DIABASS®
Eine Software für alle Messgeräte

Einsatz von Diabetes-Datenmanagementlösungen in Arztpraxis und Klinik

Wichtige Hinweise für

Praxisinhaber / Geschäftsführung von Kliniken
(als Verantwortliche gem. Art. 4 Nr. 7 DSGVO)

Datenschutzbeauftragte von Arztpraxis und Klinik
(gem. Art. 37 DSGVO)

IT-Sicherheitsbeauftragte
(gem. BSIG)

Hintergrund

Systeme zum digitalen Diabetes-Datenmanagement sind für eine moderne Diabetes-Therapie unverzichtbar. Verantwortliche von Praxis bzw. Klinik müssen beim Einsatz solcher Lösungen jedoch sicherstellen, dass die gesetzlichen Pflichten (u.a. aus DSGVO und BSI-Gesetz) eingehalten werden, ansonsten drohen erhebliche Bußgelder, womöglich sogar auch eine persönliche Haftung.

Manche der am Markt angebotenen Lösungen verstoßen in eklatanter Weise gegen deutsche und europäische Gesetze; zudem nutzen viele Anbieter die Patientendaten auch für eigene kommerzielle Zwecke.

Der Einsatz solcher Systeme bringt dann erhebliche Risiken mit sich.

Etwaige Bedenken werden meist durch missverständliche oder gar wahrheitswidrige Angaben der Anbieter relativiert, denen Ärzte unkritisch vertrauen. Auch korruptive Zuwendungen sollen die Anschaffungsentscheidung beeinflussen, daher werden datenschutzrechtlich riskante Lösungen oft weit unterhalb der ansonsten marktüblichen Kosten medizinischer IT-Anwendungen oder gar gänzlich kostenfrei offeriert.

Unsere Datenmanagementlösung ***DIABASS®*** genießt seit fast 30 Jahren (!) europaweit das Vertrauen von Ärzten und Patienten - nicht zuletzt auch deswegen, weil wir als Hersteller ehrlich kommunizieren und unseren Kunden keine unnötigen Risiken zumuten.

Mit dieser Broschüre haben wir daher ausführliche Informationen zusammengestellt, die eine umfängliche datenschutzrechtliche Bewertung eines Einsatzes von ***DIABASS®6 PRO*** ermöglichen.

Angaben zur Software

DIABASS®6 PRO (Hersteller: mediaspects GmbH, Friedrichstr. 49, D-72336 Balingen) ist eine lokal installierte und betriebene Software zum Diabetes-Datenmanagement.

Alle mit ***DIABASS®6 PRO*** erfassten Daten werden ausschließlich im lokalen Netzwerk von Praxis/Klinik verarbeitet und gespeichert. Es werden keine Patientendaten an Dritte übermittelt oder Dritten zugänglich gemacht. Auch Telemetriedaten (beispielsweise zur Ausforschung des Verordnungsverhaltens) werden nicht erhoben.

Stellungnahmen der Datenschutzbehörden

Für eine zutreffende datenschutzrechtliche Bewertung von Diabetes-Datenmanagementlösungen sind u.a. die nachstehenden Stellungnahmen von Behörden maßgeblich:

- Gemeinsame Stellungnahme der deutschen Datenschutzbehörden zu Diabetes-Clouds:
  https://www.diabetologie-online.de/a/datenmanagement-diabetes-clouds-und-datenschutz-dringender-handlungsbedarf-2366301
- „Muss"-Liste der Datenverarbeitungen, die nach Auffassung der Datenschutzbehörden zwingend eine Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO erfordern.
  https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/DSFA_muss_Liste_DSK_de.pdf
- Stellungnahme der europäischen Datenschutzbehörden, welche Anforderungen an die Wirksamkeit von Einwilligungen u.a. in Bezug auf Gesundheitsdaten zu stellen sind:
  https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf
- Bußgeldkonzept der deutschen Datenschutzbehörden
  https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf

Fragen & Antworten

Werden mit *DIABASS®6 PRO* personenbezogene bzw. personenbeziehbare Daten übermittelt?

