Welchen Schutz brauchen sensible Gesundheitsdaten?

Elektronische Gesundheitskarte mit elektronischer Patientenakte und elektronische Gesundheitsakte

Das Terminservice- und Versorgungsgesetz (TSVG), das der Bundestag am 14. März 2019 beschlossen hat, verpflichtet die Krankenkassen, spätestens ab 2021 den Versicherten elektronische Patientenakten anzubieten. Auf die darin gespeicherten Daten sollen die Versicherten auch mittels Smartphone oder Tablet zugreifen können. Sie sollen also auch ohne Arzt Zugriff auf ihre Daten haben.

Was bedeutet diese Aktualisierung der elektronischen Gesundheitskarte (eGK) für die Versicherten? Wollen sie ihre Gesundheitsdaten überhaupt auf zentralen Servern speichern lassen? Worin unterscheidet sich die ePatientenakte der eGK von der elektronischen Gesundheitsakte, die viele Krankenversicherungen den Versicherten bereits anbieten?

Geschichte der Einführung der eGK

Anfang der 2000er Jahre begann die Diskussion darüber, dass das Gesundheitswesen und vor allem die Kommunikation aller Beteiligten untereinander modernisiert werden müssten. Typische Stichworte dazu waren: Mehr Wirtschaftlichkeit und Effizienz, Verringerung von Missbrauchspotentialen, Erhöhung der Eigenverantwortung der Patienten, mehr Leistungstransparenz. Tatsächlich war die Erhöhung der Wirtschaftlichkeit im Gesundheitsbereich ein zentrales Ziel. Die Kontrolle von Ärzten und Patienten hängt eng damit zusammen. Von Verbesserung der medizinischen Versorgung ist nachrangig und eher im „Akzeptanzmanagement“ die Rede. Das Ganze war Teil des 1999 gestarteten Reformprogramms „Moderner Staat – Moderne Verwaltung“, mit dem die Digitalisierung in die staatliche Verwaltung der Bürger Einzug nehmen sollte.

Die rechtlichen Voraussetzungen zur Einführung einer elektronischen Gesundheitskarte (eGK) wurden 2004 mit dem „Gesundheitsmodernisierungsgesetz“ geschaffen. Zum 1. Januar 2006 sollte die Karte die alte Krankenversicherungskarte ablösen. Von einigen Seiten wurde Protest gegen diese Planungen organisiert. Viele Versicherten boykottierten die eGK, indem sie kein Foto abgaben. Mehrere Ärztekongresse verabschiedeten Resolutionen gegen die Einführung der eGK. Alle – oder fast alle - gesetzlich Versicherten haben inzwischen die elektronische Gesundheitskarte, da der Druck auf die Versicherten stetig erhöht wurde. Erst die eGK der zweiten Generation, die seit dem 1. Januar 2019 allein gültig ist, unterstützt kryptographische

Verfahren und medizinische Fachanwendungen. Technische Probleme und Fragen begleiteten den Einführungsprozess von Anfang an.

Mit dem TSVG wird nun neuer Druck aufgebaut. Aktuell warnen die Krankenkassen, dass mit dieser Fristsetzung, also mit der Einführung von elektronischen Patientenakten 15 Jahre nach der vorgesehenen Einführung, ein Zeitdruck geschaffen würde, der kontraproduktiv und überstürzt sei. Die Erwartungen der Patienten könnten enttäuscht werden. https://www.heise.de/newsticker/meldung/Krankenkassen-warnen-vor-ueberstuerzter-Einfuehrung-der-Patientenakte-4359189.html

Zugleich haben die Krankenkassen längst begonnen, eigene elektronische Gesundheitsakten anzubieten bzw. die Angebote von privaten Unternehmen ihren Versicherten vergünstigt zur Verfügung zu stellen.

