Prof. Dr. Michaela Geierhos
Professorin für Data Science und
Technische Direktorin am Forschungsinstitut CODE
der Universität der Bundeswehr München

Michaela Geierhos

/// Erwägungen über den passenden Umgang mit Patientendaten in Deutschland

German Angst und Datensicherheit

Der bloße Gedanke daran, dass die eigenen Gesundheitsdaten auf einmal zentral und vollständig digital(-isiert) verfügbar sein könnten, schürt Ängste und wirft Umsetzungsfragen auf. Ein Paradigmenwechsel in der IT-Sicherheit, der nach dem Zero-Trust-Prinzip arbeitet, könnte trotz Nullvertrauen das Vertrauen in die Datensicherheit wiederherstellen.

Sorglosigkeit ade?

Müssen wir uns jetzt vom Rundum-Sorglos-Paket verabschieden? Diese Frage stellt sich nicht mehr. Denn seit Einführung der Datenschutzgrundverordnung (DSGVO) muss sich jeder Einzelne damit auseinandersetzen, welche personenbezogenen Daten bei wem und in welcher Form gespeichert und zu welchem Zweck verarbeitet werden dürfen. Aufgrund der dezentralen Datenhaltung im Gesundheitswesen (zum Beispiel bei den Haus- oder Fachärzten) waren wir durch die DSGVO gezwungen, schriftliche Einverständniserklärungen zu geben, damit unsere vorhandenen Patientendaten weiter genutzt werden dürfen. Es mag sein, dass die juristische Absicherung der Datenhaltung und -verarbeitung bei den Beteiligten nicht gerade als Bürokratieabbau wahrgenommen wurde und Patienten vermeintlich keine andere Wahl hatten, als die Erklärungen zu unterschreiben – doch wer die mehrseitigen Belehrungen gelesen hatte, war vollumfänglich informiert. Ob jeder von uns jetzt noch weiß, was er im Detail unterschrieben und wem er sein Einverständnis erteilt hat, sei mal dahingestellt.

Eine schriftliche Einverständniserklärung zur Datennutzung ist hierzulande Pflicht.

Der Zugriff von behandelnden Ärzten auf die Patientenakte fördert den Behandlungserfolg.

Fakt ist aber, dass wir immer eine Wahl haben. Häufig ist es die individuelle Abwägung zwischen Kosten und Nutzen oder einfach nur Bequemlichkeit, dass wir unreflektiert eine Zustimmung zur Erhebung und Analyse bis hin zur Weitergabe unserer Daten geben. Wenn es aber um unsere Gesundheit geht, steht es außer Frage, dass wir einen persönlichen Nutzen sehen, wenn Ärzte im Zuge der Behandlung Zugriff auf unsere Patientenakte bekommen. In anderen Bereichen geben wir unser Einverständnis oft leichtfertiger: Egal ob es die Cookies von Webseiten oder Social-Media-Plattformen sind, meist werden die Bedingungen – ohne das Kleingedruckte zu lesen – akzeptiert, um die Services vollumfänglich weiternutzen zu können. Inwieweit unterscheidet sich nun die Erlaubnis zur Analyse und Weitergabe unseres Surf- und Kommunikationsverhaltens, die wir häufig ohne Zögern Fremden erteilen, zur künftig möglichen Auswertung unserer Gesundheitsdaten, wenn beides anonym passiert?

Privatheit ade?

Wer hindert Ratsuchende heute daran, ihre Krankheitssymptome nicht nur Medizinern, sondern auch Dr. Google zu schildern? Niemand! Wie verlässlich die Ratschläge tatsächlich sind, muss jeder selbst bewerten, wobei einigen Quellen ein höherer Vertrauensbonus als anderen entgegengebracht wird. Leider kursieren auch zahlreiche Falschinformationen im Netz, sodass eine gute Medien- und Gesundheitskompetenz unerlässlich ist, um nicht völlig verunsichert auf dem Weg zur Selbstdiagnose zu werden. Dass Dr. Google nicht den Arztbesuch ersetzt und nur die Informationen bereitstellen kann, welche Dritte – ohne weitere Qualitätskontrolle – ins Internet gestellt haben, sollte nicht überraschend sein.

