Datenschutz und Datensicherheit Ihrer TK-Gesundheitskarte

Die elektronische Gesundheitskarte bietet Möglichkeiten für sicheres Speichern und Austauschen von Informationen. Dabei steht der Datenschutz im Vordergrund. Was bedeutet das?

Schon seit einigen Jahren hat Ihre TK Gesundheitskarte ein Foto und einen Chip. Das ist Ihre "elektronische Gesundheitskarte" (**eGK**). Der Chip auf dieser Karte ist der Grundstein für eine neue, digitale und sichere Kommunikation in der Medizin. Mit der eGK und dem für diesen Zweck geschaffenen Kommunikationsnetz, der "Telematikinfrastruktur" (**TI**), wird das digitale Speichern und Austauschen von medizinischen Informationen möglich.

Dabei ist der Datenschutz von entscheidender Bedeutung. Nur ein verlässlicher **Datenschutz** garantiert, dass Ihre sensiblen Gesundheitsinformationen sicher sind. Er gewährleistet damit das Arztgeheimnis und das Arzt-Patienten-Vertrauensverhältnis.

Das sieht der **Gesetzgeber** genauso. Er hat spezielle Datenschutzregeln für die eGK und die TI festgelegt. Was darin geregelt wurde, erfahren Sie hier.

Viele Anwendungen sind freiwillig

Bei den freiwilligen Anwendungen **entscheiden Sie**, ob Sie diese nutzen oder nicht. Sie können z. B. Ihre Notfalldaten oder Informationen zu eingenommenen Arzneimitteln speichern. Tun Sie es nicht, entstehen Ihnen selbstverständlich keinerlei Nachteile.

PIN-Schutz für freiwillige Anwendungen

Ähnlich wie bei einer Bankkarte werden die freiwilligen Anwendungen durch eine **Geheimnummer** (PIN) geschützt. Die PIN brauchen Sie, wenn die Ärztin oder der Arzt auf die Daten Ihrer Karte zugreifen soll. Mit der Eingabe Ihrer PIN stimmen Sie in jedem einzelnen Fall zu, dass Ihre Daten gespeichert oder eingesehen werden dürfen.

Nur die **Notfalldaten** können von berechtigten Personen auch ohne Ihre PIN ausgelesen werden. Damit ist es möglich, dass im Notfall Ihre Daten zuverlässig und schnell bei Ihrer Behandlung helfen.

Zugriff nur für Berechtigte

Nur wer einen Heilberuf ausübt und einen **Heilberufsausweis** hat, kann Daten auf Ihrer Karte schreiben oder lesen. Der Zugriff ist also nicht allein mit Ihrer eGK und Ihrer PIN möglich, sondern es muss auch diese zweite Karte in das Lesegerät gesteckt werden (**2-Karten-Prinzip**).

Elektronische Signatur

Wenn die Ärztin oder der Arzt Informationen auf Ihrer Karte speichert, müssen sie digital unterschrieben werden. Mit dieser elektronischen **Signatur** wird garantiert, wer die Autorin oder der Autor ist und dass die Information nicht verändert wurde.

Die letzten 50 Zugriffe werden protokolliert

Jede Abfrage Ihrer Daten wird **protokolliert**. Die letzten 50 Zugriffe werden auf Ihrer Gesundheitskarte gespeichert und **nur Sie** können sie sehen.

> Die eGK gilt unter Datenschützern als das sicherste elektronische System außerhalb geschützter Rechenzentren. Es wird laufend geprüft, verbessert und zertifiziert.

Datensicherheit auch durch die Technik

Es wurden bundesweit einheitliche **Technikstandards** verbindlich festgelegt. Diese sorgen dafür, dass auch die Geräte und Vorgänge hinter dem Datenaustausch Sicherheit bieten.

Datensicherheit bei technischen Komponenten

Die eGK und die technischen Geräte werden von der "Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH" (**gematik**) und dem "Bundesamt für Sicherheit in der Informationstechnik" (**BSI**) zertifiziert und zugelassen.

