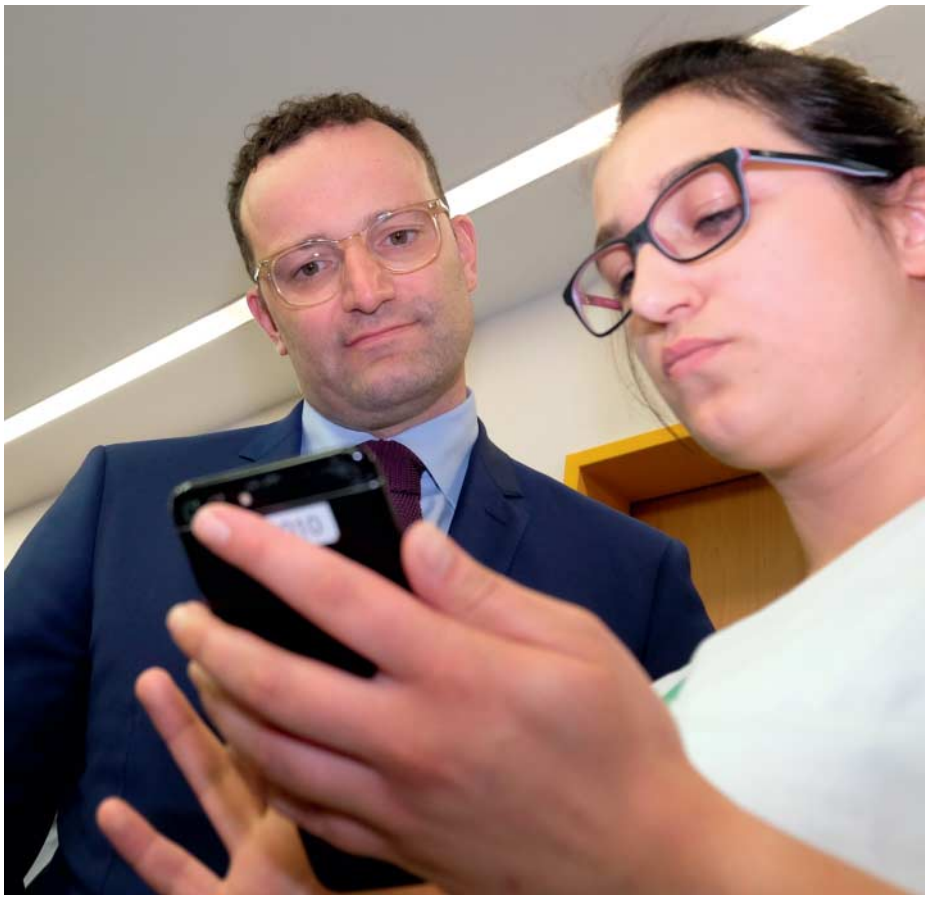

Bild: Sebastian Willnow/dpa

Risiken und Nebenwirkungen

Warum Sie bei Medizin-Apps unbedingt das Kleingedruckte lesen sollten

Nach dem Entwurf des digitalen Versorgungsgesetzes (DVG) sollen Krankenkassen künftig die Kosten für digitale Medizin-Apps erstatten. Eine aufwendige CE-Zertifizierung soll Qualität garantieren. Doch gerade beim so wichtigen Datenschutz klaffen gesetzlich noch immer Lücken.

Von Hartmut Gieselmann

Gesundheitsminister Spahn drückt aufs Tempo. Er will die Digitalisierung des Gesundheitssystems vorantreiben und setzt Herstellern, Krankenkassen und Ärzten ambitionierte Termine für die Umsetzung. Doch selbst Experten halten diese für wenig realistisch – es sei denn, man mache bei einigen aufwendig umzusetzenden Vorgaben Abstriche. Dazu gehören etwa der Nachweis der klinischen Wirksamkeit oder auch der Datenschutz.