Vermutlich hat so mancher Suchmaschinenanbieter oder Social-Media-Betreiber weit mehr Daten über uns gesammelt, als es im Gesundheitswesen jemals der Fall sein wird. Auch sorgt die Zweckbindung der Datennutzung laut DSGVO in Deutschland dafür, dass wir immer nur für einen klar definierten Rahmen unsere Zustimmung erteilen. Beispielsweise muss in einer Praxisgemeinschaft allen Ärzten der Zugriff auf die Patientendaten erteilt werden, damit die Krankengeschichte nicht nur für einen Arzt zur Behandlung einsehbar ist. Auch Studienteilnehmer müssen erneut zweckgebundene Datennutzungsfreigaben erteilen. Dieses sogenannte Opt-in-Verfahren (Zustimmungsregelung) schafft maximale Transparenz und Selbstbestimmtheit für die Patienten, ist aber mit einem hohen Verwaltungsaufwand verbunden. Das ist vermutlich mit ein Grund, warum wir es in Deutschland während der COVID-19-Pandemie nicht geschafft haben, ein zentrales

Impfregister aufzubauen, welches es in unserem Nachbarland Österreich schon seit 10 Jahren gibt. Dort müssen folgende Daten vom Impfenden für den Impfling hinterlegt werden: Angaben zum Impfstoff (unter anderem Handelsname, Hersteller, Chargennummer, Verfallsdatum), Angaben zur verabreichten Impfung (unter anderem Datum der Verabreichung, Dosis), Angaben zum Impfling (unter anderem Name, Geburtsdatum, Geschlecht, Wohnadresse, Sozialversicherungsnummer, impfrelevante Vorerkrankungen und besondere Impfindikationen) sowie Angaben zum Impfenden (Name, Rolle, Berufsadresse und Datum der Speicherung). In Deutschland dürfen laut DSGVO personenbezogene Daten, wie die Angaben zum Impfling, nur mit dessen Einwilligung weitergegeben werden.

Zustimmungsregelung ade?

Opt-out-Regelung versus Opt-in

Wieso wird dann nicht eine Widerspruchsregelung (Opt-out) eingeführt? Das würde bedeuten, dass sämtliche Zustimmungen zur Nutzung der eigenen Gesundheitsdaten standardmäßig für die vorgesehenen Zwecke erteilt sind und jeder selbst entscheiden muss, wofür die initiale Datenfreigabe eventuell wieder zurückgezogen wird. Es ist davon auszugehen, dass später keine weitere Auseinandersetzung mit den erteilten Datenfreigaben mehr stattfindet, auch wenn es jeder weiterhin selbst in der Hand hat. Die Gründe hierfür sind zahlreich und wurden vor ein paar Jahren im Zuge der Debatte um die Organspende in Deutschland kontrovers diskutiert. Es ist bekannt, dass in Ländern, in denen eine Zustimmung zur Organspende als Standard angenommen wird (Opt-out), deutlich mehr Organspender erfasst sind als in Ländern (wie zum Beispiel Deutschland), in denen der Organspende ausdrücklich zugestimmt werden muss (Opt-in). Ob diese Tatsache durch mangelnden aktiven Widerspruch bedingt ist, soll hier nicht weiter thematisiert werden. In diesem Kontext stellt sich vor allem die Frage nach der Umsetzbarkeit beider Varianten, die in Deutschland noch ernsthaft diskutiert wird, während es beispielweise kein Opt-out aus dem zentralen Impfregister in Österreich gibt, was dort als Eingriff in die Grundrechte noch kritisch diskutiert wird.

