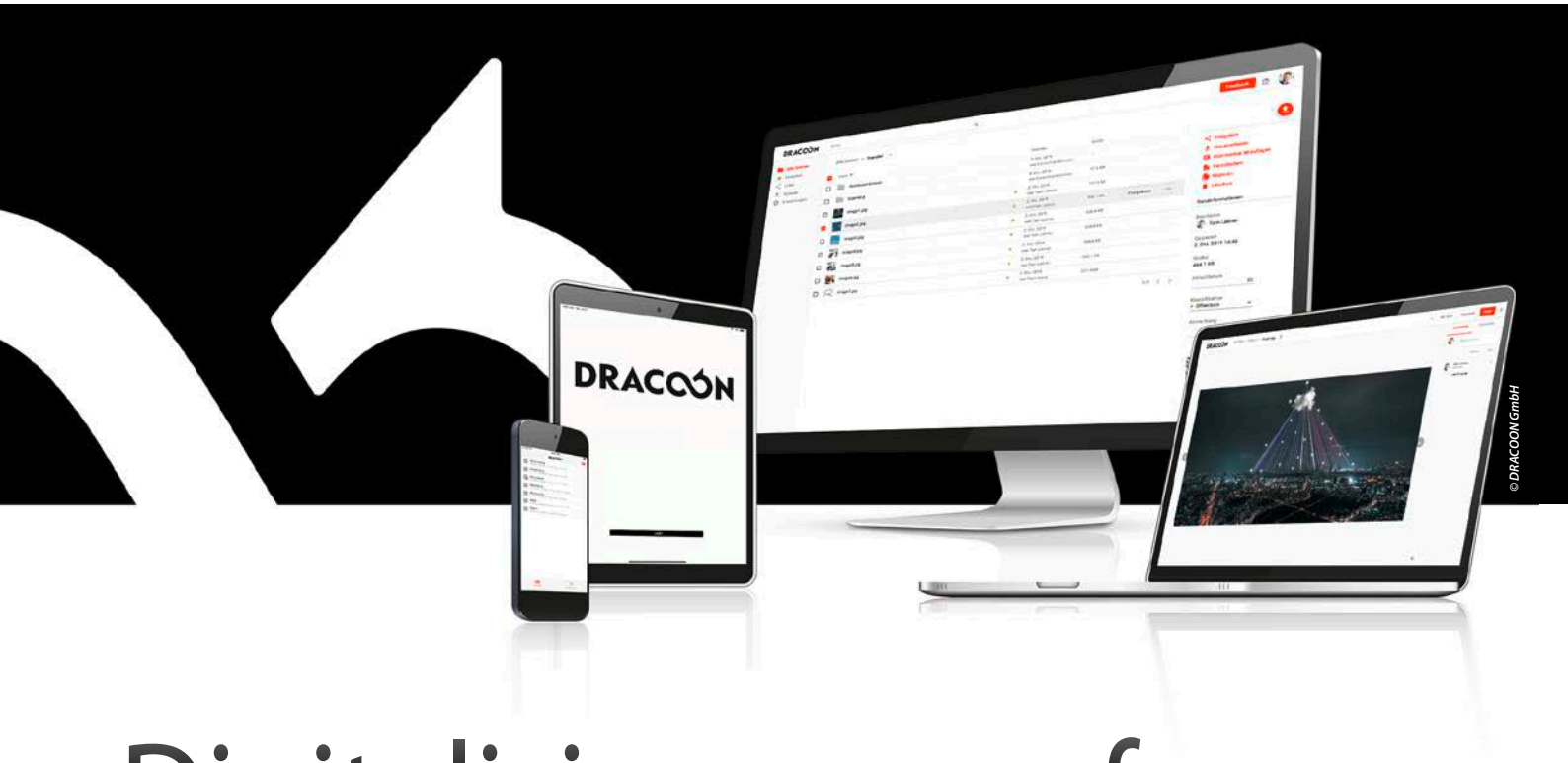

Digitalisierung: auf Nummer **sicher** gehen

Ergänzung *Digitalisierungsansätze in der Diabetes-Therapie: bestmögliche Versorgung und Datenschutz ergänzen einander – so sollte es in der Praxis sein. Wie das zu realisieren ist, erklärt Thomas Haberl beispielhaft anhand der Dienstleistungen der Firma Dracoon.*

Text: Thomas Haberl.

Der Einsatz von Diabetes-Clouds ist für Kliniken und Praxen nicht unbedingt neu und in vielen Einrichtungen längst Standard. Datenschutzexperten sind jedoch ob der Sorglosigkeit der Verantwortlichen im Hinblick auf die Risiken und gesetzlichen Pflichten alarmiert. Denn auch die Deutsche Diabetes Gesellschaft (DDG) wies im Frühjahr 2021 in einem Gutachten auf die Problematik hin. Egal, ob Missachtung oder Unwissenheit, wer die datenschutzrechtlichen Bestimmungen nicht einhält, nimmt nicht nur drastische Sanktionen, sondern auch Datenklau billigend in Kauf.

