

Ist die elektronische Patientenakte sicher?

Was man aus der Causa ePA für künftig Digitalisierungsprojekte lernen kann

Auch den Hessischen Beauftragten für Datenschutz und Informationsfreiheit erreichten zu Beginn des Jahres Anfragen von Patienten und Ärzten, die aufgrund der Berichterstattung zur elektronischen Patientenakte (ePA) wissen wollten, ob man diese überhaupt noch guten Gewissens einsetzen könne. Diese Sensibilität ist in Anbetracht dessen, dass man der ePA besonders schützenswerte Gesundheitsdaten gemäß Art. 9 der Datenschutz-Grundverordnung anvertraut, nur allzu berechtigt und richtig.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesdatenschutzbeauftragte für Datenschutz und Informationsfreiheit (BfDI) sind in die Ausgestaltung der elektronischen Patientenakte leider nur noch „im Benehmen“ eingebunden – das heißt, beide Kontrollinstanzen müssen im Entwicklungsprozess zwar angehört werden, aber nicht aktiv ihre Zustimmung geben. Ihre Kontrollmöglichkeiten sind somit begrenzt. Laut dem Bundesministerium für Gesundheit wird die ePA erst dann vollständig

ausgerollt, wenn alle noch im Raum stehenden, potenziellen Sicherheitsmängel überprüft und ausgeräumt sind. Das BSI und die BfDI haben aktuell noch Sicherheitsmängel gegenüber dem Bundesministerium für Gesundheit geltend gemacht. Sowohl BSI als auch BfDI halten auf ihren Websites grundlegende und aktuelle Informationen zur ePA bereit.^{1, 2}

Der Schaden, der durch die aufgedeckten Mängel in Sachen ePA entstanden ist, ist leider groß. Gerade im Hinblick auf künftige Digitalisierungsprojekte zeigt sich damit, dass die Punkte Sicherheit und Datenschutz an erster Stelle stehen müssen, um Vertrauen bei den Anwendern zu schaffen. Leider war diese Priorisierung bei der ePA offenbar nicht der Fall.

Es bleibt zu hoffen, dass die seitens des Chaos Computer Clubs und von anderer Seite aufgedeckten Schwachstellen restlos aufgeklärt und geschlossen werden, um dem Projekt doch noch zu einem guten Start zu verhelfen. Anderenfalls bleibt den Patienten nur die Option, vorerst von ihrem Widerspruchsrecht Gebrauch zu machen oder die ePA mit weniger sensiblen Daten zu befüllen.

Dr. Nils Gaebel

Hessischer Beauftragter für Datenschutz und Informationsfreiheit, Gesundheit und Pflege, Wissenschaft und Forschung, Statistik; Wiesbaden

Private Krankenversicherung & ePA

„In der Privaten Krankenversicherung (PKV) gibt es keine elektronische Gesundheitskarte. PKV-Versicherte gelangen ausschließlich auf digitalem Wege an ihre elektronische Patientenakte. Dafür gibt es die Gesundheits-ID, die in einer separaten App abgelegt ist und die in der Arztpraxis auch für die Übermittlung der Patientendaten genutzt wird. Die vom Chaos Computer Club entwickelten potenziellen Angriffsszenarien setzen vor allem bei der elektronischen Gesundheitskarte an. Insofern wären PKV-Versicherte von diesem beschriebenen Missbrauch potenziell eher nicht betroffen. Unabhängig davon begrüßen wir die geplanten Maßnahmen für eine sichere Nutzung der Telematik-Infrastruktur (TI) und der elektronischen Patientenakte. Dass die Daten sicher verwahrt und Missbrauch und Betrug verhindert

werden, ist eine Grundvoraussetzung für das Vertrauen in die ePA und deren Nutzung. Wichtig ist natürlich auch, dass die Patientendaten innerhalb der Praxissysteme entsprechend geschützt sind. Cybersicherheit ist in diesem Zusammenhang ein wichtiges Thema für alle Leistungserbringer im Gesundheitswesen“, so eine Mitteilung von Dr. Anke Schlieker, Verband der Privaten Krankenversicherung e.V. Berlin, auf Anfrage der HÄBL-Redaktion: Aufgrund anderer rechtlicher Rahmenbedingungen, aber auch aufgrund von gesetzlichen Verzögerungen insbesondere was die Ausstattung aller Privatversicherten mit einer Krankenversichertennummer (KVNR) angeht, gebe es für die PKV-Branche beim Zugang zur TI und der Ausstattung der Versicherten mit ePA/E-Rezept zeitliche Verzögerungen. (red)

1 <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/E-Health/Elektronische-Patientenakte/elektronische-patientenakte.html> oder Kurzlink: <https://tinyurl.com/2m3bveb4>

2 <https://www.bfdi.bund.de/DE/Buerger/Inhalte/GesundheitSoziales/eHealth/elektronischePatientenakte.html> oder Kurzlink: <https://tinyurl.com/69j8vr7x>

Antwort der Bundesregierung zu den Sicherheitsbedenken bei der elektronischen Patientenakte

Um mögliche Hacker-Angriffe auf die elektronische Patientenakte (ePA) zu verhindern, sollen in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) kurzfristig zusätzliche Sicherheitsvorkehrungen umgesetzt werden. So solle der Zugriff auf das Aktensystem während der Pilotphase ausschließlich auf die in den Modell- und Pilotregionen teilnehmenden und verifizierten Leistungserbringer beschränkt werden, heißt es in der Antwort (20/14939) der Bun-

desregierung auf eine Kleine Anfrage (20/14668) der AfD-Fraktion. Vor dem bundesweiten Rollout bei allen Leistungserbringern würden zudem weitere technische und organisatorische Lösungen zur Erhöhung der Sicherheit umgesetzt und abgeschlossen. Die zuständige Behörde (gematik) habe mit dem BSI einen Plan erarbeitet, wie der Start der neuen ePA, die Pilotierungsphase und der sich daran anschließende bundesweite Rollout so flankiert werden könne, dass

ein angemessenes Sicherheitsniveau erhalten bleibt.

Die gematik und das BSI hätten das Risiko möglicher Angriffsszenarien bewertet. Dementsprechend wäre ein Angriff zwar „möglich“, sei in der Realität aber eher unwahrscheinlich. Es müsste ein hoher technischer Aufwand betrieben werden mit einem Identitätsdiebstahl, um die erforderlichen Mittel zu erlangen.

(red/Stand 11.02.2025)