

Wenn alle erfahren, was einem fehlt

Gesundheitsminister Karl Lauterbach will die elektronische Patientenakte einführen. Verpflichtend. Das ist gut für die Forschung – aber wie sind die Daten zu schützen? VON EVA WOLFANGEL

Mehrere Monate lang klagte Martina Radu* über starke Unterleibsschmerzen. Im Sommer 2022 schließlich überwies ihr Arzt sie zur Computertomografie an eine radiologische Praxis. Alles verlief gut, Radu bekam mehr Klarheit über die Ursachen ihrer Beschwerden. Was allerdings danach mit den medizinischen Bildern der Patientin geschah, beschäftigt bis heute die Gerichte. Obwohl Radu expliziten Widerspruch eingelegt hatte, wurden diese an den Dienstleister Telepaxx weitergeleitet, der damals damit warb, Daten an Start-ups weiterzugeben, um »innovative Gesundheitsprodukte« zu entwickeln.

»Medizinische Bilder sind biometrische Daten«, sagt die 47-Jährige. Sie ist überzeugt, dass diese selbst in anonymisierter Form ihrer Person zugeordnet werden können. »Und dann erfährt mein Arbeitgeber und was weiß ich wer davon.«

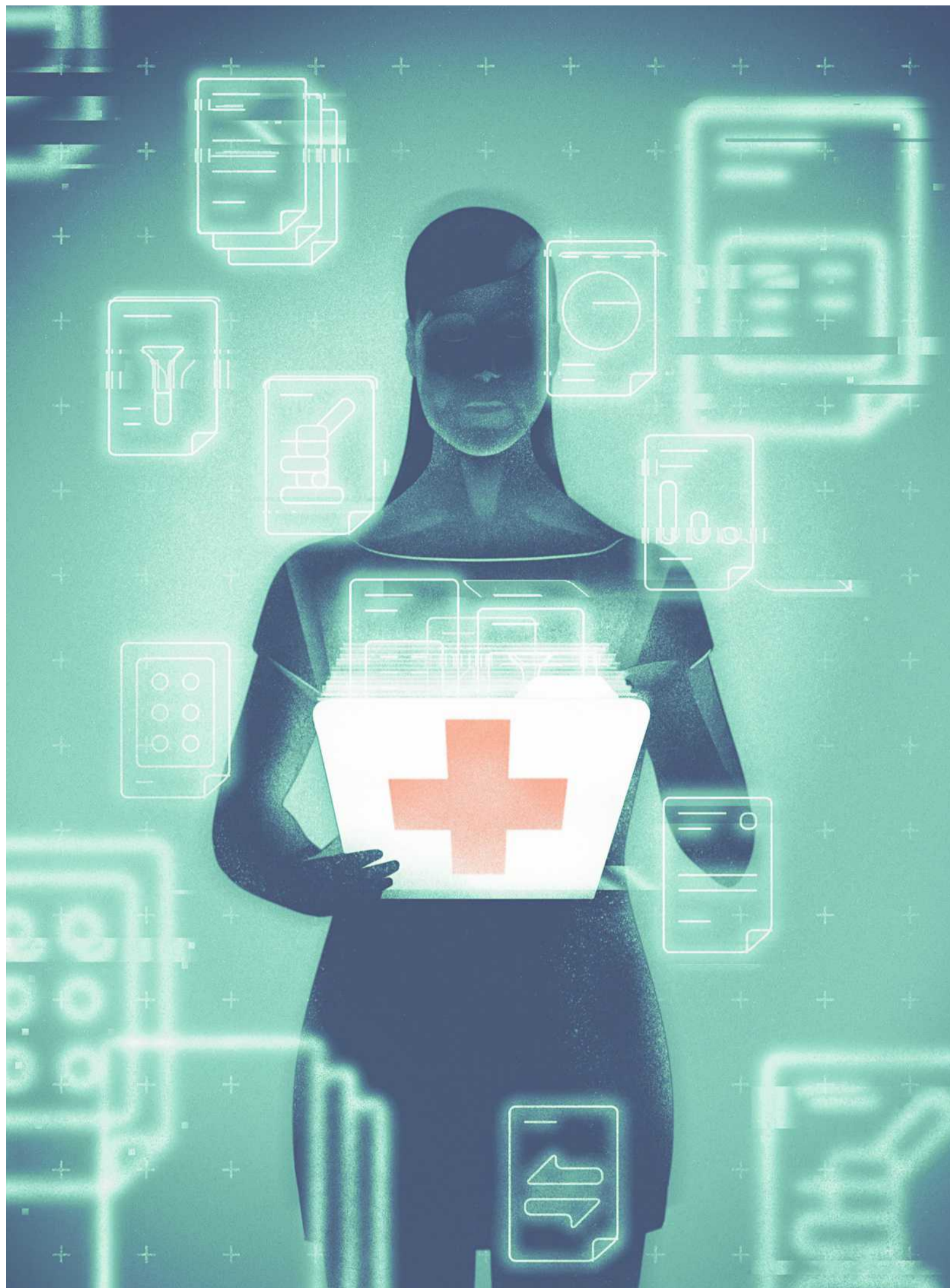
In der Tat gelten medizinische Bilder und andere Gesundheitsinformationen als sensible Daten, die aus gutem Grund besonders geschützt sind. Die Kehrseite: Wissenschaftler in Deutschland beklagen, dass genau diese Daten für die medizinische Forschung fehlten.