Das Bundeskabinett hat nun den Entwurf des „Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation“ (Digitale-Versorgung-Gesetz, DVG) beschlossen. Bevor es im Januar 2020 in Kraft treten kann, muss es noch den Bundestag passieren.

Einer der Kernpunkte sind Änderungen und Ergänzungen im fünften Sozialgesetzbuch. Nach den neuen Paragrafen 33a und 139e sollen Krankenkassen künftig die Kosten für Gesundheits-Apps erstatten, die Patienten von Ärzten verschrieben wurden. Solche Apps müssen zuvor vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zertifiziert und in ein neues Verzeichnis für digitale Gesundheitsanwendungen aufgenommen werden.

Als Grundlage für diese CE-Zertifizierung (die sich der Hersteller im Unterschied zu Haushaltsprodukten nicht einfach selbst ausstellen kann) gilt die EU-Medizinprodukteverordnung (MDR). Sie trat bereits am 25. Mai 2017 in Kraft. Allerdings gilt bis zum 26. Mai 2020 noch eine Übergangsregelung nach der älteren und nicht so rigiden Medizinprodukterichtlinie (MDD). Hersteller von Medizin-Apps stören sich vor allem an der neuen Regel 11 der MDR. Sie besagt, dass jede Software, die für diagnostische oder therapeutische Zwecke herangezogen wird, mindestens in die Risikoklasse IIa eingestuft werden soll. Bislang genügte für solche Apps oftmals die Klasse I, die deutlich geringere Anforderungen stellt und beispielsweise kein Qualitätsmanagement vorschreibt.

Zu den CE-zertifizierten Medizinprodukten gehören etwa auch die populären Apps ADA und Moodpath, die in der Kategorie Medizin der Online-Stores von Apple und Google auf den Top-Plätzen rangieren. ADA ist ein KI-gesteuerter Chat-Bot, der Fragen zu Beschwerden und Symptomen stellt. Die App macht Vorschläge für wahrscheinliche Diagnosen, die der Patient anschließend mit seinem Arzt genauer besprechen soll. Moodpath ist ein Stimmungstagebuch für Patienten, die unter Depressionen leiden. Die App scannt Texteingaben und schlägt Alarm, wenn sich Anzeichen für eine depressive Phase häufen.

Austausch mit den USA

Die Hersteller der Apps arbeiten mit namhaften deutschen Universitäten zusammen, was in medizinischer Hinsicht für Seriosität spricht. Ein Blick ins Kleingedruckte der Datenschutzbestimmungen beider Apps wirft jedoch Fragen auf, ob der Patient über die sensiblen Gesundheitsdaten, die diese Apps über ihn sammeln, tatsächlich die volle Kontrolle behält.

Immerhin listen beide Anbieter kleinteilig auf, mit welchen Firmen sie bei der Datenverarbeitung zusammenarbeiten – das tun längst nicht alle Hersteller. Beide betonen, konform zur DSGVO zu sein. Allerdings schließt das nicht aus, dass die Daten auch an Dritte außerhalb der EU übermittelt und gespeichert werden.

So arbeitet Aurora, der Hersteller von Moodpath, etwa mit US-Firmen wie Google, Crashlytics, Tenjin und Branch Metrics zusammen. Verwunderlich ist beispielsweise, dass an Tenjin Daten mit Werbe-Tracking-IDs übermittelt werden, obwohl Moodpath in der App gar keine Werbung schaltet und sich die Dienstleistung per Abo bezahlen lässt. Zusätzlich erhält der Betreiber des App-Stores, Apple oder Google, davon Kenntnis, dass die App heruntergeladen und installiert wurde. Zwar betont Aurora, dass die Datenübertragung in die USA auf Grundlage des Privacy-Shield-Abkommens rechtens sei. Doch egal, ob US-Firmen die an sie übermittelten Daten in der EU oder in den USA speichern: Sie müssen seit Inkrafttreten des Cloud Acts im März 2018 alle Daten an US-Behörden auf Verlangen aushändigen – ohne dass der Betroffene etwas davon erfährt. Das gilt auch für ADA Health, die betonen, dass ihre Daten nur innerhalb der EU gespeichert würden. Wenn die betreffenden Server-Zentren jedoch US-Firmen gehören, sind sie nach dem Cloud Act zur Herausgabe der Daten auf Nachfrage an US-Behörden verpflichtet.

