Diabetes-Clouds und Datenschutz

Datenmanagement *Erste Stellungnahme von Datenschutzbehörden zu Diabetes-Clouds: Für Praxen/Kliniken besteht nun Handlungsbedarf!*

Datenschutzexperten warnen schon länger, dass beim Einsatz von Diabetes-Clouds häufig elementare gesetzliche Pflichten grob missachtet werden. Spätestens nachdem auch die Deutsche-Diabetes-Gesellschaft DDG Anfang des Jahres offiziell über die Problematik informierte, war Handlungsbedarf für Praxen bzw. Kliniken angezeigt.

> *„Die Datenschutzbehörden der Länder haben eine gemeinsame Stellungnahme herausgegeben."*

Dies bedeutet im Klartext: wer solche Cloud-Lösungen ohne sorgfältige Prüfung einsetzt, fährt derzeit– bildlich gesprochen – im Blindflug durch ein juristisches Minenfeld. Vielen Ärzten ist offensichtlich nicht bewusst, dass Datenschutzverstöße keine Bagatellen sind und gerade im Gesundheitsbereich mit teilweise exorbitanten Bußgeldern sanktioniert werden.

Eine Möglichkeit wäre, einfach unverändert weiterzumachen. Das ist aber nicht ratsam: Keine Praxis kann sicher sein, dass sie nicht plötzlich im Fokus der Behörde steht - beispielsweise aufgrund der Anzeige eines unzufriedenen Patienten, eines missgünstigen „Kollegen" oder eines Mitarbeiters, von dem man sich im Streit getrennt hat.

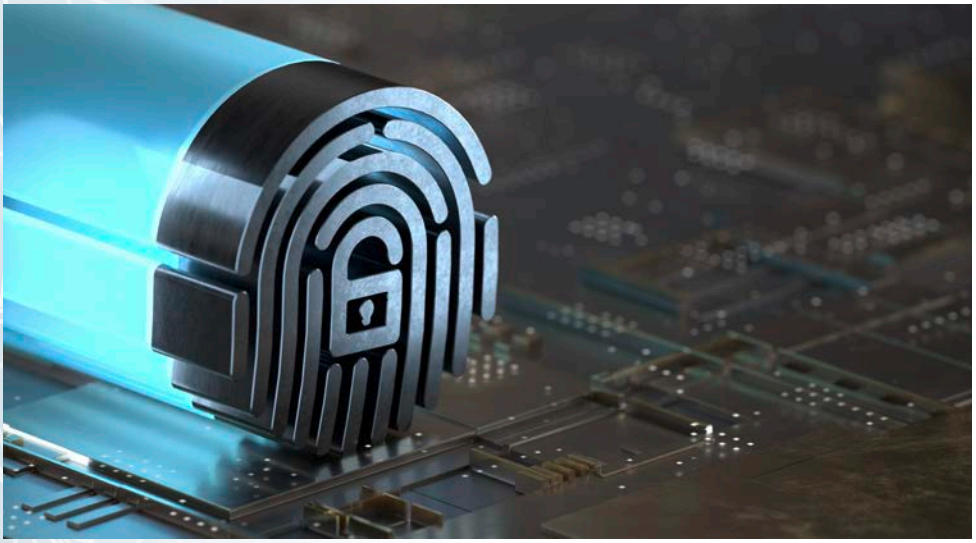
Schon oberflächliche Recherchen bei google zeigen, dass die Behörden bei Datenschutzverstößen zwischenzeitlich konsequent durchgreifen und hohe Strafen festsetzen.

Ein anderer Ansatz bestünde darin, die Rechtslage durch juristische Gutachten klären zu lassen. Das ist aber teuer und hilft nur, wenn die Expertise lege artis erstellt wird und dabei auch keine relevanten Tatsachen unter den Tisch gekehrt werden, die für irgendjemanden vielleicht unbequem sind. Selbst dann bliebe ein Graubereich, denn die Behörden könnten es im Ergebnis auch anders sehen als die befragten Anwälte.