Mit Einführung der elektronischen Patientenakte (ePA) in Deutschland kann ein Patient selbst medizinisch relevante Daten lebenslang zentral und einrichtungsübergreifend speichern und den behandelnden Ärzten zur Verfügung stellen. Hierbei wäre die Implementierung von Opt-in beziehungsweise Opt-out in der ePA analog zur Erstkonfiguration eines Smartphones vorstellbar: Gewisse Standardeinstellungen sind gesetzt und können individuell verändert werden. Bei Opt-in wären die Freigaben minimalistisch

gesetzt und jeder Patient würde diese bei Bedarf erweitern, während bei Opt-out zunächst alles zulässig wäre, bis aktiv widersprochen würde. Technisch handelt es sich immer um ein Rechtemanagement: Entweder gewähre ich Personen oder Institutionen Zugriff auf meine Gesundheitsdaten oder entziehe ihnen diesen. In der Konsequenz bedeutet Letzteres, dass zum Beispiel beim Arztwechsel der Vorgänger zwar keinen Zugriff mehr auf die künftigen Gesundheitsdaten hat, aber der Status Quo – zumindest partiell – aufgrund von gesetzlichen Fristen, beispielshalber zur Abrechnung mit den Krankenkassen, für eine gewisse Mindestdauer weiterhin lokal vorgehalten werden muss.

Dezentrale Datenhaltung ade?

Die meisten Daten werden irgendwo über kurz oder lang gespeichert. Die Frage ist nur: Wo? Dabei steht einerseits der Schutz sensibler (Gesundheits-)Daten im Fokus, aber andererseits haben auch die Benutzerfreundlichkeit und Leistung der Anwendung (zum Beispiel ePA) immensen Einfluss auf die Speicherstrategie. Grundsätzlich stehen zwei Optionen zur Wahl: zentrale und dezentrale Datenhaltung. Aber was ist damit gemeint? Welche Auswirkungen hat die Datenspeicherung in der Anwendung? Und inwiefern betrifft es den Nutzer im Alltag?

In der dezentralen Datenspeicherung werden Daten lokal abgelegt.

Von dezentraler Datenspeicherung ist die Rede, wenn Daten nicht mehr zentral im Rechenzentrum, sondern lokal abgespeichert werden. Ein sehr bekanntes Beispiel dafür ist die Corona-Warn-App der Bundesregierung. Sie speichert Daten über Begegnungen mit anderen Geräten ausschließlich auf dem eigenen Gerät und nicht zentral. Erst wenn ein Nutzer sich als infiziert meldet, wird die zentrale Serverinstanz im Hintergrund aktiv. Die Entwickler der Corona-Warn-App entschieden sich für diesen dezentralen Ansatz, da Gesundheitsdaten dann nicht zentral angreifbar sind und leichter vor unbefugtem Zugriff geschützt werden können. Denn bei großen Datenmengen besteht immer die Gefahr des Datenmissbrauchs.

Bei der zentralen Datenhaltung werden die meisten Daten zentral auf einem Server und kaum noch auf den jeweiligen Endgeräten gespeichert. Beispiele hierfür sind Cloud-Dienste, die Fotos, Videos und weiteres auf ihren Servern vorhalten. Somit liegt der Vorteil bei der zentralen Datenspeicherung im Komfort für die Nutzer, dass sie jederzeit von überall mit ihren Zugangsdaten auf ihre Dateien zugreifen können. Sollte beispielsweise das Smartphone verloren gehen, sind die Daten (in der Cloud) weiterhin verfügbar. Hätten die Entwickler der Corona-Warn-App diese so implementiert, hätte

eine Datenbank zentral ermitteln können, mit wem die infizierte Person in Kontakt gestanden hat und direkt eine Nachricht an alle Betroffenen schicken können. Das wäre die einfachere und unaufwendigere Lösung aus Entwicklerperspektive gewesen, aber nicht in puncto Datenschutz.

Datensicherheit ade?

Ganz und gar nicht! Durch Kryptographie – die Verschlüsselung von Informationen – kann Unbefugten der Zugriff auf unsere (Gesundheits-)Daten verwehrt werden. Diese Verschlüsselungsverfahren können sowohl zentral als auch dezentral eingesetzt werden. Denn die persönlichen Daten können nur mit einem Schlüssel, den der Patient selbst besitzt, gelesen werden. In diesem Fall ist eine zentrale Datenspeicherung möglich, ohne dass der Betreiber (zum Beispiel Cloud-Anbieter) oder Dritte (Ärzte, Krankversicherungen etc.) die Daten lesen können. Ein Restrisiko bleibt jedoch – wenn der sogenannte kryptographische Schlüssel verloren geht, sind die Daten nicht mehr lesbar und somit nutzlos.