Zudem gelten in den USA andere Vorgaben zur Vorratsdatenspeicherung. So kann ein Nutzer zwar die Löschung seiner Daten hier in Deutschland verlangen, bei Drittanbietern, mit denen Aurora die Daten ausgetauscht hat, bleiben sie unter Umständen aber weiterhin gespeichert. Auf Nachfrage will Aurora auch nur dann bei den Drittanbietern um Auskunft oder Löschung bitten, solange dies nicht mit einem „unverhältnismäßigen Aufwand“ verbunden sei.

ADA Health, Hersteller der gleichnamigen kostenlosen App, nimmt sich wiederum das Recht heraus, „Einzelheiten der Besuche“ wie Besuchslänge und Seiteninteraktionen sowie recherchierte Konditionen und Symptome zu speichern und an Analysedienste zu übertragen. Genannt werden hier unter anderem Amazon, Facebook, Amplitude, Adjust und Sentry. So erfährt Facebook beispielsweise jedes Mal davon, wenn die App gestartet wird. Auf Anfrage von c’t erklärte ADA, dass lediglich anonymisierte Daten „zur fortlaufenden Verbesserung des Produkts“ genutzt würden. Eine Studie des US-Magazins Nature kam allerdings zu dem Ergebnis, dass bereits 15 Merkmale aus anonymisierten Datensätzen genügen, um einen US-Amerikaner mit einer Sicherheit von 99,98 Prozent zu identifizieren. Eine bloße Anonymisierung reiche laut der Forscher daher nicht aus, um die Identität von Patienten zu schützen.

Als Grund für die Datenweitergabe an Dritte wird von ADA Health in den Datenschutzbestimmungen lapidar ein „berechtigtes Interesse“ angegeben. Bei der Frage, warum die Gesundheits-App durch das eingebaute Facebook-SDK Daten an den Zuckerberg-Konzern übermittle, wird schlicht auf eine „Vertragserfüllung“ verwiesen.

Verkauf von Daten

Zudem nimmt sich ADA Health das Recht heraus, personenbezogene Daten nicht nur mit der eigenen in den USA ansässigen Holding und deren Tochtergesellschaften zu teilen, sondern auch durch Mitarbeiter außerhalb des europäischen Wirtschaftsraums verarbeiten zu lassen. Nicht zuletzt könnten die personenbezogenen Daten einem „potenziellen“ Käufer oder Verkäufer als „Vermögenswert“ offengelegt werden. Das Bayerische Landesamt für Datenschutzaufsicht hatte bei einem „Asset-Deal“ in ähnlichen Fällen allerdings bereits sechsstellige Bußgelder gegen andere Firmen verhängt, die personenbezogene Kundendaten veräußert und damit gegen das Datenschutzrecht verstoßen hatten.

Als expliziten Grund für eine Herausgabe personenbezogener Daten nennt ADA etwa die „Betrugsverhinderungen“ bei sich und „anderen Organisationen“. Zu solchen „anderen Organisationen“ gehören laut ADA „staatliche Behörden“ und „eine Vielzahl von Unternehmen“, die vom Gesetzgeber festgelegt worden seien. Nicht ausgeschlossen, dass dazu eventuell auch Krankenversicherungen zählen, die bei einem Schadensfall die Kosten drücken wollen. Wenn ein Bewerber etwa bei Vertragsabschluss bestimmte Vorerkrankungen außen vor lässt, sich später aber herausstellt, dass er sich selbige in ADA hat diagnostizieren lassen, könnte eine Versicherung dies womöglich zum Anlass nehmen, die Kosten nicht zu übernehmen oder den Vertrag zu kündigen.

