der Versicherte sie dazu berechtigt hat. Sie benötigen hierfür ihren Heilberufsausweis.
4. Der Versicherte muss dem Zugriff auf seine Daten zustimmen. Dies tut er durch Übergabe seiner eGK an den Arzt oder Apotheker oder indem er eine entsprechende Berechtigung erteilt.
5. Die Daten des Versicherten werden – je nach Bestimmung – auf voneinander getrennten Servern unterschiedlicher Betreiber gespeichert, so dass sie nicht zusammengeführt werden können. Diese Daten sind jedoch immer auch noch in der Arztpraxis oder Klinik vorhanden.
6. Die Grundsätze der Datensparsamkeit und Datenvermeidung werden eingehalten.

Das bedeutet, dass im Rahmen der freiwilligen Anwendungen nur diejenigen Daten gespeichert werden, die der Versicherte auch speichern will und im Rahmen der Pflichtenwendungen nur diejenigen Daten gespeichert werden, die für die Aufgabe (z.B. Leistungsnachweis gegenüber dem Arzt, Rezepteinlösung) unbedingt erforderlich sind.

### **Fazit**

- è Die Einführung der elektronische Gesundheitskarte (eGK) ist ein grundlegender Schritt zur Modernisierung des Gesundheitswesens. Mit den Investitionen in die Infrastruktur dieses Zukunftsprojekts legt der Gesetzgeber den Grundstein für ein zukunftsfähiges und effizientes Gesundheitssystem.
- è Mit Hilfe der eGK wird Kommunikation innerhalb des Gesundheitssystems sicherer. Sie ist kein Sicherheitsproblem, sondern die Lösung bestehender Datenschutz- und Sicherheitsprobleme im Gesundheitswesen!
- è Die Vernetzung im Gesundheitswesen findet ohnehin statt. Der Gesetzgeber hat sich entschieden, diese Entwicklung im Interesse der Patientinnen und Patienten nicht einfach geschehen zu lassen, sondern diese durch die Einführung der eGK aktiv zu gestalten.

Die kommende Ausgabe eGK Aktuell wird im Zeichen der Kosten- und Nutzenbewertung der elektronischen Gesundheitskarte stehen...

#### **Herausgeber:**

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Daniel Poeschkens

Tel.: +49 (0) 30 / 400 41-231

Friedrichstr. 136

10117 Berlin

Amtsgericht Berlin-Charlottenburg HRB 96351 B

Geschäftsführer Cord Bartels, Peter Bonerz