Das mag auf den ersten Blick absurd und widersprüchlich klingen, hat aber durchaus auch eine Logik. Viele Interessen stehen im Gesundheitssektor gegeneinander und erschweren die Entwicklung. Im Streit um die eGK geht es einerseits um die Frage, ob und wie Gesundheitsdaten gespeichert werden dürfen. Es geht aber nicht nur um die Frage der sicheren Speicherung, es geht auch um einen grundlegenden Umbau des Gesundheitssystems. Es geht um eine Ökonomisierung des ganzen Bereichs, der bei der Privatisierung von Krankenhäusern anfängt und beim Handel mit Daten noch längst nicht aufhört. Zugleich werden die Bürger und Bürgerinnen immer mehr verantwortlich gemacht dafür, wie es ihnen gesundheitlich geht und was sie für ihre Gesundheit tun. Das hat Kontrolle zur Folge und fördert eine Entwicklung der Entsolidarisierung. Die Entsolidarisierung in der Finanzierung des Gesundheitssystems gehört ebenfalls zu den Folgen. Die Interessen von Patienten stehen sicherlich nicht im Vordergrund, auch wenn zumindest die Politik so tut, als wenn sie deren Interessen in den Mittelpunkt rücken wollte.

Selbstverständlich ist eine „Modernisierung" der Abläufe und Kommunikationswege im Gesundheitssektor sinnvoll. Aber über die Formen der Speicherung von Gesundheitsdaten und den Nutzen, den dies für Versicherte hat, muss öffentlich gestritten werden.

Im gegenwärtigen werbenden Neusprech ist davon die Rede, dass man einfach mal erst anfangen muss. Es würde nur eine Autobahn gebaut und man könne später sehen, wofür diese nützlich ist und wohin sie führt. Digitalisierung hätte schon an anderen Stellen so funktioniert, dass man mal erst ein nur bedingt taugliches Projekt in die Welt setzt und dieses dann weiterentwickelt. Es scheint allerdings äußerst fragwürdig, einen solchen Weg in der zentralen Speicherung von Gesundheitsdaten zu verfolgen.

Sensible Gesundheitdaten, ...

- Gesundheitsdaten sind extrem sensible Daten, die individuelle Merkmale enthalten (können), die lebenslang erhalten bleiben. Sie können zur Stigmatisierung und

Benachteiligung beitragen, eröffnen Möglichkeiten des racial profiling in diversen Hinsichten. Gemeint ist hier der umfassende Begriff des racial profiling, der Benachteiligungen unter verschiedenen Aspekten berücksichtigt. Je mehr Aspekte von Gesundheit, von individuellen Anlagen, Hinweise auf potentielle Krankheiten – etwa durch die Genforschung – erkannt werden können, desto mehr gilt es diese Sensibilität der Daten zu berücksichtigen.

- Gesundheitsdaten können so sensibel sein, dass außer einem Arzt, dem der Patient vertraut und der gesetzlich zum Schweigen verpflichtet ist, und ihm selbst niemand darüber informiert sein soll. Wenn es etwa um genetische Veranlagungen geht, sind es nicht mehr nur „meine" Daten, sondern auch die von Verwandten. Angehörige haben ein Recht auf Nichtwissen.

Der Verlust von Zugangsdaten ist immer heikel und macht die Verletzlichkeit in der digitalen Welt deutlich. Der „Verlust" von Gesundheitsdaten kann erhebliche Konsequenzen mit sich bringen. Die Informationen gehen dabei selbstverständlich nicht verloren, sondern sie werden im Gegenteil öffentlich und können unbegrenzt kopiert werden. Das kann einen tiefgreifenden Einschnitt bedeuten, der den Rest des Lebens verändert. Reisemöglichkeiten könnten eingeschränkt werden, Versicherungen stehen nicht mehr zur Verfügung, die Aussicht auf einen Job wird gemindert …

Wenn Informationen über die Gesundheit von Menschen einmal öffentlich sind, können diese Informationen nicht mehr zurückgeholt werden. Kein neues Passwort schützt die Daten. Das ist grundlegend anders als beim Verlust des Schlüssels zu Kontodaten. Der Verlust ist begrenzt, das Konto kann neu geschützt werden. Gesundheitsdaten, die öffentlich bekannt wurden, sind für immer in der Welt und nicht rückholbar. Deshalb ist nicht ein vergleichbarer Schutz wie bei Bankkonten notwendig, sondern ein um vieles höherer.