Die Digitalisierung hat jedenfalls im Bereich der Diabetologie inzwischen eine tragende Rolle eingenommen. So erhalten Patienten beispielsweise schnell und einfach klare Handlungshinweise und dedizierte Informationen, gleichzeitig profitieren die Behandlungsteams von intuitiven und benutzerfreundlichen Oberflächen. Entscheidend ist, dass der Aufwand und eine einfache Handhabung im Verhältnis stehen – Datenschutz inklusive. Denn im Zuge der Digitalisierung werden Daten gesammelt, die es sowohl vor neugierigen Blicken als auch vor Cyberangriffen zu schützen gilt. Die Frage, die sich für die Ärzteschaft stellt, ist jedoch, welche Clouds eingesetzt werden dürfen, welche Risiken und Pflichten damit verbunden sind und welche gesetzlichen Rahmenbedingungen es zu beachten gilt.

So dürfen Diabetes-Clouds beispielsweise nicht auf Basis eines Auftragsverarbeitungsvertrags genutzt werden. Außerdem sind Ärzte und Kliniken verpflichtet, eine Datenschutz-Folgenabschätzung (DSFA) vorzunehmen. Das bedeutet, jede Datenverarbeitung, die aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss einer formalen Prüfung

heinz@kirchheim-verlag.de

unterzogen werden, die alle Datenschutzrisiken beleuchtet und Maßnahmen zur Risikominimierung nachweist. Daher müssen die Nutzungsbedingungen der eingesetzten Diabetes-Clouds eingehend geprüft werden, damit festgestellt werden kann, ob die Datenverarbeitungsvorgänge von der Liste der Behörden umfasst werden.

Mit der zunehmenden Angebotsvielfalt an Cloud-Diensten steigt aber auch die Zahl der Zertifizierungen und Gütesiegel, sodass es für Nutzer immer schwieriger wird, den Überblick zu behalten. Und auch die Anbieter selbst tun sich schwer, die individuellen Anforderungen ihrer Kunden zu verstehen und die erforderlichen Compliance-Bestätigungen zu identifizieren. Der Anforderungskatalog des BSI (Bundesamt für Sicherheit in der Informationstechnik) für mehr Transparenz in der Cloud soll ein Mindestniveau für IT-Sicherheit definieren, das sich Cloud-Anbieter von einem unabhängigen Dritten bestätigen lassen können. Der BSI C5 fußt auf etablierten Prüfschemen, Richtlinien sowie Best Practices. Die Anforderungsbereiche umfassen unter anderem die Organisation der Informationssicherheit, das Identitäts- und Berechtigungsmanagement, Compliance und Datenschutz, Portabilität und Interoperabilität sowie Kryptographie und Schlüsselmanagement. Auf diese Weise können Kunden schnell und einfach feststellen, ob ein Cloud-Dienst den gesetzlichen Vorschriften, insbesondere auch der DSGVO, den eigenen Richtlinien oder auch der Gefährdungslage in Bezug auf Wirtschaftsspionage entspricht und auch die KRITIS-Vorgaben (B3S-Katalog) erfüllt.

Daten EU-DSGVO-konform speichern und teilen

Die Frage ist also, auf welche Aspekte sollten Ärzte und Kliniken achten, wenn es um den Einsatz von Diabetes-Clouds geht?

Ein zentraler Punkt ist der verschlüsselte Datenaustausch, wenn Befunde und andere sensible Daten über die Cloud sicher an die jeweiligen Patienten versandt werden sollen. Maximalen Schutz bietet die Ende-zu-Ende-Verschlüsselung, die auch eine clientseitige Verschlüsselung beinhaltet. Ist dies gewährleistet, kann nicht einmal der Betreiber der Cloud die Daten des Kunden entschlüsseln, da der Schlüssel zu jedem Zeitpunkt beim Besitzer bleibt. Eine weitere Sicherheit bietet die optionale Vergabe von zusätzlichen Passwörtern.

„Ein zentraler Punkt ist der verschlüsselte Datenaustausch.“

Am Beispiel eines Speicheltests könnte das zum Beispiel so aussehen: Bei Abgabe der Probe hinterlässt die Testperson ihre Kontaktdaten, bestehend aus E-Mail-Adresse und Mobilfunknummer. Liegt ein Ergebnis vor, wird der Befund hochgeladen, woraufhin automatisch eine Download-Freigabe inklusive Passwort zum Testergebnis generiert wird. Diese Download-Freigabe erreicht die Testperson via E-Mail, während das Passwort aus Sicherheitsgründen auf einem gesonderten Kommunikationsweg per SMS zugestellt wird. So hat die Testperson über das Passwort die Möglichkeit, ihr Untersuchungsergebnis noch am selben Tag sicher abzurufen, während das ausstellende Institut eine Auslieferungsbestätigung erhält.