Es gibt aber auch noch eine dritte Möglichkeit, um verlässlich Klarheit zu bekommen: man braucht die Behörden doch einfach nur zu fragen! Und das haben wir nun für unsere Leserinnen und Leser getan. Wir haben an zahlreiche Datenschutzbehörden sowie an DDG und BVND einen ausführlichen Fragenkatalog zu Diabetes-Clouds ge-

Text: RA Oliver Ebert.

© Marje - iStockphoto



© Just_Super - iStockphoto

Das Diabetes-Forum hat nachgehakt und die Datenschutzbehörden um Auskunft gebeten.

schickt; selbstverständlich haben wir dabei auf keinen konkreten Anbieter Bezug genommen.

Darauf hat man uns mitgeteilt, dass bereits bei mehreren Datenschutzbehörden diesbezügliche Anzeigen von Patienten vorliegen. Mutmaßlich hatte man behördlicherseits auch die von der DDG veröffentlichten Bedenken bereits zur Kenntnis genommen. Die Datenschutzbehörden halten die Problematik daher wohl für so wichtig, dass man sich zu einer gemeinsamen und im fachlich zuständigen Arbeitskreis Gesundheit und Soziales der Datenschutzkonferenz abgestimmten Stellungnahme veranlasst sah.

Unsere Anfrage dürfte daher gerade noch rechtzeitig gekommen sein: die ungewöhnlich ausführliche Stellungnahme der Behörden kann als unmissverständliche Warnung an die Ärzteschaft verstanden werden, rechtswidrige Datenverarbeitungen im Zusammenhang mit Diabetes-Clouds sofort einzustellen und die gesetzlichen Pflichten zu beachten.

heinz@kirchheim-verlag.de

Dank der nun vorliegenden Antworten können Datenschutzbeauftragte von Praxis/Klinik jetzt deutlich besser abschätzen, ob eine Diabetes-Cloud eingesetzt werden darf und welche Pflichten, Kosten und Risiken damit einhergehen.

© Grkpro - iStockphoto

Folgende Aussagen und Konsequenzen lassen sich aus der Stellungnahme ableiten:

- Wenn der Anbieter die Patientendaten auch für eigene Zwecke (beispielsweise für „statistische Zwecke, Marktforschungszwecke, Forschungszwecke, Produktoptimierungszwecke oder andere Zwecke“) verarbeiten darf, dann ist die Cloud-Nutzung auf Basis eines Auftragsverarbeitungsvertrags illegal.
- Praxis/Klinik sind datenschutzrechtlich entweder allein oder gemeinsam mit dem Cloud-Anbieter verantwortlich. In letzterem Fall wäre die Nutzung der Cloud-Lösung nur legal, wenn mit dem Anbieter eine Vereinbarung gem. Art 26 DSGVO geschlossen wurde, in dem die wechselseitigen Verantwortlichkeiten geregelt sind.
- Arzt/Klinik müssten sich in einer solchen Vereinbarung transparent dazu bekennen, dass ihre Verantwortlichkeit auch darin besteht, dem Cloud-Anbieter die kommerzielle Nutzung der Patientendaten ermöglichen. Eine solche Kooperation – vor allem mit Anbietern verordnungsfähiger Produkte – dürfte aber sowohl strafrechtlich (§§ 203, 299a ff StGB) als auch berufsrechtlich nicht unproblematisch sein.
- Datenschutzrechtlich Verantwortlicher ist, wer die Mittel und Zwecke der Datenverarbeitung bestimmt. Entgegen anderslautender Behauptungen von Anbietern dürfte daher unbeachtlich sein, ob der Patient seine Daten selbst in die Cloud einstellt. Denn allein der Arzt entscheidet, ob er einen vom Patienten bereitgestellten „passiven“ Cloud-Zugang als Mittel zur Datenverarbeitung im Rahmen der Behandlungstätigkeit nutzen und die damit für die IT-Sicherheit von Praxis/Klinik verbundenen Risiken eingehen möchte.
- Patienten müssen so aufgeklärt werden, um „das Risiko der Verarbeitung personenbezogener Daten antizipieren können.“ Die Informationen müssen „in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache zur Verfügung gestellt werden.“