… an denen es vielfältige Interessen gibt:

- Arbeitgeber (auch unter dem Deckmantel, Arbeitnehmer zu ihrem eigenen Schutz entsprechend ihrer Möglichkeiten einsetzen zu können)
- Versicherungen (angepasste Tarife, statt solidarische Versicherungen)
- Staat (Kontrolle, Vorhersage, Abwehr von Gefahren)
- Unternehmen (gezielte Werbung)
- Forschung und speziell Pharmafirmen (Eine bedeutende Ausnahme vom Datenschutz in der DSGVO betrifft die medizinische Forschung, die inzwischen vor allem große Datenmengen braucht. Forschung ist jedoch nicht neutral, sondern oft ausgerichtet an Interessen derer, die sie fördern.

Exkurs: Die NAKO (Nationale Kohorte) ist ein Beispiel für den Versuch, möglichst viele Bürger für langfristige Studien zu gewinnen. Der Datenschutz wird in diesem Feld ausgehebelt. Während die informierte Zustimmung Voraussetzung für die Nutzung von Daten ist, wird hier eine Zustimmung für die Zukunft und völlig unkonkretisierte weitere Forschungsvorhaben eingeholt. (Streit um die Formen der Zustimmung: von informierter Zustimmung – über dynamic consent bis hin zu broad consent, also allgemeiner Zustimmung für alle zukünftigen Projekte.)

... die vom uralten Arztgeheimnis geschützt sind.

Gesundheitsdaten stehen traditionell unter dem besonderen Schutz des uralten Arztgeheimnisses,

- Bisher lagern die Daten in der Arztpraxis. Ärzte haben ein Zeugnisverweigerungsrecht. Und sie haben die Pflicht, dafür zu sorgen, dass Unbefugte diese Daten nicht einsehen können. Im abgeschlossenen Raum einer Praxis ist dies möglich, wenn es auch angesichts der Digitalisierung sicherlich immer schwieriger wird. (Darüberhinaus gibt es teilweise lokale Kommunikationsnetze und in Krankenhäusern sind komplexe Formen der Datenspeicherung entwickelt.)
- Notwendig ist, dass Informationen zwischen den Beteiligten im Gesundheitswesen ausgetauscht werden können. Gesundheitsdaten müssen dafür sicher – digital – weitergeleitet werden können. Dies geschieht auch häufig. Von denen, die jede Kritik an der eGK lächerlich machen wollen, wird jedoch behauptet ohne die zentrale Speicherung käme nur der Einsatz von Faxgeräten infrage. Sichere Verschlüsselungsmethoden in der direkten Kommunikation gibt es.
- Manchmal könnte es hilfreich sein, wenn Krankheitsdaten so gespeichert sind, dass jederzeit ein Zugriff darauf möglich ist. Es ist aber zu fragen, ob dies für alle Patienten notwendig ist oder ob es andere Speicherungsmöglichkeiten für diese speziellen Anforderungen gibt.

Regelungen mit der elektronischen Gesundheitskarte

- Mit dem Gesundheitsmodernisierungsgesetz ist im Sozialgesetzbuch V der § 291 eingeführt worden, der die Einführung der elektronischen Gesundheitskarte und dessen Nutzung regelt. Im Folgenden beziehe ich mich vorrangig auf die Fragen zu den Gesundheitsdaten und vernachlässige Fragen um den Abgleich der Stammdaten (administrativen Daten). Diese Anforderung ist erst später als weitere Notwendigkeit in das Gesetz eingefügt worden.