Ist es möglich, Zugriffsberechtigungen einfach und individuell an interne Mitarbeiter genauso wie an externe Beteiligte zu vergeben, lässt sich sicherstellen, dass bestimmte Personen beispielsweise nur Leserechte erhalten, während andere Daten auch bearbeiten oder löschen können. In geeigneten Datenräumen, die nur für definierte Nutzergruppen zugänglich sind, könnten weitere Patientendaten in Echtzeit gesichert und weiterverarbeitet werden. Solch eine feingra-

Kontakt

DRACOON GmbH
93053 Regensburg
Telefon:
0941/7 83 85 – 0
Fax:
0941/7 83 85 – 150
info@dracoon.com
www.dracoon.com

Das bietet DRACOON

- ***Maximale Sicherheit dank clientseitiger Verschlüsselung:*** *So wird sichergestellt, dass weder DRACOOON als Anbieter noch Dritte in der Lage sind, auf gespeicherte Daten zuzugreifen*
- ***E-Mail-Verschlüsselung via Outlook Add-In:*** *DRACOON wandelt E-Mail-Anhänge und vollständige E-Mails in sichere Download-Freigaben um*
- ***Made & Hosted in Germany:*** *DRACOON wird in Deutschland entwickelt und in ISO27001-zertifizierten Rechenzentren betrieben*
- ***Mehrfach ausgezeichnet und zertifiziert:*** *Verschiedene Siegel wie ISO27001, IDW PS 951 und BSI C5 bescheinigen DRACOON höchste Sicherheitsstandards*
- ***DSGVO-konform dank Privacy by Default und Privacy by Design:*** *DRACOON hilft Organisationen bei der Einhaltung der DSGVO dank datenschutzfreundlicher Technikgestaltung (Privacy by Design) sowie Voreinstellung (Privacy by Default). So arbeiten Nutzer automatisch datenschutzkonform*
- ***Modernes Berechtigungskonzept:*** *Zugriffsrechte können unkompliziert an interne Mitarbeiter oder externe Beteiligte vergeben werden. So wird sichergestellt, dass bestimmte Personen nur Leserechte haben, andere aber Daten bearbeiten und löschen können. Auch können Daten in ihrer Verfügbarkeit zeitlich befristet werden*

DRACOON

www.dracoon.com

© DRACOON GmbH

Autor

Thomas Haberl

Director Key Account von DRACOON (wir weisen in diesem Zusammenhang auf den Interessenkonflikt hin)

Experte für Digitalisierung im Gesundheitswesen

nulare Rechtevergabe stellt sicher, dass jeder Nutzer nur über die Rechte verfügt, die er wirklich benötigt. Die organisatorische Hoheit liegt dabei in der IT-Abteilung, ohne dass sie Leserechte auf Datenräume wie Patientendaten oder Laborbefundung hat. Außerdem ist auch eine zeitliche Beschränkung von Nutzern oder Nutzerrechten denkbar – unter anderem ist das bei der Einbindung externer Partner, wie Lieferanten oder bei Audits, ein wichtiger Punkt.

Fazit: Mehr Rückenwind durch Digitalisierung – ohne dass der Datenschutz ausbremst

Ineffiziente IT-Strukturen, Insellösungen oder Informationssilos gehören mit der fortschreitenden Digitalisierung und modernen Cloud-Lösungen der Vergangenheit an. Wichtig ist aber, dass Effektivitätssteigerungen nicht durch Datenschutzrisiken konterkariert wer-

Redaktion: 06131/9607035

den. Das sichere Speichern, Verwalten, Versenden und Teilen von Daten sollte durch eine lückenlose clientseitige Verschlüsselung sichergestellt werden. Denn lassen sich die Daten bereits am Endgerät sicher verschlüsseln, besteht auf dem Server selbst keine Möglichkeit, die Daten zu entschlüsseln, da sich das Schlüsselmaterial auf dem Client befindet. So werden sensible Gesundheitsdaten vor ungewollten Zugriffen nachhaltig geschützt. Granulare Rechtesysteme und integrierte Reporting-Tools stellen, genau wie die Möglichkeit der zeitnahen Wiederherstellung geschädigter Daten, eine zusätzliche Sicherheitsschicht dar. Generell lassen sich mit einer guten und zertifizierten Cloudlösung die Anforderungen an eine E-Mail-Verschlüsselung über ein einfaches Outlook Add-In lösen, indem E-Mail-Anhänge in beliebiger Größe und komplette E-Mails automatisch in sogenannte Downloadfreigaben umgewandelt werden, die sich dann DSGVO-konform versenden lassen. Wichtig ist außerdem, eine Softwarelösung „Made & Hosted in Germany“ zu wählen, da deutsche Anbieter den strengen deutschen Datenschutzgesetzen unterliegen und versichern müssen, dass die Lösung auch der EU-DSGVO entspricht. So können Anwender sicher sein, dass ihre Daten in guten Händen sind.