Das soll sich jetzt ändern: Ende 2024 soll die elektronische Patientenakte in Deutschland für jeden Patienten verpflichtend werden. Behandelnde Ärzte sollen in dieser Akte dann Diagnosen und andere Untersuchungsergebnisse vermerken. Ausgedient hätten damit Zettelwirtschaft und große Aktschränke in den Praxen. Wie Gesundheitsminister Karl Lauterbach außerdem verkündete, sollen Patientendaten in Zukunft auch der Forschung zur Verfügung gestellt werden. Wer sie nutzen will, stellt einen Antrag an das Forschungsdatenzentrum des Bundes. Denn dorthin sollen sämtliche Informationen aus den Praxen übertragen und anonymisiert gespeichert werden.

Die Patientenakte ist nicht ganz neu in Deutschland, seit Jahren diskutieren Experten und Politiker über das Projekt. Auf freiwilliger Basis gibt es sie bereits heute. Allerdings wird sie nur von rund einem Prozent der gesetzlich Versicherten genutzt. Das führe zu unnötigen und teuren Doppeluntersuchungen, findet Lauterbach. So mancher Patient würde zudem nicht optimal behandelt, weil die Ärztinnen und Ärzte keine Einsicht in frühere Diagnosen haben. Künftig soll dies möglich sein. Wer das nicht will, kann die Akte nach dem Opt-Out-Prinzip ablehnen. Dieser »Druck« sei nötig, so Lauterbach, um dem »Defätismus in den Arztpraxen« zu begegnen.

Dabei seien Bedenken wie die von Patientin Radu gegen das allzu freizügige Teilen von Gesundheitsdaten durchaus gerechtfertigt. Das jedenfalls findet Carmela Troncoso, die an der Ecole Polytechnique in Lausanne das Security and Privacy Engineering Laboratory leitet. Natürlich könne es praktisch sein für Patienten, wenn Diagnosen mit anderen behandelnden Ärzten geteilt werden. »Das Problem fängt an, wenn wir diese Daten mit anderen Zwecken verbinden.« Denn wenn sie nun mit der Forschung geteilt werden, haben immer mehr Menschen darauf Zugriff. Das vergrößert die potenziellen Einfallstore für Hacker. Der Patient selbst gerät hier in die Zwickmühle. Hält er die digitale Patientenakte für sinnvoll, werden seine Daten automatisch auch an die Forschung weitergegeben. Wer das nicht will, kann die Akte nicht nutzen.

Noch ist nicht geklärt, inwiefern Versicherte bei der elektronischen Patientenakte den Zugriff auf bestimmte Informationen (zum Beispiel über psychotherapeutische Behandlungen) selbst steuern können.



Wenn Daten geteilt werden, öffnet das potenzielle Einfallstore für Hacker

und Patienten aus ganz Europa verpflichtend zusammengeführt und für die Forschung bereitgestellt werden. Dorthin werden dann auch die Daten aus Deutschlands elektronischen Patientenakten weitergeleitet. Sollte der Gesetzentwurf in Brüssel so beschlossen werden, wie er derzeit diskutiert wird, wird es für Patienten kaum möglich sein, die Kontrolle über ihre Daten zu behalten – geschweige denn zu erfahren, wer diese wofür nutzt.

Der Grund: Der europäische Entwurf enthält keine der klassischen Mechanismen, die die europäische Datenschutz-Grundverordnung DSGVO für die meisten anderen persönlichen Daten vorsieht, wie etwa Information und Einwilligung. Betroffene können laut dem Entwurf nicht einmal widersprechen, dass ihre Daten an Institute, Unternehmen, Start-ups oder Einzelpersonen weitergegeben werden, die damit forschen wollen.

Das sei rechtlich problematisch, sagt Stefan Brink vom Wissenschaftlichen Institut für die Digitalisierung der Arbeitswelt: »Die Betroffenenrechte vom Tisch zu wischen lässt sich mit der Datenschutz-Grundverordnung nicht vereinbaren.« Zumindest ein Widerspruchsrecht und Möglichkeiten, Informationen löschen zu lassen, müssten gewährleistet sein. Eine sinnvolle Forschung sei schließlich auch dann möglich, wenn Einzelne die Weitergabe ihrer Daten ablehnten.

