



711.395.2

13. Dezember 2018

**Prüfung einer elektronischen Gesundheitsakte durch die  
Berliner Beauftragte für Datenschutz und Informationsfreiheit**

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit prüft derzeit eine durch Krankenkassen und private Krankenversicherungen geförderte elektronische Gesundheitsakte auf die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit. Das Produkt ermöglicht es Patientinnen und Patienten, Unterlagen und Daten zu ihrer Gesundheit und zur medizinischen Behandlung zu sammeln. Erbringer medizinischer Leistungen können auf Anfrage Patientendaten in die elektronische Gesundheitsakte einstellen. Auch Krankenkassen und -versicherungen können die Akte zur gezielten Ansprache ihrer Versicherten verwenden, deren Einverständnis vorausgesetzt.

Im Rahmen dieser Prüfung wurden verschiedene Mängel in Bezug auf die Information der Versicherten, die Einholung von Einwilligungen, die Gewährleistung der Datensicherheit und die Durchführung einer Datenschutz-Folgenabschätzung festgestellt. Der Anbieter erhält nun Gelegenheit, sich zu den festgestellten Mängeln zu äußern und diese zu beseitigen. In Teilen ist dies bereits geschehen.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit weist in diesem Zusammenhang bereits jetzt Ärztinnen und Ärzte, die aufgefordert werden, Daten in die Gesundheitsakte einzustellen, auf Folgendes hin:

Medizinische Leistungserbringer sind nicht dazu verpflichtet, patientenbezogene Daten in eine elektronische Gesundheitsakte einzutragen. Zwar räumt Art. 15 Abs. 3 Satz 2 Datenschutz-Grundverordnung betroffenen Personen das Recht ein, eine elektronische Kopie der sie

betreffenden Daten zu erhalten. Die Leistungserbringer können jedoch den Weg zur Übermittlung der elektronischen Kopie selbst wählen, solange hierdurch der Empfang für die betroffene Person nicht erschwert wird.

Medizinische Leistungserbringer dürfen patientenbezogene Daten nur dann an Betreiber elektronischer Gesundheitsakten übermitteln, wenn die entsprechende Anforderung tatsächlich von der behandelten Person ausgeht. Hiervon müssen sich die Leistungserbringer selbst und in eigener Verantwortung überzeugen, wobei insbesondere die Echtheit der Schweigepflichtentbindungserklärungen überprüft werden muss. Eine Übermittlung ohne eine solche Genehmigung stellt nicht nur einen Datenschutzverstoß dar, sondern auch eine Verletzung der ärztlichen Schweigepflicht.

Jede Übermittlung patientenbezogener Daten muss den Anforderungen an die Datensicherheit genügen. Nicht nur die Diagnose und die Art der Behandlung bedürfen einer besonderen Vertraulichkeit, sondern bereits die Tatsache, dass überhaupt eine Behandlung durch einen bestimmten Leistungserbringer stattgefunden hat. Die Datensicherheit muss sowohl vom Betreiber der elektronischen Gesundheitsakte gewährleistet werden, als auch vom medizinischen Leistungserbringer.

Patientenbezogene Daten sollten vom Leistungserbringer vor der Übermittlung so verschlüsselt werden, dass nur die behandelte Person selbst die Entschlüsselung durchführen kann. Der Leistungserbringer hat in diesem Fall dafür Sorge zu tragen, dass die Verschlüsselung nur mit dem von der behandelten Person zur Verfügung gestellten Schlüssel erfolgt, und muss die Verwendung des richtigen Schlüssels im Zweifelsfall nachweisen können.

Unverschlüsselte patientenbezogene Daten sollten nicht auf Arbeitsplatzrechnern verarbeitet werden, die ungehindert auf das Internet zugreifen können. Dies entspricht den Empfehlungen der Kassenärztlichen Bundesvereinigung und der Bundesärztekammer.

Maja Smoltczyk:

„Elektronische Gesundheitsakten bieten Patientinnen und Patienten die Möglichkeit, ihre Gesundheitsdaten an zentraler Stelle zu speichern und zu verwalten. Die potentiellen Vorteile, die sich hieraus ergeben können, dürfen jedoch nicht zulasten des Datenschutzes und der Datensicherheit gehen. Die datenschutzrechtlichen Anforderungen müssen daher bereits bei der Konzeptionierung entsprechender Angebote beachtet und umgesetzt werden.“