Datensicherheit bei den Netzverbindungen

Das Gesundheitsnetz ist ein **geschlossenes** Netz. Anders als im Internet können in der sogenannten TI Daten nur zwischen registrierten Partnern ausgetauscht werden.

0007805594 - 3514280000000

Die Daten werden bereits beim Speichern verschlüsselt und dann in kleinen, voneinander getrennten Paketen verschickt. Jedes Datenpaket wird erneut verschlüsselt und adressiert. Erst dann wird die Verbindung zum Empfänger hergestellt und nach der Datenübertragung automatisch geschlossen.

Datensicherheit bei der Verschlüsselung

Alle Gesundheitsdaten müssen **hybrid verschlüsselt** werden (siehe Kasten unten). Dadurch werden sie so verändert, dass sie von Außenstehenden nicht mehr dekodiert werden können. Die notwendigen Schlüssel und Zertifikate liegen geschützt auf der eGK.

Symmetrisches Kryptosystem: Für Ver- und Entschlüsselung wird der gleiche Schlüssel benutzt. Die Sicherheit des Verfahrens hängt von der Geheimhaltung des Schlüssels ab. Er muss also über einen sicheren Kanal übertragen werden.

Asymmetrisches Kryptosystem: Beim asymmetrischen Verschlüsselungsverfahren generiert der Empfänger 2 verschiedene Schlüssel: den öffentlichen (zur Verschlüsselung) und den privaten Schlüssel (zur Entschlüsselung). Der öffentliche Schlüssel wird dem Sender zugänglich gemacht, der damit seine Nachricht verschlüsseln kann. Einmal verschlüsselt, kann diese vom Sender nicht mehr entschlüsselt werden. Die verschlüsselte Nachricht kann nun über unsichere Kanäle an den Empfänger geschickt werden. Ohne Kenntnis des Privatschlüssels kann niemand außer dem Empfänger die Nachricht entschlüsseln.

Hybride Verschlüsselung: Bei dieser Methode werden die 2 genannten Verfahren kombiniert und deren Vorteile genutzt. Zunächst werden die Daten symmetrisch verschlüsselt. Danach wird der hierzu verwendete Schlüssel asymmetrisch verschlüsselt. Auf diese Weise ist ein Höchstmaß an Sicherheit gewährleistet.

Sicherheit durch permanente Anpassung

Jeder, der mit Computern oder dem Internet arbeitet, weiß, dass Sicherheit ein Prozess ständiger **Anpassung und Aktualisierung** ist. Darum werden die Richtlinien für die eGK und das Gesundheitsnetz laufend geprüft und bei Bedarf neu definiert.

Datenschützer von Anfang an dabei

Der Gesetzgeber hat von Anfang an eng mit den "Bundesbeauftragten für den Datenschutz und die Informationsfreiheit" (BfDI), den Datenschutzbeauftragten der Länder und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammengearbeitet. Es wurden spezielle **Datenschutzregeln** für eGK und TI festgelegt und die Gesetze dafür geschaffen.

Gesetzliche Regelungen

Wesentliche gesetzliche Grundlagen für die Gestaltung der eGK und des Gesundheitsnetzes, der TI, finden Sie in den folgenden Gesetzestexten:

- Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung (SGB V) – vor allem die §§ 291, 291a und 291b
- Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz (SGB X)
- Bundesdatenschutzgesetz (BDSG)
- Datenschutz-Grundverordnung (DSGVO) – Informationen zur Datenverarbeitung nach Art. 13

Hier erfahren Sie mehr

Weitere Informationen zu Datenschutz und -sicherheit sowie die technischen Vorgaben der TI finden Sie online unter **gematik.de.**

Bei Interesse empfehlen wir Ihnen auch unser Beratungsblatt "Zertifikate und Schlüssel".

0007805594 - 35142800000000