- Vorgesehen ist die Speicherung der Daten auf zentralen Servern. Die Daten sollen selbstverständlich verschlüsselt gespeichert werden. Der Zugang zu den Daten soll nur über die gemeinsame und gleichzeitige Nutzung von elektronischer Gesundheitskarte und Heilberufsausweis möglich sein. Beide Ausweise sollten mit einer 6-stelligen Geheimnummer geschützt werden. (Zu den aktuellen Änderungen später mehr.)
- Das Erstellen einer Patientenakte soll freiwillig sein.
- Der Patient entscheidet, welche Daten in der Patientenakte gespeichert werden. Der Arzt wird weiterhin seine Diagnosen selbst speichern und für die Abrechnung mit der Krankenkasse notwendige Daten übertragen.
- Vorgeschrieben ist das e-Rezept, also die digitale Übermittlung der Rezeptdaten an die Apotheke. Auf die damit verbundenen Probleme gehe ich hier nicht weiter ein. Der elektronische Medikationsplan zur Arzneimittelsicherheit ist dagegen freiwillig,
- Freiwillig ist auch die Speicherung von Notfalldaten.

Wie steht es nun um den Schutz der Daten?

- Können zentral gespeicherte Daten wirklich auf Dauer geschützt werden? Prinzipiell nein, aber es können immer neue Verfahren der Sicherung entwickelt werden. An der Spezifizierung der elektronischen Gesundheitskarte ist das BSI beteiligt und soll dauerhaft für die Sicherheit sorgen. Voraussetzung für die Sicherheit ist jedenfalls, dass diese Spezifizierung auch tatsächlich den geprüften Angaben gemäß umgesetzt wird. Skepsis ist geboten.
- Die bisherigen Erfahrungen zeigen, dass gegenwärtig die Sicherheit nicht gewährleistet ist. Das bezieht sich selbstverständlich nicht auf die elektronische Gesundheitskarte, mit der noch keine Gesundheitsdaten gespeichert werden können.

  Immer wieder kommt es zu Datenpannen. Patientendaten werden für viel Geld im Darknet verkauft. In den USA war schon jeder zehnte von Datenverlust betroffen. In Singapur gelangten Anfang 2019 über eine zentrale Datenbank die Namen von 14.000 HIV-Patienten an die Öffentlichkeit. https://www.medinside.ch/de/post/hiv-daten-leck-zeigt-elektronisch-gespeicherte-gesundheitsdaten-sind-extrem-heikel 2018 sollen in Singapur Angreifer Gesundheitsdaten von 1,5 Millionen Menschen erbeutetet haben. https://netzpolitik.org/2018/singapur-angreifer-erbeuten-gesundheitsdaten-von-15-millionen-menschen/

  In England kam es mehrfach zu „Datenpannen“, bei denen Gesundheitsdaten öffentlich wurden. In Norwegen wurden 2018 3 Millionen Patientenakten gestohlen und in Dänemark wurden 2016 irrtümlich Gesundheitsdaten an die chinesische Visastelle

geschickt. https://www.br.de/nachrichten/deutschland-welt/elektronische-patientenakte-experten-warnen-vor-datenmissbrauch,RHrsXfG

Prinzipielle Fragen müssen gestellt werden:

- Jede **zentrale Speicherung** solch sensibler Daten trägt zur Erhöhung von Gefahren bei. Eine große Anzahl von Gesundheitsdaten mit einem Coup zu erbeuten, ist attraktiver als diese einzeln ausfindig zu machen.
- Wenn die Schlüssel der individuellen eGK und des Heilberufsausweises für den Fall des Verlustes „irgendwo" gelagert werden, ist dies eine potentielle Einbruchstelle. Würde keine Kopie des Schlüssels gespeichert, würden die Daten jedoch im Falle des Verlustes des Schlüssels unzugänglich.
- Wenn wir zentrale Datensammlungen überhaupt zulassen wollen – vieles spricht ganz prinzipiell dagegen – stellt sich auch die Frage, in wessen Händen die Daten liegen sollen, wem wir also vertrauen würden. Soll es die öffentliche Hand sein oder Hochschulen oder unabhängige Beteiligte? Wollen wir diese Daten den Krankenkassen anvertrauen (die selbstverständlich schon jetzt eine Menge Daten gespeichert haben)? Die Daten, die mit der eGK gespeichert werden, sollen auf Rechnern der Krankenkassen gespeichert werden.