„Patienten müssen umfassend aufgeklärt werden.“

- Soll den Cloud-Anbietern vereinbarungsgemäß eine Eigennutzung der Patientendaten erlaubt werden, dann bedarf es hierzu einer Rechtsgrundlage. Solche Datenverarbeitungsvorgänge dienen allerdings allein den wirtschaftlichen Zwecken des Anbieters und sind aus medizinischer Sicht weise nicht erforderlich. Diese sind daher nur zulässig, wenn hierzu eine informierte, ausdrückliche und wirksame Einwilligung aller betroffenen Patienten vorliegt.
- Eine wirksame Einwilligung setzt voraus, dass der Patient frei entscheiden kann. Der Patient muss die kommerzielle Nutzung seiner Daten durch Dritte somit auch ablehnen können, ohne dabei Nachteile in Thera-

100 Jahre Insulin

WIR FEIERN DEN LEBENSRETTER

Sei am 25.09. virtuell dabei

DAS JUBILÄUMS-Barcamp

Du bestimmst den Inhalt! Das Barcamp ist ein offenes Treffen, dessen Inhalte und Ablauf von den Teilnehmer:innen im Verlauf selbst gestaltet werden.

JETZT TICKET SICHERN!
www.blood-sugar-lounge.de/barcamp

Triff Dich mit anderen.
Diskutiere Deine Themen.
Denn Du bist das Barcamp.

BLOOD SUGAR LOUNGE

DIABETES 100 Jahre Insulin BARCAMP

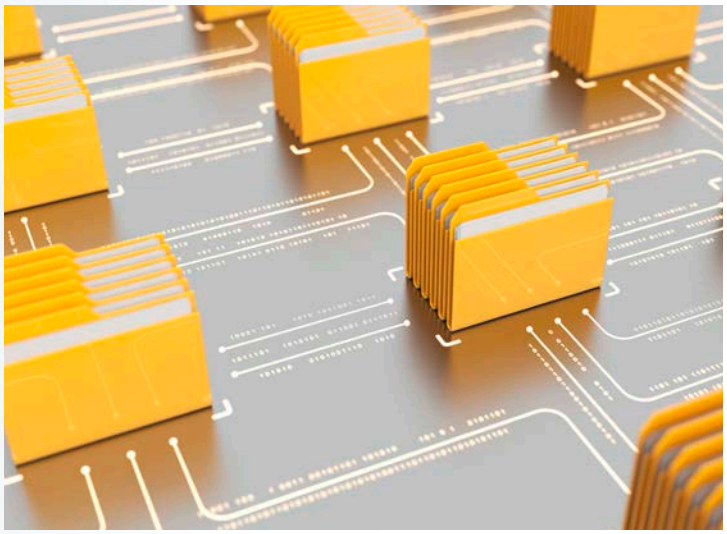
Unterstützt von: novo nordisk®

VIRTUELL | 25.09.2021

28.0021

pie oder Behandlungsqualität zu erfahren.

- Praxen/Kliniken müssen für jede Cloud eine gem. Art. 35 DSGVO gesetzlich vorgeschriebene Datenschutzfolgeabschätzung (DSFA) vornehmen, sofern diese mindestens eine der in der sog. „Muss-Liste" der Datenschutzkonferenz (DSK) gelisteten Konstellationen erfüllt. „Relevant für den Kontext der Verarbeitung von Gesundheitsdaten im medizinischen Behandlungszusammenhang" sei hiernach „insbesondere die Konstellation von Nr. 16". Auch eine Konsultation der Behörde gem. Art. 36 DSGVO könnte notwendig sein.



Heikel: die Übermittlung von Patientendaten an Dritte.