Bezeichnend für derartige Klauseln ist, dass ADA Health als „offiziellen Wortlaut“ der Datenschutzrichtlinie die englische Version angibt. Sie wurde offenbar vom US-amerikanischen Mutterkonzern vorgegeben. Allerdings ist ADA Health eine in Deutschland ansässige GmbH und es ist fraglich, ob eine solche Klausel nach hiesigem Recht wirksam ist.

Moodpath soll depressiven Menschen helfen. Der eingebaute Werbe-Tracker von Google tut dies aber sicherlich nicht.

CE-Zeichen schützt keine Daten

Wie gesagt, ADA und Aurora gelten nicht als schwarze Schafe, sondern als Vorzeigeanbieter der Branche, die mit Universitäten kooperieren und mit Forschungsgeldern gefördert werden. ADA arbeitet zudem nach eigenen Angaben eng mit der Techniker Krankenkasse zusammen. Mit ihren CE-Zeichen und ISO-Zertifizierungen suggerieren sie dem Anwender, bei ihnen würde kein Schindluder mit seinen Daten getrieben. Doch sowohl die MDR als auch das neue DVG gehen auf die Anforderungen für den Datenschutz nur am Rande ein: Er solle schlicht dem „Stand der Technik“ entsprechen, heißt es etwa im DVG-Entwurf. Die DSGVO müssen Firmen in der EU ja eh einhalten, egal ob sie nun Medizinprodukte verkaufen oder Butterkekse.

So stellte denn auch der Geschäftsführer des Instituts für Qualität und Regulation digitaler Medizin (QuR), Philip Kopf, im Gespräch mit c’t klar, dass eine

Zertifizierung durch das BfArM, bei der sein Institut die Hersteller berät, im Wesentlichen um medizinische Aspekte wie einen Nachweis der klinischen Wirksamkeit geht. Auch diese muss übrigens bei der Einführung einer App nicht vorab nachgewiesen werden, sondern erst innerhalb des ersten Jahres nach der Erteilung des CE-Zertifikats und der Kostenübernahme der Krankenkassen.

Aspekte des Datenschutzes würden jedoch von anderen Richtlinien wie etwa der DSGVO abgedeckt. Sie seien deshalb zwar für die Zertifizierung durch das BfArM relevant, würden aber unabhängig von der CE-Zertifizierung betrachtet. Das erklärt auch, warum ein CE-Zeichen kein Garant für besonders hohe Anforderungen an den Datenschutz ist. Bei Firmen, die dieses Logo verwenden, können sich trotzdem die zuvor genannten Klauseln in den Datenschutzbestimmungen verstecken.

Kopf kritisierte zudem den zu knappen Zeitrahmen für die Umsetzung der Vorgaben der MDR. So gebe es bislang in Europa nur zwei Prüfstellen, die die CE-Zertifizierungen überhaupt vornehmen könnten. Bis Mai nächsten Jahres sei mit einem großen Stau bei den Anträgen von Herstellern zu rechnen, die das begehrte CE-Zeichen für ihre Apps erhalten wollen, um in den lukrativen Pool der von Krankenkassen bezahlten Gesundheits-Apps zu kommen. Realistischer wäre laut Kopf eine Verlängerung der Übergangsfrist der MDR bis 2024. Das BfArM wollte sich auf Nachfrage von c't nicht zum DVG-Entwurf äußern. *(hag@ct.de)* c't

Kommentar: Unabsehbare Folgeschäden

Von Hartmut Gieselmann

Die in Medizin-Apps gespeicherten Daten sind nicht nur besonders brisant, sondern können auch Personen betreffen, die die Apps gar nicht nutzen und deren Datenschutzbestimmungen gar nicht abgenickt haben. Besonders tückisch sind etwa Erbkrankheiten. Wenn diese bei einzelnen Patienten diagnostiziert werden, dann betreffen die Informationen auch andere Familienmitglieder bis hin zu noch ungeborenen Enkeln und Urenkeln.