Ganz praktische Fragen und die daraus folgenden Gefahren

- Können sich Patienten und Heilberufler die Passwörter merken und können dies auch kranke Patienten, demente Patienten ...? Soll dann die Arztpraxis zum Hüter der Passwörter der Patienten werden?
- Wenn der Patient tatsächlich nach seiner Meinung entscheidet, welche Daten mit Hilfe der eGK auf Servern gespeichert werden, dann ist die Datensammlung für Ärzte nichts wert. Sie können sich auf keinen Fall darauf verlassen, dass die wichtigen Informationen zur Verfügung stehen und sind auf die Informationen angewiesen, die sie auch bisher haben. Der immense finanzielle Aufwand der Entwicklung der eGK lohnt sich aber nur (Kosten-Nutzen-Analyse der Beratungsfirma Booz/Allen/Hamilton, siehe: https://www.ccc.de/de/elektronische-gesundheitskarte), wenn die weitaus meisten Versicherten eine elektronische Patientenakte anlegen, diese nutzen und die Daten vollständig sind.

Also stellt sich die Fragen, wie lange die Freiwilligkeit erhalten bleibt und mit welchen Mitteln dafür gesorgt werden wird, dass die Daten vollständig sind. Auch Anreize und Druckmittel sind denkbare Möglichkeiten, um dies zu erreichen.

Aktuell wird noch einmal sehr betont, dass die Patienten „Herr" ihrer Daten bleiben sollen. Sie sollen mit dem Arzt entscheiden, was gespeichert wird. Sie können jedoch gemäß den

Änderungen, die mit dem Terminservice- und Versorgungsgesetz eingeführt werden, auch allein auf die Daten zugreifen und diese verändern. Dafür sollen sie eine Möglichkeit erhalten, über Smartphone oder Tablet auf die Daten zuzugreifen. Das verstärkt die Fragen sowohl nach der Zuverlässigkeit der Daten für den Arzt als auch die nach der Sicherheit der Daten.

Es klingt so bürgerfreundlich, wenn die Autonomie des Einzelnen betont wird. Endlich wird man als Patient und Versicherter ernst genommen, behält man alle Daten in der eigenen Hand. Über die Verantwortung, die einem aufgebürdet wird, spricht keiner. Der Versicherte aber kann gar nicht wissen, welche Interpretationen aus den Gesundheitsdaten im Einzelnen möglich sind.

Darüber hinaus werden Menschen dadurch auch erpressbar. Um eines Vorteils willen könnten sie Arbeitgebern den Zugang zu Informationen eröffnen oder Versicherungen Daten weitergeben. Eine Menge solcher Szenarien wäre denkbar.

Ärzte dagegen wissen, welche Informationen aus den Daten abgelesen werden können und müssen sich im Rahmen des rechtlich Zulässigen auf ihre ärztliche Schweigepflicht berufen.

Diese Bedenken finden gerade erneut Aufmerksamkeit bei BSI und Datenschutzbehörde. Ganz aktuell hat das BSI mitgeteilt, dass es die vorgesehenen Authentifizierungsverfahren, mit denen per Smartphone auf die elektronische Patientenakte zugegriffen werden kann, als „neuralgischen Punkt für die gesamte nachfolgende Sicherheitskette" betrachtet. Das Ärzteblatt (2.5.2019) zitiert aus dem Brief des BSI an das Gesundheitsministerium: „Die Gesamtsicherheit des Systems wird hierdurch deutlich verringert." Zugleich liegt dem Ärzteblatt ein Schreiben des Datenschutzbeauftragten vor, der ein juristisches Problem sieht. Mit „dem neuen Verschlüsselungskonzept (könne) ohne eine rechtliche Klarstellung die Möglichkeit eröffnet werden, im Rahmen strafrechtlicher Ermittlungen ohne Wissen des Betroffenen Gesundheitsdaten zu erheben, da sich die elektronische Patientenakte nicht im Gewahrsam des zeugnisverweigerungsberechtigten Arztes befinde."
https://www.aerzteblatt.de/nachrichten/102771/Behoerde-sieht-Sicherheitsluecken-bei-mobilem-Authentifizierungsverfahren-fuer-elektronische-Patientenakte