Nein, es werden keine Patientendaten an Dritte übermittelt oder Dritten zugänglich gemacht. Auch Telemetriedaten (beispielsweise zur Ausforschung des Verordnungsverhaltens) werden nicht erhoben.

Nur in folgenden Fällen werden Daten übermittelt:

Updateprüfung:

Wenn die automatische Updateprüfung aktiviert ist, dann sucht ***DIABASS®6 PRO*** per Internet-Abruf nach einer neuen Programmversion und bietet diese dann zur Installation an.

Hierzu werden folgende Daten an mediaspects übermittelt, die möglicherweise personenbeziehbar sind:
IP-Adresse (notwendig für jede Internet-Verbindung), Serien-/Lizenznummer von ***DIABASS®6 PRO***
Zusätzlich werden folgende technische Angaben übermittelt:
Programmversion, Betriebssystem, Sprache sowie ein bei der Installation zufällig erzeugter Hash-Wert

Hinweis: Die Updateprüfung ist optional und kann in den Einstellungen deaktiviert werden.

Einstellungen von *DIABASS® SecureSend*:

Damit Daten per ***DIABASS® SecureSend*** empfangen werden können, müssen administrative Angaben der Praxis/Klinik auf einem zentralen, von mediaspects betriebenen Server gespeichert und für Patienten vorgehalten werden.

Hierzu ist erforderlich, dass folgende administrative Daten an mediaspects übermittelt werden:
IP-Adresse (notwendig für jede Internet-Verbindung), Name und Adresse der Praxis/Klinik, Logo der Praxis/Klinik, email-Adresse der Praxis/Klinik, Statusinformation (Datenempfang erlaubt/nicht erlaubt) sowie ein optionaler Nachrichtentext für alle Patienten (z. B. Hinweis auf Praxisurlaub).

Hinweis: Die Nutzung von ***DIABASS® SecureSend*** ist optional und nicht zwingend erforderlich.

Erforderliche Freigaben:

Für die Updateprüfung bzw. zur Verwaltung der Einstellungen von ***DIABASS® SecureSend*** muss der Internetzugriff (Ports: 80 bzw. 443) auf folgende Adressen zugelassen sein:

http(s)://www.mediaspects.com

http(s)://www.diabass.com

Ist für den Einsatz von *DIABASS®6 PRO* ein Auftragsverarbeitungsvertrag gem. Art. 28 DSGVO mit mediaspects erforderlich?

Nein. mediaspects verarbeitet keine personenbezogenen oder personenbeziehbaren Daten für die Praxis/Klink. Daten werden ausschließlich durch die Praxis/Klink selbst verarbeitet und werden auch nur dort lokal gespeichert. Es werden keine Patientendaten an mediaspects oder sonstige Dritte übermittelt oder zugänglich gemacht.

Info: Das ist der Unterschied zu Cloud-Lösungen

Die Nutzungsbestimmungen nahezu aller Diabetes-Clouds verlangen die Zustimmung von Arzt/Klinik, dass der Anbieter die mit der Cloud verarbeiteten Patientendaten auch für eigene Zwecke verwenden bzw. an Dritte weitergeben darf. Manche dieser Anbieter behaupten dennoch, dass die Cloud auf Basis eines privilegierenden AV-Vertrags gem. Art. 28 DSGVO genutzt werden könne.

Nach eindeutiger Rechtsauffassung der deutschen Datenschutzbehörden kommt eine Auftragsverarbeitung tatsächlich jedoch nicht in Betracht, wenn der Anbieter die Daten auch für eigene Zwecke verarbeitet; dies sei dann *„datenschutzrechtlich unzulässig“*.