- Ändern sich Nutzungsbedingungen einer Cloud-Lösung, dann muss das Datenschutzrisiko neu bewertet und ggf. eine neue DSFA vorgenommen werden. Vielmals bedarf es auch einer neuen Aufklärung und Einwilligung der Patienten.
- Als „anonym" behauptete Uploads von CGM- und Pumpendaten sind kritisch zu prüfen. Bei Übermittlung der Geräteseriennummer liegt keine Anonymisierung vor. Selbst lediglich Glukosemess- bzw. Verlaufsdaten lassen sich aufgrund ihres individuellen Musters oft wieder einer Person zuordnen.
- Krankenhäusern könnte die Nutzung einer Diabetes-Cloud womöglich auch aus anderem Grund verboten sein: So sehe „etwa § 47 des Landeskrankenhausgesetzes Baden-Württemberg vor, dass Patientendaten in dem Krankenhaus selbst, im Auftrag des Krankenhauses durch ein anderes Krankenhaus oder unter weiteren Bedingungen durch ein Rechenzentrum zu verarbeiten sind."
- Wenn Praxen/Kliniken bei bisheriger Nutzung einer Diabetes-Cloud die gesetzlichen Pflichten nicht erfüllt haben, ist umgehendes Handeln erforderlich: Rechtswidrige Datenverarbeitungen sind sofort einzustellen. Entsprechend Art. 33 DSGVO müssen auch unabsichtlich begangene Verstöße gegen datenschutzrechtliche Pflichten unverzüglich an die Behörde gemeldet werden.

> *„Unbedingt klären, in welchem Umfang eine Übermittlung von Patientendaten an Dritte einhergeht."*

In der kommenden Ausgabe des Diabetes-Forums werden wir die Stellungnahme der Datenschutzbehörde ausführlich vorstellen und

Redaktion: 06131/9607035

– ebenso wie die Antworten, die wir von anderen befragten Stellen erhalten haben – im Volltext veröffentlichen. Vor diesem Hintergrund empfiehlt sich folgende Vorgehensweise:

Ärzte/Kliniken sollten unverzüglich alle eingesetzten Cloud- und Softwarelösungen zum Diabetes-Management dahingehend überprüfen, ob mit deren Nutzung eine Übermittlung von Patientendaten an Dritte einhergeht.

Dazu müssen die mit dem Cloud-Einsatz akzeptierten Nutzungsbedingungen UND etwaige Verträge mit den Anbietern vollständig geprüft werden. Aufgrund der Komplexität der meisten Regelungen können Datenschutzbeauftragte ohne dezidierte juristische Qualifikation hierzu selten hinreichend rechtsicher beraten. Es empfiehlt sich eine Prüfung durch datenschutzrechtlich spezialisierte Kanzleien, auch wenn dies mit nicht unerhebliche Kosten verbunden ist. In eigenem Interesse sollte man keinesfalls auf die Angaben der Anbieter vertrauen. Um eine wirklich objektive Rechtsberatung sicherzustellen, sollte der Anwalt möglichst auch keine Berührungspunkte mit der „Diabetes-Szene" haben.

Nach Prüfung der Nutzungsbedingungen sollten mit dem Anwalt bzw. Datenschutzbeauftragten dann die weiteren organisatorischen Maßnahmen und Konsequenzen abgestimmt werden, insbesondere die etwaige Notwendigkeit einer Selbstmeldung an die Behörde.

Aufgrund der Wichtigkeit des Themas stellen wir die erhaltenen Antworten sowie eine ausführliche Kommentierung schon jetzt online zur Verfügung.

www.bit.ly/3jdYoTM

Autor

Oliver Ebert
Rechtsanwalt und Fachanwalt für IT-Recht
Hochschullehrbeauftragter für e-commerce und Internetrecht
TÜV-zertifizierter Datenschutzbeauftragter
TÜV-zertifizierter Datenschutzauditor
REK Rechtsanwälte
Nägelestraße 6A
70597 Stuttgart
E-Mail: sekretariat@rek.de
www.diabetes-und-recht.de