Anmerkungen zu den Notfall- und Medikamentendaten

Die Fragen danach, was mit sensiblen Daten passiert und wie sie geschützt werden sollen, stellt sich nicht erst bei der elektronischen Patientenakte. Auch die Speicherung der Notfalldaten ist freiwillig, aber damit sind ähnliche Fragen verbunden.

Der Notfalldatensatz kann so umfassend sein, dass darin schon eine kleine Patientenakte enthalten ist. Wenn diese Daten nur nach Authentifizierung zugänglich wären, wären sie im Notfall möglicherweise gerade nicht zugänglich. Folglich müssen die Notfalldaten auch ohne Netzzugang lesbar sein.

Ist nicht ein ganz analoger Notfallausweis hilfreicher, der auf die notwendigsten Informationen begrenzt ist? Wenn die Daten offen auf der eGK gespeichert sind, sind sie quasi öffentlich, selbst dann, wenn für das Auslesen ein Heilberufsausweis notwendig ist. Bei fast 400.000 Ärzten in

Deutschland, deren Personal ebenfalls Zugriff hat, ist eine beträchtliche Anzahl von Menschen berechtigt auf Daten zuzugreifen oder kann dies auch ohne Berechtigung tun.

Immer wieder wird behauptet, die Blutgruppe könnte so erfasst werden und für den Notfall bereitstehen. Das ist einer der Werbemythen, der sich hartnäckig hält und dennoch der größte Blödsinn ist. Nie würde sich ein Arzt auf eine solche Angabe verlassen. Er muss die Blutgruppe vor einer Bluttransfusion immer aktuell prüfen.

Auch bei der elektronischen Speicherung der verschriebenen Medikamente, um Unverträglichkeiten und Wechselwirkungen digital zu überprüfen, werden eine Menge Informationen über den körperlichen Zustand zugänglich.

Die Psychopharmaka, die man von dem einen Arzt verschrieben bekommt, möchte man vielleicht dem Augenarzt nicht sichtbar machen. Und die Potenz steigernden Mittel gehen den Zahnarzt nichts an.

Im Zweifel werden sich Patienten selbst die Medikamente besorgen, die sie haben wollen und die Kontrolle umgehen.

Von der „komplizierten“ elektronischen Gesundheitskarte (mit ePatientenakte) zur elektronischen Gesundheitsakte

Die Tatsache, dass sich die Entwicklung der elektronischen Gesundheitskarte lange verzögert und immer wieder zu kontroversen Diskussionen geführt hat, hat private Anbieter auf den Plan gerufen, die in Zusammenarbeit mit den Krankenkassen eigene „elektronische Gesundheitsakten“ anbieten. Die Nutzung dieser Angebote ist freiwillig – sowohl für die Patienten als auch für die Ärzte. Der Vorteil scheint zu sein, dass man den Schutz der Gesundheitsdaten noch weniger genau nehmen muss.

Gegen einen grundlegenden Schutz der Gesundheitsdaten kann man auch einwenden, dass viele Menschen schon längst freiwillig Informationen über ihren Körper und seinen Zustand speichern und weitergeben. Das ist richtig. Deshalb ist es um so wichtiger, sich über die Bedeutung dieser Daten bewusst zu werden und eigene Entscheidungen zu treffen.

Fitness-Tracker und Lifestyle-Apps zeichnen Körperdaten auf und schicken sie ins weltweite Netz, wo sie für alle möglichen Zwecke ausgewertet werden, Sie können nützlich sein für personalisierte Werbung oder gezielte Angebote von Versicherungen. Genauso gut können sich Ablehnungen (z.B. von Arbeitgebern, von Versicherungen etc.) darauf stützen.