Um solche eigenen Zwecke des Dienstleisters handele es sich beispielsweise, *„wenn die Daten etwa für von ihm festgelegte oder mitdefinierte statistische Zwecke, Marktforschungszwecke, Forschungszwecke, Produktoptimierungszwecke oder andere Zwecke verarbeitet werden. [..]“*

Ist für den Einsatz von *DIABASS®6 PRO* eine Vereinbarung gem. Art. 26 DSGVO erforderlich?

Nein. mediaspects verarbeitet keine der personenbezogenen oder personenbeziehbaren Daten, die mit ***DIABASS®6 PRO*** verwaltet werden. Alle personenbezogenen oder personenbeziehbaren Daten werden ausschließlich durch die Praxis/Klink selbst verarbeitet und werden auch nur dort lokal gespeichert. Es werden keine Patientendaten an mediaspects oder sonstige Dritte übermittelt oder zugänglich gemacht.

Info: Das ist der Unterschied zu Cloud-Lösungen

Wenn Arzt/Klinik die Nutzungsbedingungen eines Cloud-Anbieters akzeptieren und diesem damit eine über die zum Betrieb der Cloud technisch notwendige Datenverarbeitung weit hinausgehende Eigennutzung der Patientendaten ermöglichen wollen, besteht insoweit in der Regel eine gemeinsame Verantwortlichkeit mit dem Anbieter gem. Art. 26 DSGVO.

Die zu regelnde Verantwortlichkeit von Arzt/Klinik besteht dann primär darin, dem Anbieter eine kommerzielle Nutzung der Daten zu ermöglichen. Eine glaubhafte medizinische Notwendigkeit für eine solche Vereinbarung ist schwer vorstellbar. Derartige Kooperationen von Ärzten mit Anbietern verordnungsfähiger Produkte dürften zudem sowohl strafrechtlich (§§ 203, 299a ff StGB) als auch berufsrechtlich nicht unproblematisch sein.

Ist zur Verarbeitung der Gesundheitsdaten mit *DIABASS®6 PRO* eine gesonderte bzw. ausdrückliche Einwilligung der Patienten gem. Art. 9 Abs. 2 lit a) DSGVO erforderlich?

Nein. Die Erhebung und Verarbeitung dieser Daten erfolgt zur Erfüllung gesetzlicher Pflichten (u.a. § 630f BGB, § 10 MBO-Ä) von Arzt/Klinik bzw. zur Erfüllung des Behandlungsvertrags.

Gem. Art. 9 Abs. 2 lit h) DSGVO ist daher keine ausdrückliche Einwilligung erforderlich.

Info: Das ist der Unterschied zu Cloud-Lösungen

Die dortigen Nutzungsbestimmungen verlangen meist die Zustimmung, dass der Cloud-Anbieter die dort verarbeiteten Patientendaten auch für eigene Zwecke verwenden bzw. an Dritte weitergeben darf. Eine derart weitgehende Datenverarbeitung ist medizinisch bzw. zur Behandlung aber nicht *„erforderlich"* im Sinne von Art. 9 Abs. 2 lit h) DSGVO.

Es bedarf hierzu einer ausdrücklichen Einwilligung jedes einzelnen Patienten. Diese ist aber nur wirksam, wenn der Patient zuvor umfassend aufgeklärt wurde und er eine echte Wahlfreiheit hatte.

Daran ändert sich auch nichts, wenn der Patient seine Daten selbst in die Cloud einstellt:

Die Praxis/Klinik ist gem. Art. 4 Nr. 7 DSGVO trotzdem datenschutzrechtlich Verantwortlicher, denn sie allein entscheidet, ob ein vom Patienten bereitgestellter Cloud-Zugang als Mittel zur Datenverarbeitung für die Behandlungstätigkeit eingesetzt werden soll.