In diesem Zusammenhang verlieh Digitalcourage e.V. just der US-Firma AncestryDNA den Big Brother Award 2019. AncestryDNA bietet im Web Gen-Analysen zur sogenannten Ahnenforschung an – zum Schnäppchenpreis von 89 Euro. Doch laut Digitalcourage verkauft Anchestry die DNA-Daten weiter an Forschungsinstitute und Pharmaunternehmen, die für die Nutzung solcher Gendatenbanken hunderte Millionen Dollar springen lassen. US-Behörden nutzen DNA-Datenbanken inzwischen auch bei der Strafverfolgung. Begehrlichkeiten gibt es zudem bei Versicherungen, mit DNA-Analysen ihre Risikoabschätzung zu „optimieren“. Das Nachsehen haben dann Patienten, die aufgrund einer genetischen Besonderheit ein höheres Risiko für bestimmte Krankheiten bedingen, daraufhin teurere Tarife bezahlen müssen oder gar keinen Vertrag mehr bekommen.

Aber selbst wenn keine Profildaten aus den Apps an Firmen wie Google oder Facebook weitergereicht werden, ist oft allein schon die Information kritisch, welche Gesundheits-App von wem wie häufig genutzt wird. Das gilt nicht nur für Moodpath: Wenn Google oder Apple in ihren Shops registrieren, wer die App heruntergeladen hat und regelmäßig nutzt, dann können sie daraus schließen, dass die betreffende Person vermutlich unter Depressionen leidet. Derartige Therapie-Apps für psychologische Probleme und Suchterkrankungen gibt es viele: Es gibt digitale Hilfen für entwöhnte Alkoholiker (SmartAssistEnz), für Raucher (CureApp) oder Geschlechtskrankheiten (Intimarzt).

Hier wäre ein besonderer Schutz nötig. Bislang verstehen Rechtsprechung und Zertifizierungstexte unter Datenschutz hauptsächlich den Schutz vor unbefugtem Zugriff. Die *befugte* Weitergabe und den Verkauf der Daten durch die Firmen wird – DSGVO hin oder her – vor dem Patienten aber weitestgehend verschleiert.

Deshalb muss nicht nur die Technik für die digitale Datenverarbeitung im Gesundheitswesen fit werden, sondern auch die Rechtssprechung: App-Store-Betreiber müssten per Gesetz gezwungen werden, dass Aufzeichnungen über medizinische Käufe nach kurzer Zeit gelöscht und Daten zur Nutzung gar nicht erst erhoben werden. Anbietern von Gesundheits-Apps müsste zudem untersagt werden, Tracker-Dienste einzusetzen und Daten mit Drittfirmen zu teilen. Denn es gibt aus Sicht der Patienten keinen Grund, warum eine Depressions-App etwa Googles Werbe-ID braucht oder sich eine Diagnose-App mit dem Facebook-Konto verbinden muss. Der Patient muss sicher sein, dass seine Daten nicht weitergegeben werden und alle Beteiligten sie auf seinen Wunsch hin löschen. Bisherige Anonymisierungsverfahren genügen hier nicht, sondern die Datensätze müssten zusätzlich in Gruppen zusammengefasst werden.

Wenn selbst Experten einen Aufschub der MDR bis 2024 fordern, wäre für eine Nachbesserung noch Zeit genug. Es gibt keinen guten Grund dafür, dass Gesundheitsminister Spahn hier im Eilverfahren Gesetze durchpeitscht. Er sollte sich lieber die nötige Zeit nehmen, um den Datenschutz für medizinische Apps auf Vordermann zu bringen. Dies würde zur Akzeptanz in der Bevölkerung und bei Ärzten beitragen und berechtigte Vorbehalte zerstreuen.

Bis es so weit ist, sollten Patienten die Datenschutzbestimmungen der Gesundheits-Apps gründlich studieren und ihre Gesundheitsdaten im Zweifel nur dem anvertrauen, der gesetzlich zum Schweigen verpflichtet ist: Ihrem Arzt. *(hag@ct.de)*