Allerdings werden derzeit vor allem diejenigen diese Angebote nutzen, die sich Vorteile davon versprechen, z.B. auch im Rahmen von Bonusprogrammen der Krankenkassen. Aber auch dies hat letztlich Konsequenzen – zunächst für diejenigen, die diese Informationsweitergabe nicht nutzen. Ihnen muss unterstellt werden, dass sie über „schlechtere“ Informationen verfügen. Zugleich werden die jetzigen Nutzer unter der damit verbundenen schleichenden Aufhebung

des Solidaritätsprinzips dann leiden, wenn sie selbst einmal krank werden oder z.B. genetische Untersuchungen potentielle Krankheiten sichtbar machen.

Hinzu gekommen sind also nun noch die elektronischen **Gesundheitsakten,** die von den Krankenkassen unterstützt bzw. angeboten werden.

Diese Möglichkeit ist im Sozialgesetzbuch V vorgesehen.

Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477)

§ 68 Finanzierung einer persönlichen elektronischen Gesundheitsakte

Zur Verbesserung der Qualität und der Wirtschaftlichkeit der Versorgung können die Krankenkassen ihren Versicherten zu von Dritten angebotenen Dienstleistungen der elektronischen Speicherung und Übermittlung patientenbezogener Gesundheitsdaten finanzielle Unterstützung gewähren. Das Nähere ist durch die Satzung zu regeln.

Allerdings hat die damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit am 19.07.2018 in einem Schreiben festgestellt: "Das Zurverfügungstellen einer *elektronischen Gesundheitsakte* (eGA) ist keine gesetzliche Aufgabe der Sozialleistungsträger im Sinne des Sozialgesetzbuches. Die Krankenkassen haben gemäß § 68 SGB V lediglich die Möglichkeit, finanzielle Unterstützung zu einer persönlichen eGA ihrer Versicherten zu leisten. Es handelt sich bei den eGA-Lösungen um ein privates Angebot von Dritten, die weder Sozialdaten im Sinne des § 67 Abs. 1 SGB X verarbeiten noch das Sozialgeheimnis gemäß § 35 SGB I beachten müssen." https://ddrm.de/berliner-datenschutzbeauftragte-prueft-elektronische-gesundheitsakte-von-vivy-nach-wie-vor-grosse-datenschutzrechtliche-maengel/

Das liest sich wie eine Warnung vor dieser Art der Verarbeitung von Gesundheitsdaten.

Über die Gesundheits-App ViVy und deren vielen technischen Lücken liegen mehrere Berichte vor. Allen, die die technischen Details etwas genauer interessieren – nicht nur bei ViVy, sondern auch bei vielen weiteren Angeboten – sei der Vortrag von Martin Tschirsich auf dem chaos communication congress (35C3 2018) im Dezember 2018 empfohlen: „All Your Gesundheitsakten are belong to us" Das Video gibt es im Internet.
https://berlin-ak.ftp.media.ccc.de/congress/2018/h264-sd/35c3-9992-deu-eng-fra-All_Your_Gesundheitsakten_Are_Belong_To_Us_sd.mp4

Mitte September 2018 wurde die Gesundheits-App ViVy gestartet, die inzwischen sowohl Mitgliedern gesetzlicher als auch privater Krankenkassen angeboten wird. Insgesamt sollen 13,5 Millionen Versicherte darauf zugreifen können.

Die Berliner Datenschutzbeauftragte hat diese App geprüft und darüber im Jahresbericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2018 berichtet. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/

jahresbericht/BlnBDI-Jahresbericht-2018-Web.pdf#2019-Datenschutz-Bericht-Berlin-2018-WEB.indd%3A.84874%3A9548

Aus dem Bericht der Berliner Datenschutzbeauftragten:

Der Gesetzgeber erlaubt den Krankenkassen, elektronische Gesundheitsakten zu fördern. Diese sollten dazu dienen, dass Versicherte selbstbestimmt Unterlagen zu ihrer Gesundheit verwahren und in die weitere Behandlung einbringen können. Die beteiligten Krankenkassen und Krankenversicherungen möchten diese Akten ebenfalls gern für die gezielte Ansprache ihrer Versicherten nutzen.