Fest steht: Mit der digitalen Patientenakte und den Plänen für den europäischen Datenraum

stellen sich zwei bisher ungelöste Aufgaben. Die Gesundheitsdaten vor kriminellen Hackern zu schützen – und sie zuverlässig zu anonymisieren.

All die sensiblen Daten seien ein »riesiger Hacking-Honeypot«, sagt Jan Penfrat vom Verband European Digital Rights. Was er meint: Der künftige Datenraum lockt kriminelle Hacker an wie ein Honigtopf einen Bären. Einfach, weil es sich lohnt.

Eine Möglichkeit wäre, die Daten dezentral zu speichern, beispielsweise auf den Geräten der Patienten, und sie erst zusammenzuführen, wenn eine konkrete Forschungsfrage bearbeitet werden soll. Dann böten sie viel weniger Angriffsfläche für Hacker und Spione.

Zentral gespeicherte Gesundheitsdaten können kaum gut genug geschützt werden – das zeigen zahlreiche Fälle der jüngsten Vergangenheit. So werden seit 2020 die Patienten eines finnischen Psychotherapiezentrum von einem Hacker erpresst, der deren gesamten Leidensgeschichten ins Internet stellte – unter den Betroffenen sind zahlreiche Prominente. In Australien wurden die Daten von fast zehn Millionen Kunden der größten privaten Krankenversicherung durch eine russische Gruppe gehackt, die Lösegeld erpresen wollte. In Pennsylvania wurde in den vergangenen Wochen eine ganze Klinikgruppe angegriffen. Seitdem stehen Nacktbilder von Brustkrebspatientinnen im Netz.

Carmela Troncoso beschäftigt sich seit vielen Jahren mit der Frage, wie Daten so ausgewertet

werden können, dass sie sicher und privat bleiben. Die Anonymisierung von Gesundheitsdaten sei extrem kompliziert: »Menschen sind gewissermaßen einzigartig«, sagt Troncoso, »die Kombination unserer Attribute macht uns identifizierbar.« Dazu müsse man nicht einmal eine seltene Krankheit haben, eine Handvoll Merkmale wie Alter, Postleitzahl und eine Erkrankung, »die nicht die Grippe ist«, genüßten häufig, um anonymisierte Daten realen Menschen zuzuordnen.

Um eine De-Anonymisierung zu verhindern, müssten einzelne Informationen aus einem Datensatz herausgenommen oder verallgemeinert werden – nur welche? Schließlich könnten gerade dadurch jene Zusammenhänge verloren gehen, welche die medizinische Forschung braucht. Für Wissenschaftler ist es gerade interessant, welche Krankheiten miteinander korrelieren, welche genetische Disposition mit welchen Beschwerden zusammenhängt, in welchen Umständen die Patienten leben, wie alt sie sind, welches Geschlecht sie haben. Und so werden die pseudonymisierten Datensätze, die von der Forschungsstelle herausgegeben werden, zahlreiche Merkmale enthalten – und lediglich der Name der Betroffenen wird durch eine Nummer ersetzt.

Troncoso prognostiziert, dass es ein Leichtes sein wird, die realen Namen herauszufinden. Und wer diese kennt, der kennt am Ende die komplette Krankengeschichte.

Spätestens seit Mitte der 1990er-Jahre gibt es einen Wettlauf zwischen jenen, die versuchen, Gesundheitsdaten zu anonymisieren, und jenen, die zeigen, wie aussichtslos dieses Unterfangen ist. So veröffentlichte der Bundesstaat Massachusetts damals die anonymisierten Daten über die Krankenhausaufenthalte aller Staatsbediensteten, dazu Postleitzahl, Geschlecht und Alter. Die Informatikerin Latanya Sweeney, heute Direktorin des Harvard Data Privacy Lab, nutzte Postleitzahlen und andere verfügbare Informationen – und konnte den Gouverneur des Bundesstaates William Weld identifizieren. Woraufhin sie ihm seine vollständige Krankengeschichte zukommen ließ.

Einige Jahre später identifizierte Sweeney anonyme Teilnehmer einer großen DNA-Studie, und kürzlich glichen Forschende der Harvard University anonyme Krankenakten von Krankenhäusern mit Presseberichten ab. Sie konnten ein Drittel der in Artikeln erwähnten Unfallopfer eindeutig einer Patientenakte zuordnen. So wurde beispielsweise eine junge Frau aus Maine identifiziert, die bei einem Unfall Knochenbrüche und Kopfverletzungen erlitt. Sie ließ sich eindeutig ihrer pseudonymisierten Krankenakte zuordnen, in der Geschlecht, Alter und die Region, in der sie lebte, verzeichnet waren. Der Akte war auch zu entnehmen, dass die 19-Jährige an Depressionen und einer Angststörung leidet.