Eine solche Cloud-Nutzung wäre dann auch nicht „passiv", wie dies manche Anbieter behaupten: Denn der Behandler erzeugt beispielsweise durch den Umstand des „Einloggens", den Zeitabstand seiner Einsichtnahmen sowie Art und Umfang der abgerufenen Auswertungen auch selbst jeweils Daten, die der ärztlichen Schweigepflicht unterliegen. Die Praxis/Klinik trägt somit das volle Risiko, ob eine vom Patienten erhaltene „Cloud-Einladung" tatsächlich eine ausdrückliche, informierte und selbstbestimmte Einwilligung darstellt. Davon kann aber nur ausgegangen werden, wenn der der Patient umfassend aufgeklärt war und ihm seitens der Praxis/Klinik auch eine datensparsamere Alternative zur Übermittlung bzw. Verarbeitung seiner Daten angeboten wurde.

Muss *DIABASS®6 PRO* in das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) aufgenommen werden?

Ja. Praxis/Klinik sind verpflichtet, alle Verarbeitungstätigkeiten gem. Art. 30 DSGVO zu dokumentieren. Allerdings ist dies mit wenig Aufwand erledigt, da bei ***DIABASS®6 PRO*** nur wenige Angaben erforderlich sind. Auf Anfrage stellen wir gerne eine kostenlose Vorlage zur Verfügung.

Info: Das ist der Unterschied zu Cloud-Lösungen

Die Nutzungsbestimmungen aller gängigen Diabetes-Clouds sind sehr komplex und umfangreich. Arzt/Klinik müssen dort in eine Vielzahl von Datenverarbeitungsvorgängen einwilligen, die vielmals auch weit über die medizinisch notwendigen Zwecke hinausgehen. Alle Nutzungsbedingungen sowie als mitgeltend vereinbarten Dokumente müssen dann sorgfältig geprüft und alle dort geregelten Datenverarbeitungsvorgänge gem. Art. 30 DSGVO in das Verzeichnis aufgenommen werden. Das Verzeichnis darf inhaltlich nicht in Widerspruch zu den Nutzungsbedingungen stehen.

Muss für *DIABASS®6 PRO* eine Datenschutzfolgenabschätzung gem. Art. 35 DSGVO vorgenommen werden?

Eine Datenschutz-Folgenabschätzung muss durchgeführt werden, wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 35 DSGVO).

Dies wird man bei ***DIABASS®6 PRO*** nicht annehmen können, denn alle Daten werden ausschließlich im lokalen Netzwerk von Praxis/Klink verarbeitet und es werden nur bewährte Technologien eingesetzt.

Der Einsatz von ***DIABASS®6 PRO*** ist daher vergleichbar mit anderer lokaler Software, die im Rahmen der Behandlungstätigkeit genutzt wird, beispielsweise Word zum Schreiben der Arztbriefe oder lokal installierte Praxisverwaltungssoftware.

Info: Das ist der Unterschied zu Cloud-Lösungen

Dia Datenschutzbehörden haben eine Liste mit Datenverarbeitungen veröffentlicht, die zwingend eine Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO erfordern.

(https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/DSFA_muss_Liste_DSK_de.pdf)

Die meisten Diabetes-Clouds dürften mindestens eine der in dieser Liste beispielhaft genannten Verarbeitungstätigkeiten erfüllen, insbesondere Nr. 16, 17 und 15

Zudem setzen die Nutzungsbestimmungen vieler Diabetes-Clouds voraus, dass der Cloud-Anbieter die dort verarbeiteten Patientendaten auch für eigene Zwecke verwenden bzw. an Dritte weitergeben darf. Allein aus diesem Grund wird man dort wohl von einem hohen Risiko für die Rechte der Patienten ausgehen müssen.

Müssen kleinere Praxen zum Einsatz von *DIABASS®6 PRO* eigens einen Datenschutzbeauftragten bestellen?

Es ist nicht ersichtlich, dass der Einsatz von ***DIABASS®6 PRO*** einen Datenschutzbeauftragten erfordert.