Folgende Warnungen spricht sie aus:

„Nach den von uns unterstützten Empfehlungen der Bundesärztekammer sollten Ärzte unverschlüsselte medizinische Unterlagen nicht auf Rechner überspielen, die freien Zugang zum Internet haben. Derzeit lassen sich der Gesundheitsakte jedoch nur von einem solchen Rechner aus Dokumente hinzufügen.

Schon die Tatsache, dass jemand von einer bestimmten Ärztin oder einem bestimmten Arzt behandelt wird, ist geheim zu halten, da sich daraus Rückschlüsse auf die Art einer Erkrankung ziehen lassen. Die Abfrage der Unterlagen bei den medizinischen Leistungserbringern erfolgte zum Prüfungszeitpunkt jedoch unverschlüsselt. Wir haben den Anbieter aufgefordert, dies zu ändern.“

Die Schlussfolgerung lautet:

„Wir werden im Jahr 2019 auf das Unternehmen einwirken, dass etablierte Standards für die Sicherheit derartiger Dienste durchgängig eingehalten werden und das gleiche Sicherheitsniveau erreicht wird, wie es das Gesetz von den elektronischen Patientenakten erfordert.“

Das klingt nicht so, als sollte man seine Gesundheitsdaten auf diese Weise verarbeiten lassen.

Tschirsich weist in seinem Vortrag nicht nur nach, wie unsicher die Daten gespeichert sind und wie leicht es für Fachleute ist, an Daten heranzukommen. Er macht auch ein anderes Problem deutlich: "Die elektronische Gesundheitskarte ist gescheitert. Stattdessen kommt jetzt die elektronische Patientenakte ...“

Noch bleibt es jedem Bürger und jeder Bürgerin selbst überlassen, ob sie ihre Krankendaten zentral speichern lassen will. Man muss keine der angebotenen Akten nutzen. Es ist auf jeden Fall sicherer, notwendige Daten gesichert auf privaten Datenträgern zu speichern und ansonsten dem Arzt und dem Arztgeheimnis zu vertrauen.

Veränderungen des Gesundheitssystems

Zu bedenken und gesellschaftlich zu diskutieren ist immer neu, wohin die Entwicklungen des Gesundheitssystems gehen.

Auch die eGK dient vor allem einem Umbau des Gesundheitssystems. Verantwortung wird auf den einzelnen Bürger geschoben, der sich aller Risiken – von denen der Krankheit bis zu denen des Datenmissbrauchs - bewusst sein und sich entsprechend verhalten soll. Die durchaus sympathischen Entwicklungen, jedem die Hoheit über seine Daten selbst zuzuschreiben, führen jedoch zu einer schleichenden Aushebelung des Arztgeheimnisses.

„Die öffentliche Gesundheitsversorgung wird zunehmend privatisiert, ökonomisiert und individualisiert. Kostenersparnis, Prävention und individuelle Risikovermeidung sind die gesundheitspolitischen Ziele. Die frühzeitige „Erkennung" vermeintlicher individueller Gesundheitsrisiken soll Menschen befähigen, Krankheiten vorzubeugen, macht sie jedoch auch individuell für den Erhalt der eigenen Gesundheit verantwortlich." https://www.gen-ethisches-netzwerk.de/biopolitik-und-bioethik/gesundheitssystem

Hinweis

Der Kurzfilm „Chancen und Risiken von Gesundheitsdaten" von Meret Kaufmann ist einer von drei zur Endrunde nominierten Einreichungen für den Datenschutz Medienpreis (DAME) des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.: https://www.youtube.com/watch?time_continue=5&v=Io_TF2haAmE

Dr. Elke Steven
Geschäftsführerin Digitale Gesellschaft e.V.
Groninger Straße 7
13347 Berlin
digitalegesellschaft.de
@digiges
030 450 840 17