Sobald es möglich sei, mehrere Datensätze zu kombinieren, seien Informationen nicht mehr anonym, sagt Troncoso. Das Problem: Es gibt heute jede Menge Datensätze, die öffentlich verfügbar sind und die dabei helfen, pseudonymisierte Informationen Personen zuzuordnen.

Zurück zu Martina Radu: Ihre Sorge, dass medizinische Bilder zugleich biometrische Daten und damit einem Fingerabdruck ähnlich seien, ist nicht abwegig. Die Technologie der Gesichtserkennung hat in der Vergangenheit bereits gezeigt, dass es durch die zugrunde liegenden Modelle künstlicher Intelligenz (KI) kaum mehr möglich ist, unerkannt zu bleiben. Im Herbst vergangenen Jahres gelang es Forschenden der Universität Erlangen-Nürnberg, mithilfe von KI anonymisierte Röntgenbilder der Lunge den realen Patienten zuzuordnen.

Wenn nun in Zukunft Krankheitsgeschichte und Diagnosen noch einfacher mit Forschungsinstitutionen geteilt werden sollen, besteht die Gefahr, dass private Unternehmen versuchen, die Grenzen immer mehr zu verschieben. Telepaxx zum Beispiel, jenes Unternehmen, das die Daten von Martina Radu erhalten hat, wirbt damit, »Gesundheitsinformationen von jedem zweiten Deutschen gespeichert zu haben« Radu hat inzwischen Strafanzeige gegen Telepaxx gestellt, unter anderem wegen der Erschleichung von Daten. Dabei ist das Unternehmen nur ein Beispiel von vielen Dienstleistern, die mit dem Speichern und Teilen von Gesundheitsdaten ein Geschäft machen.

Ein Grund dafür liegt ausgerechnet in der Datenschutz-Grundverordnung. Denn mit ihrem Inkrafttreten wurde der Schutz von Gesundheitsdaten im Vergleich zum bisherigen deutschen Recht gelockert – ebenfalls mit dem Ziel, diese einfacher der Forschung zur Verfügung zu stellen. Stefan Brink, der bis Ende 2022 Datenschutzbeauftragter von Baden-Württemberg war, hat damals eine regelrechte Bewegung beobachtet. Es hätten sich prompt jede Menge Dienstleister gebildet, die anboten, Forschern Datenpools zu erschließen. Denn eine Einwilligung sei ja nun nicht mehr nötig. Damit warb auch Telepaxx: Patientendaten ohne Zustimmung der Betroffenen für KI-Projekte zu benutzen sei »in vollem Umfang datenschutzkonform«, hieß es kürzlich noch auf der Website der Firma. Von der DSGVO sei das nicht gedeckt, sagt Brink: »Die Einwilligung ist nur dann nicht nötig, wenn der behandelnde Arzt oder die Klinik selbst die Forschenden sind.«

Mit dem Europäischen Datenraum wird sich das ändern: Dann genügt es, wissenschaftliche Gründe anzuführen, um die Daten nutzen zu können. Auch Unternehmen oder Einzelpersonen könnten das tun. Die Datenschutzbehörden werden damit künftig noch mehr in der Verantwortung stehen, zu prüfen, ob all jene, die vorgeben zu forschen, die nötigen Kriterien erfüllen. Wie aber soll das angesichts überlasteter Behörden funktionieren? »Wir brauchen aufmerksame Patienten und Patientinnen«, sagt Brink.

Martina Radu findet diese Rolle alles andere als angenehm. Sie fühlt sich nicht ernst genommen. Viele tun ihre Sorge, dass ihr Chef von ihrer Erkrankung erfahren könnte, als paranoid ab. Dabei könnte es für künftige Arbeitgeber durchaus interessant sein, über psychische Erkrankungen oder andere Beschwerden von Bewerbern Bescheid zu wissen – schließlich verursachen diese Fehlzeiten und Kosten. Wie sehr solche Daten gefragt sind, zeigte eine Forscherin der amerikanischen Duke University, als sie im Februar zahlreiche Datenhändler im Internet identifizierte, die Namen und Adressen von US-Bürgern feilboten. Zum Sonderangebot gehörten auch deren Diagnosen zu psychischen Krankheiten.

*Name von der Redaktion geändert

LESEN SIE IN UNSERER AKTUELLEN AUSGABE:

Wie sicher sind unsere Banken?

AB FREITAG IM HANDEL

Wirtschafts Woche

Was sie mit Sicherheit nicht beeinflussen werden, ist, dass die Daten später in einen sogenannten Europäischen Gesundheitsdatenraum weitergegeben werden. Hier sollen Informationen über Patientinnen