Info: Das ist der Unterschied zu Cloud-Lösungen

Mit Diabetes-Clouds sind in der Regel Datenverarbeitungstätigkeiten verbunden, die in der Muss-Liste der Datenschutzbehörden zu Art. 35 DSGVO aufgeführt sind. Gerade wenn der Anbieter die Patientendaten auch für eigene Zwecke verwenden bzw. an Dritte weitergeben darf, wird man von einem hohen Risiko für die Rechte der Patienten ausgehen müssen.

Aufgrund der zwingenden gesetzlichen Sonderregelung in § 38 Abs. 1 S.2 BDSG führt die Nutzung einer Diabetes-Cloud daher regelmäßig dazu, dass in jedem Fall ein Datenschutzbeauftragter bestellt werden muss – unabhängig von der Anzahl der Praxismitarbeiter.

Was ist beim Einsatz von *DIABASS® SecureSend* zu beachten?

DIABASS® SecureSend dient der sicheren Übermittlung von Daten durch den Patienten.

Die Daten werden lokal auf dem PC bzw. Smartphone des Patienten hochsicher „end-to-end" verschlüsselt (AES-256) und dann per email an die Praxis/Klinik übermittelt. Abhängig von den lokalen Einstellungen beim Empfänger werden die Daten dann automatisch oder per Doppelklick durch den Programmbediener entschlüsselt und in den Datenbestand von ***DIABASS®6 PRO*** eingepflegt.

Allein der Patient entscheidet, ob er die Mail mit den verschlüsselten Daten über sein eigenes eMail-Programm versenden will oder ob er das Angebot zum Versand über den von mediaspects betriebenen Server nutzen möchte. In letzterem Fall werden die verschlüsselten Daten per eMail und mit neutraler Absenderadresse an den Empfänger weitergeleitet. Die verschlüsselten Daten können dabei weder von mediaspects oder Dritten eingesehen werden, die Verschlüsselungsinformationen sind nur bei Patient und Empfänger bekannt.

Info: Das ist der Unterschied zu Cloud-Lösungen

Bei einer Datenübermittlung unter Einsatz von Cloud-Lösungen erfolgt regelmäßig keine end-to-end-Verschlüsselung, sondern lediglich eine Transportverschlüsselung. Die Gesundheitsdaten werden daher dem Cloud-Anbieter zugänglich gemacht. Zudem müssen Patient und Arzt fast immer in die kommerzielle Nutzung der Daten durch den Anbieter bzw. in die Weitergabe der Daten an Dritte einwilligen, ansonsten kann die Cloud gar nicht genutzt werden.

Birgt der Einsatz von *DIABASS®6 PRO* für Arzt/Diabetesberatung das Risiko, dass Daten zu ihrem Verordnungsverhalten, zur Behandlungsqualität oder zu ihrem Nutzungsverhalten gesammelt und womöglich von Dritten ausgewertet und dokumentiert werden?

Nein. Solche Daten zum Nutzungsverhalten werden durch ***DIABASS®6 PRO*** nicht erhoben. Alle beim Einsatz von ***DIABASS®6 PRO*** entstehenden Daten werden nur lokal gespeichert und sind Dritten nicht zugänglich.

Info: Das ist der Unterschied zu Cloud-Lösungen

Die Nutzungsbestimmungen der meisten Cloud-Lösungen sehen vor, dass solche Nutzungs- und Qualitätsdaten umfassend vom Anbieter verwendet und/oder an Dritte weitergegeben werden dürfen. Aber auch manche lokal arbeitende Diabetes-Managementsoftware übermitteln Telemetrie- und Nutzungsdaten an den Hersteller, ohne dass die Nutzer hierüber wahrnehmbar informiert werden.

Sind Cloud-Lösungen nicht besser als lokale Lösungen?

In Publikationen oder Vortragveranstaltungen wird gerne behauptet, dass eine „Cloud" wünschenswert bzw. optimal für das ärztliche Diabetes-Datenmanagement sei. Häufig handelt es sich dabei aber nur um Werbebehauptungen, die einer kritischen Nachfrage nicht standhalten.

