Geschützte Gesundheitsdaten?

Zentrale Speicherungen werfen Fragen auf – eine Analyse

Elke Steven (Berlin), Soziologin und Geschäftsführerin von Digitale Gesellschaft e.V.

Das Terminservice- und Versorgungsgesetz (TSVG) ist Mitte Mai in Kraft getreten. Es verpflichtet die Krankenkassen auch, den Versicherten elektronische Patientenakten anzubieten – spätestens ab 2021. Was bedeutet das für die Betroffenen?

Anfang der 2000er Jahre begann die Diskussion darüber, dass das Gesundheitswesen und vor allem die Kommunikation aller Beteiligten modernisiert werden müssten. Typische Schlagworte damals: mehr Wirtschaftlichkeit und Effizienz, Verringerung von Missbrauchspotentialen, Erhöhung der Eigenverantwortung der Patienten, mehr Leistungstransparenz.

2006 sollte die elektronische Gesundheitskarte (eGK) die alte Krankenversicherungskarte ablösen. Viele Versicherte boykottierten das, indem sie kein Foto abgaben, und mehrere Ärztekongresse verabschiedeten Resolutionen gegen die Einführung der eGK. Der Druck wurde stetig erhöht, inzwischen haben fast alle Versicherten die Karte. Die zweite Generation der eGK, allein gültig seit 2019, unterstützt nun auch kryptographische Verfahren und medizinische Fachanwendungen. Technische Probleme begleiteten den Einführungsprozess kontinuierlich. Mit dem TSVG wird neuer Druck aufgebaut.

Gesundheitsdaten sind sensibel; je mehr Aspekte von Gesundheit, von individuellen Anlagen, Hinweisen auf potentielle Krankheiten erkannt werden können, desto mehr gilt es, diese Sensibilität zu berücksichtigen. 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. Sind Informationen über die Gesundheit von Menschen einmal öffentlich, können diese nicht mehr zurückgeholt werden. Und an Gesundheitsdaten sind viele interessiert: Arbeitgeber; Versicherungen (angepasste Tarife); Staat (Kontrolle, Vorhersage, Abwehr von Gefahren); Unternehmen (gezielte Werbung); Forschung und speziell Pharmafirmen.

Mit dem »Gesundheitsmodernisierungsgesetz« von 2004 ist im Sozialgesetzbuch V der § 291 eingeführt worden, der die Einführung der eGK und deren Nutzung regelt. Vorgesehen ist die Speicherung der Daten auf zentralen Servern. Der Zugang zu den verschlüsselten Daten soll nur über die gemeinsame und gleichzeitige Nutzung von eGK und Heilberufsausweis möglich sein. Beide Ausweise sollten mit einer 6-stelligen Geheimnummer geschützt werden.

Das Erstellen einer elektronischen Patientenakte soll freiwillig sein. Welche Daten sie speichert, entscheidet der Patient. Der Arzt wird weiter seine Diagnosen selbst speichern und zur Abrechnung mit der Krankenkasse notwendige Daten übertragen. Vorgeschrieben ist das e-Rezept, also die digitale Übermittlung der Rezeptdaten an Apotheken. Der elektronische Medikationsplan zur Arzneimittelsicherheit ist dagegen freiwillig, ebenso die Speicherung von Notfalldaten.

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 eGK ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) beteiligt.

Noch können mit der eGK keine Gesundheitsdaten gespeichert werden. Internationale Erfahrungen zeigen, dass die Sicherheit gegenwärtig nicht gewährleistet ist. 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. 2018 sollen in Singapur Angreifer Gesundheitsdaten von 1,5 Millionen Menschen erbeutet haben. In England kam es mehrfach zu »Datenpannen«, bei denen Gesundheitsdaten öffentlich wurden. In Norwegen wurden 2018 drei Millionen Patientenakten gestohlen, und in Dänemark wurden 2016 irrtümlich Gesundheitsdaten an die chinesische Visastelle geschickt.

Eine große Anzahl von Gesundheitsdaten mit einem Coup zu erbeuten, ist attraktiver als diese einzeln ausfindig zu machen. Wenn wir zentrale Datensammlungen überhaupt zulassen wollen, stellt sich auch die Frage, in wessen Händen die Daten liegen sollen. Soll es die öffentliche Hand sein oder Hochschulen oder unabhängige Beteiligte? Wollen wir diese Daten den Krankenkassen anvertrauen?

Zudem stellen sich ganz praktische Fragen: Können sich Heilberufler und Patienten die Passwörter merken, auch Menschen mit Demenz? Soll dann die Arztpraxis zum Hüter ihrer Passwörter 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. Der immense finanzielle Entwicklungsaufwand lohnt sich aber nur, wenn die weitaus meisten Versicherten eine elektronische Patientenakte anlegen und die Daten vollständig sind. Also stellt sich die Frage, wie lange die Freiwilligkeit erhalten bleibt – und mit welchen Mitteln dafür gesorgt ›

Rechte im digitalen Netz entfalten und bewahren

»Je mehr Menschen sich für Grundrechte im digitalen Raum einsetzen, desto besser.« Das ist die Devise von Digitale Gesellschaft e.V. Der gemeinnützige Verein, gegründet 2010 in Berlin, engagiert sich »für die Realisierung digitaler Potentiale bei Wissenszugang, Transparenz, Partizipation und kreativer Entfaltung« – und »gegen den Rückbau von Freiheitsrechten im Netz«. Zu den Entwicklungen, die der Verein kritisch im Blick hat, gehört die Digitalisierung des Gesundheitswesens. Der nebenstehende Artikel von Elke Steven beruht auf dem 11-seitigen Text »Welchen Schutz brauchen sensible Gesundheitsdaten?«, online zu lesen auf der Internetseite *https://digitalegesellschaft.de*

werden wird, dass die Daten vollständig sind. Anreize und Druckmittel sind denkbar.