Unsere Gesundheitsdaten werden zur Sicherheit verschlüsselt.

In puncto Datensicherheit setzt sich die dezentrale Datenspeicherung klar durch, weil die Informationen hier nicht zentral auf dem Server, sondern auf dem jeweiligen Endgerät gespeichert werden. Das bedeutet, dass sie besser vor dem unberechtigten Zugriff durch Dritte geschützt sind. Der Nutzer behält die Kontrolle über das Gerät und damit über seine Daten. Im Prinzip entspricht das dem Grundsatz der ePA, die mit ihrem Paradigmenwechsel den Patienten zum Manager seiner eigenen Gesundheitsdaten macht. Allerdings bedeutet der Verlust des mobilen Endgeräts, auf dem die Gesundheitsdaten dezentral gespeichert wären, auch kompletten Datenverlust, selbst wenn diese darauf verschlüsselt und zweckentfremdete Datenverwendungen damit ausgeschlossen sind. Das Einzige, was zur Datensicherung beiträgt, ist ein Backup, das wiederum zentral in der Cloud gespeichert wird. Ob allerdings jeder Patient egal welcher Altersgruppe ausreichende Medienkompetenz hat und regelmäßig automatische Backups macht, die aber zur Schonung des Datenvolumens im Mobilfunknetz meist ausgesetzt werden und dann manuell im WLAN nachgeholt werden sollten, ist fraglich.

Vertrauensvorschuss ade?

Identitätsdiebstahl und anderer Datenmissbrauch müssen verhindert werden.

Wenn Gesundheitsdaten künftig zentral gespeichert werden sollten, erhöht sich auch das Missbrauchspotenzial. Darum müssen Identitätsdiebstähle oder andere Risiken minimiert und abgesichert werden. So besteht unter anderem die Gefahr der Deanonymisierung, die durch (un-)gewollte Datenverknüpfungen zwischen der ePA mit pseudonymisierten Daten aus anderen Registern, wie zum Beispiel dem Deutschen Register Klinischer Studien (DRKS), technisch möglich wäre. Deshalb sind Maßnahmen zu ergreifen, damit ein Schadensfall gar nicht eintritt oder belastendende Situationen vermieden werden. In diesem Zusammenhang ist das Vorsorgeprinzip ein gängiger Begriff und manifestiert sich in altbewährten Sprichwörtern wie „Vorsicht ist besser als Nachsicht", kann aber auch zum Credo für die Datensicherheit werden.

Vertraue niemals, überprüfe immer! Das ist das Motto des Zero-Trust-Sicherheitsansatzes. Das Zero-Trust-Prinzip (Nullvertrauen) verfolgt die Strategie, jeden einzelnen Datenfluss auf Vertrauenswürdigkeit zu überprüfen. Doch was verbirgt sich dahinter? Stellen wir uns für einen Moment vor, dass wir im Krankenhaus von einem Arzt angesprochen werden. Diese Person trägt einen weißen Kittel und wir können daher relativ schnell feststellen, ob er „echt" sein könnte. Wir wissen zu diesem Zeitpunkt nicht hundertprozentig, ob es sich bei dieser Person wirklich um einen Arzt handelt, aber wir schenken ihm vorerst ein gewisses Maß an Vertrauen. Doch was passiert, wenn dieser vermeintliche Arzt in Zivil vor uns steht? Wahrscheinlich würden wir ohne weitere Überprüfung sehr kritisch sein und hätten zunächst wenig Vertrauen in diese Person. Wie groß wäre unser Vertrauen, wenn dieser vermeintliche Arzt nicht persönlich mit uns sprechen würde, sondern beispielshalber am Telefon? Richtig, das Vertrauen wäre gleich Null, da eine schnelle Überprüfung ebenfalls unmöglich ist.