Nachstehend einige Beispiele

Behauptung …	… und Wirklichkeit
Die Cloud hat den Vorteil, dass der Patient die Daten selbst einstellt und das Diabetes-Team immer aktuelle Werte nutzen kann, man erspart sich die Mühen einer Datenübertragung	Hierfür ist keine Cloud erforderlich. Mit den Telemedizinfunktionen geeigneter lokaler Software wie ***DIABASS®6 PRO*** kann dieselbe Funktionalität erreicht werden – und dies ohne die mit einer Cloud verbundenen Risiken (beispielsweise: Bußgeldrisiko bei unzulässigen Datenweitergaben, kein Datenzugriff ohne Internetverbindung, gestörte Erreichbarkeit/ Verfügbarkeit der Cloud, ...).
Bei einer Cloud muss man nichts installieren	Bei fast allen Diabetes-Clouds muss ein sog. Uploader installiert werden. Zudem muss auch die Firewall geöffnet werden, um den Cloud-Zugang zu ermöglichen – mit allen Konsequenzen für die IT-Sicherheit von Praxis/Klinik.
Die Cloud spart Speicherplatz, da die Patientendaten extern lagern	Das ist zwar richtig, dürfte tatsächlich aber kaum eine Rolle spielen: selbst umfängliche Datenbestände (CGM und Insulinpumpe) von tausenden Patienten über den vorgeschriebenen indestaufbewahrungszeitraum (10 Jahre) lassen sich mühelos auf einem handelsüblichen USB-Stick speichern.
Die Cloud ist kostenlos bzw. kostengünstiger als die Anschaffung von lokaler Software	In Bezug auf die reinen Anschaffungskosten mag dies bei Cloud-Lösungen zutreffen, die zu einem unrealistisch niedrigen, korruptiven Preis offeriert werden. Die Annahme solcher Zuwendungen bzw. geldwerter Vorteile birgt straf- und steuerrechtlich allerdings erhebliche Risiken. Neben dem reinen Kaufpreis müssen aber auch die erheblichen Begleitkosten berücksichtigt werden, die mit dem rechtskonformen Einsatz einer Cloudlösung zwingend einhergehen. Die notwendige juristische Prüfung der meist komplexen Nutzungsbedingungen und die Durchführung einer vorgeschriebenen Datenschutzfolgeabschätzung sind mit beträchtlichen Kosten verbunden. Auch der erforderliche Personalaufwand zur Patientenaufklärung, zur Einholung wirksamer Einwilligungen sowie zur laufenden Erfüllung der gesetzlich vorgeschriebenen, administrativen Datenschutzpflichten ist erheblich.
„Unsere Cloud ist rechtlich geprüft und alles ist zulässig"	Eine durch Praxis/Klinik selbst veranlasste juristische Prüfung wird oft wohl zu anderem Ergebnis führen. Zudem müssen sich Arzt/Klinik im „Kleingedruckten" meist verpflichten, die alleinige Verantwortung für die rechtliche Zulässigkeit der Cloud-Nutzung zu übernehmen.
„Der Datenschutz unserer Cloud ist zertifiziert; der Server steht in Deutschland bzw. der EU"	Dies allein macht die Cloud-Nutzung nicht zulässig oder unproblematisch. Der Serverstandort in Europa vermeidet lediglich die zusätzlichen Probleme, die mit einer Datenübermittlung in Drittstaaten verbunden sind. Und die Zertifizierung des Anbieters spielt für die eigene Verantwortlichkeit von Praxis/Klinik keine Rolle.

DIABASS®

Eine Software für alle Messgeräte

WEITERE INFORMATIONEN

www.diabass.com

Beratungsgesellschaft
für neue Medien mbH
Postfach 10 07 31
D-72307 Balingen

Tel.: +49 (0) 7433 96 75 970
Fax: +49 (0) 7433 96 75 971
E-Mail: info@mediaspects.de
Internet: www.mediaspects.de