Aktuell wird 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 TSVG eingeführt werden, auch allein auf die Daten zugreifen und diese verändern. Dafür sollen sie eine Möglichkeit erhalten, über Smartphone oder Tablet-Computer auf die Daten zuzugreifen. Das verstärkt die Fragen nach Zuverlässigkeit und Sicherheit der Daten. Es klingt bürgerfreundlich, wenn die Autonomie des Einzelnen betont wird. Über die Verantwortung, die einem aufgebürdet wird, spricht keiner.

Das BSI betrachtet die vorgesehenen Authentifizierungsverfahren, mit denen per Smartphone auf die elektronische Patientenakte zugegriffen werden kann, als »neuralgischen Punkt für die gesamte nachfolgende Sicherheitskette«. Das *Deutsche Ärzteblatt (DÄB)* zitierte am 2. Mai aus einem Brief des BSI an das Bundesgesundheitsministerium: »Die Gesamtsicherheit des Systems wird hierdurch deutlich verringert.« Zugleich liegt dem *DÄB* ein Schreiben des Bundesdatenschutzbeauftragten 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«.

Auch die freiwillige Speicherung der Notfalldaten wirft Fragen auf. Wären diese Daten nur nach Authentifizierung zugänglich, 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?

Auch bei der 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. Bundesgesundheitsminister Jens Spahn musste kürzlich zugeben, dass die vorgesehene Möglichkeit der Trennung dieser Informationen nach Zielgruppen bis 2021 jedenfalls technisch nicht möglich sein wird.

Die Tatsache, dass sich die Entwicklung der eGK 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. Diese Möglichkeit ist im Sozialgesetzbuch V vorgesehen. Die Nutzung dieser Angebote ist freiwillig – sowohl für die Patienten als auch für die Ärzte.

Allerdings werden derzeit vor allem diejenigen diese Angebote nutzen, die sich Vorteile davon versprechen, etwa im Rahmen von Bonusprogrammen der Krankenkassen. Aber auch dies hat letztlich Konsequenzen – zunächst für diejenigen, die diese Informationsweitergabe nicht nutzen. Ihnen kann 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 Tests auf potentielle Krankheiten verweisen.

> 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.

Im September 2018 wurde die Gesundheits-App ViVy gestartet, insgesamt sollen 13,5 Millionen Versicherte darauf zugreifen können. Die Berliner Datenschutzbeauftragte hat diese App geprüft. Ihr Jahresbericht für 2018 stellt fest: »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.«

Noch bleibt es allen selbst überlassen, ob sie ihre Krankendaten zentral speichern lassen wollen; man muss keine der angebotenen Akten nutzen. Zu bedenken und gesellschaftlich zu diskutieren ist aber auch, wohin die Entwicklungen des Gesundheitssystems gehen. 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 hier jedoch zu einer schleichenden Aushebelung des Arztgeheimnisses.

Anschlusszwang

Ob sie die Telematikinfrastruktur (TI) im Gesundheitswesen nutzen oder nicht, können ÄrztInnen nicht freiwillig entscheiden – das E-Health-Gesetz setzt eine verbindliche Frist zur Vernetzung. Zwar wurde die gesetzliche Zeitvorgabe aus technischen Gründen wiederholt verschoben, doch nun wird es ernst: Bis zum 30. Juni 2019 müssen alle Praxen hierzulande an die TI mit Netzwerk und Datencloud angeschlossen sein. Können niedergelassene ÄrztInnen gegenüber der Kassenärztlichen Vereinigung nicht nachweisen, dass sie die für den Anschluss notwendigen Geräte bis zum 31. März bestellt hatten, droht ihnen ab Juli ein 1-prozentiger Honorarabzug – so lange, bis sie sich an die TI anschließen.
Die Digitalisierung und ihre Risiken beleuchtet seit vielen Jahren der Internist Wilfried Deiß, Hausarzt im westfälischen Siegen. Auf seiner Homepage *www.praxiswilfrieddeiss.de* stehen viele kritische, gut verständliche Texte. Unter der Überschrift »Mein Ärztliches Gewissen und die Arztgeheimnis-Cloud« diskutiert Deiß aktuell die heikle Frage: »eHealth-Gesetz befolgen oder verweigern?« Lesenswert ist auch sein 5-seitiges Plädoyer an die Macher, über die Zentrale TI doch bitte »in einfacher Sprache« zu informieren. Selbst ÄrztInnen hätten ja »zum Teil nicht verstanden, worum es geht«, schreibt Deiß, und bei den PatientInnen sei der Informationsstand noch schlechter. Dass die elektronische Gesundheitskarte »der Schlüssel zum bundesweiten Netzwerk ist, in dem Arztberichte dauerhaft gespeichert werden sollen, wissen nur die Wenigsten«.