Nach dem Zero-Trust-Ansatz müssten wir alle drei Ärzte aus unserem vorherigen Beispiel zuerst einmal verifizieren, bevor wir ihnen Auskunft geben. Ähnlich verhält es sich für die ePA und nicht nur für Ärzte, sondern für alle, welche Zugriff auf unsere Daten (ePA) haben möchten. Selbst wenn Zero-Trust gerade wieder im Trend ist, so wurde das Konzept bereits 1994 in der Informationstechnologie definiert. Es basiert auf der Idee, dass Unternehmen weder ihren Kunden noch ihren Mitarbeitern noch irgendwelchen Anwendungen vertrauen sollten – unabhängig davon, ob sie sich innerhalb oder außerhalb der Infrastruktur des Unternehmens befinden. Stattdessen muss der Datenzugriff jederzeit überprüft, kontrolliert, konsequent überwacht und analysiert werden. Im Zuge der zentralen (Gesundheits-)Datenspeicherung scheint es sich um eine praktikable Methode zu handeln, die

in Kombination mit Verschlüsselungsverfahren den Zugriff auf die Daten sichert und sie nur für diejenigen – durch Schlüsselaustausch – lesbar macht, denen es der Patient selbst erlaubt.

Nutzerakzeptanz ade?

Datenspeicherung kann zentral oder dezentral erfolgen.

Generell steht vor Entwicklung jeder Anwendung die Frage, welches Datenspeicherkonzept umgesetzt werden soll. Entwickler werden vermutlich für die zentrale Datenhaltung votieren. Sie können so leichter die Benutzerfreundlichkeit verbessern und machen sich nicht von bestimmten Endgeräten abhängig. Jedoch kann bei sehr sensiblen Informationen wie zum Beispiel Gesundheitsdaten eine dezentrale Datenspeicherung für Patienten von Vorteil sein. Häufig macht es den Nutzern auch nichts aus, wenn die Daten zentral gespeichert werden. Wichtig ist in diesem Fall aber, dass transparent gemacht wird, was mit den Daten geschieht und wie sie vor unberechtigtem Zugriff geschützt werden. Oft sind es auch Kostengründe, die eine dezentrale Datenhaltung forcieren: WhatsApp ist dafür das prominenteste Beispiel. Mit dem raschen Anstieg der Nutzerzahlen wuchs auch die Menge der Nachrichten, Fotos und Videos. Hätte der Messenger-Dienst auf die zentrale Variante gesetzt und alle Daten auf eigenen Servern gespeichert, wäre das mit einer Kostenexplosion einhergegangen. Allerdings erweist sich der dezentrale Ansatz schlecht für die Skalierbarkeit. Das gilt gleichermaßen für die Corona-Warn-App. Denn mit jeder Neuinfektion werden immer mehr Daten über den zentralen Server hin und her geschickt, damit jede einzelne App auf dem jeweiligen Smartphone ihre Kontakte analysieren kann. Bei einem rasanten Infektionsanstieg kann der Server überlastet werden, da viele Apps auf einmal sehr viele Abgleiche durchführen. Eine zentrale Datenspeicherung würde mit den großen Datenmengen besser zurechtkommen. Zwar hängt die Entscheidung, ob eine zentrale oder dezentrale Datenspeicherung umgesetzt wird, vom Aufwand, Betrieb und von der Benutzerfreundlichkeit ab. Letztendlich kommt es aber auf die Akzeptanz der Patienten an. Darum wäre eine Corona-Warn-App mit zentraler Datenspeicherung in Deutschland aufgrund fehlender Akzeptanz nicht realisierbar gewesen. Es kostete uns mehr Zeit, bis sie schließlich eingeführt werden konnte. Das ist jedoch der Preis, den wir für mehr Datenschutz bezahlen müssen.

Vertrauen ist gut, Kontrolle ist besser

Die ePA ist auf dem Vormarsch – seit Januar 2021 bieten die gesetzlichen Krankenkassen ihren Versicherten eine elektronische Patientenakte an. Jetzt heißt es aufzuklären und Vertrauen zu schaffen! Zwar werden darin die Gesundheitsdaten zentral und verschlüsselt bereitgestellt, aber sie soll auch – idealerweise lückenlos – die Krankengeschichte einer Person dokumentieren. Nachdem Deutschland weniger Einwohner als WhatsApp-Nutzer hat, wird wohl ausreichend Speicherplatz für alle relevanten Gesundheitsdokumente (inklusive Röntgenbilder etc.) in den kommenden Jahren zur Verfügung stehen (müssen), damit sich der zentrale Ansatz auch wirtschaftlich amortisiert: Einsparungen bei (unnötigen) Behandlungskosten bei steigenden Datenhaltungs- und Datensicherungskosten.

Übergangsweise werden Patientenakten parallel analog und elektronisch angelegt.

Anfangs ist jedoch weiterhin von einer parallelen Datenhaltung – zumindest im Übergangsbetrieb – auszugehen. Vermutlich werden die Behandlungsdaten sowohl in der ePA als auch weiterhin in Praxisverwaltungssystemen vorgehalten. Generell werden diese Doppelgleisigkeiten bei der Datenspeicherung nicht auszuschließen sein. Selbst die fortschreitende Digitalisierung wird nicht per Knopfdruck dafür sorgen, dass auf einmal analoge Patientenakten verschwinden, wenn gesetzliche Aufbewahrungspflichten noch greifen sollten und eine retrospektive Digitalisierung (unter anderem der Arztbriefe) sich gegebenenfalls nicht mehr lohnt. Darüber hinaus ist Vollständigkeit ein idealtypischer Zustand, der wahrscheinlich nur zu einem gewissen Grad erreicht werden kann. Einerseits muss Interoperabilität mit existierenden Systemen gewährleistet werden, sonst enthält die ePA nur neue und keine alten Gesundheitsdaten und andererseits werden zum Beispiel Behandlungsdaten von Auslandsaufenthalten nur bedingt Einzug in die deutsche ePA halten können. Um das Nacherfassen – egal aus welchem Grund – werden sich Patienten selbst kümmern müssen – analog zum Versicherungsverlauf bei der Deutschen Rentenversicherung, welcher von Zeit zu Zeit der Kontenklärung bedarf.

Patienten werden künftig zu Datenmanagern: Sie können ihren behandelnden Ärzten die entsprechenden Berechtigungen für den Einblick in ihre ePA erteilen. Hierbei sollten sie beispielsweise differenzieren, ob sie ihnen nur Zugriff auf den Ist-Zustand oder auch auf ihre komplette Krankengeschichte gewähren. Des Weiteren bestimmen Patienten selbst, wer welche Daten wie lange einsehen darf und per App können sie ihre Gesundheitsdokumente selbst organisieren. Fraglich ist, welche Generation dabei abgehängt wird oder ob es weniger eine Generationenfrage, sondern eher eine Frage der Medien- und Datenkompetenz ist, die nicht jeder zwangsläufig mitbringt oder noch nicht dafür geschult wurde.

Grundsätzlich sehen die europäischen Datenschutzrichtlinien vor, dass Datensätze gelöscht werden müssen, wenn sie zur Erreichung des ursprünglichen Zwecks der Datenerhebung nicht mehr erforderlich sind. Aber wer kontrolliert dieses Recht auf Vergessen in der Praxis? So mancher fragt sich auch, welche Gründe es wohl geben mag, dass Gesundheitsdaten wieder aus der ePA gelöscht werden sollten. Nichtsdestotrotz liegt auch das Löschen von Dokumenten in der Hand der Patienten. Was das dann für die Vollständigkeit der Krankengeschichte und somit für die ePA bedeutet, bedarf keiner weiteren Erläuterung.

Laut den europäischen Datenschutzrichtlinien müssen nicht mehr benötigte Daten gelöscht werden.

Fakt ist aber, dass Bedenken und Vorsicht mit zentraler Gesundheitsdatenhaltung und Sicherheitsfragen immer angebracht sind, auch wenn uns im angloamerikanischen Raum eine typisch deutsche Zögerlichkeit nachgesagt wird. Doch „German Angst" drückt vor allem aus, dass wir gelernt haben, dass es im Leben nichts umsonst gibt – es ist immer eine Abwägung zwischen Kosten und Nutzen, Komfort und Selbstbestimmung sowie Datenschatz und Datenschutz.

///