Vorteile von *DIABASS®* SecureSend

- Empfang der Daten aus **mehr als 200 Messgeräten** (BGM, CGM, Insulinpumpen, Blutdruck)
- **Kompatibel mit zahlreichen Tagebuch-Apps** für Diabetes und Blutdruck (z. B. mySugr, Contour Diabetes-App, OMRON, …)
- Keine Preisgabe von **Patientendaten** an Dritte
- Hochsichere end-to-end **Verschlüsselung** (AES-256)
- Absolut **einfach** zu bedienen
- Daten werden **automatisch** in die Auswertesoftware ***DIABASS®*** übernommen
- **Keine Abhängigkeit** von der Verfügbarkeit von Cloud-Diensten
- **Kostenlose Software/App** für Patienten
- **Offen für alle** Hersteller und Systeme
- Datenempfang kann **pausiert** werden
- Anzeige von **Praxislogo und tagesaktuellen Informationen** (z. B. Urlaub) in der App

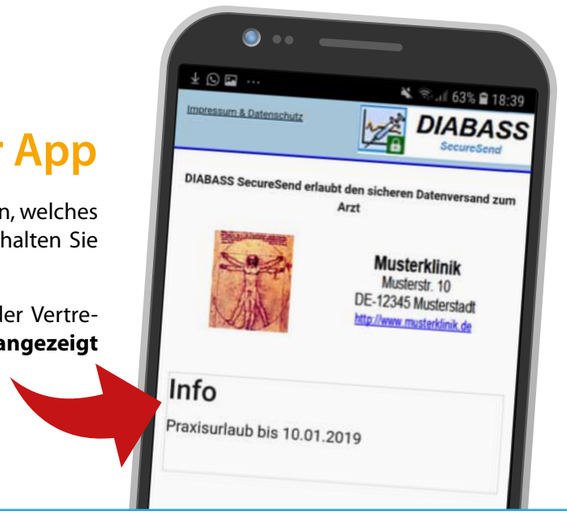
Offen für alle Messsysteme und Apps

Mit der kostenlosen Upload-Software kann der Patient die Daten aus allen gängigen Blutzuckermessgeräten, aus FGM/CGM und Insulinpumpen, aus Blutdruckmessgeräten und sonstigen Geräten (z. B. Schrittzähler) einlesen und schicken. Die kostenlose Apps für iOS/Android ermöglicht den Datenversand aus zahlreichen Tagebuch-Apps für Diabetes und Blutdruck. Die Liste der kompatiblen Geräte/Apps wird laufend erweitert.

Zusatznutzen: Ihr Praxislogo in der App

Auf Wunsch können Sie ein Praxis-Logo hinterlegen, welches dann in der Patienten-App angezeigt wird. So erhalten Sie quasi eine eigene Diabetes-App für Ihre Praxis.

Tagesaktuelle Informationen wie Praxisurlaub oder Vertretung können ebenfalls hinterlegt und **in der App angezeigt werden**.



Ein Produkt der mediaspects GmbH,
Postfach 10 07 31, D-72307 Balingen

DIABASS® SecureSend

Datenempfang aus Messgeräten und Diabetes-Apps

- kompatibel mit über 200 Messgeräten
- kompatibel mit zahlreichen Diabetes-Apps
- ohne die Nachteile von Cloud-Lösungen

A124-09122019; Bildnachweis: © ra2 studio – fotolia.com (Titelmotiv)

Cloud-Lösungen zum Diabetes-Management: kennen Sie die Risiken und Begleitkosten?

Cloudbasierte Lösungen zum digitalen Diabetes-Management bringen für Ärzte/Kliniken **erhebliche Verpflichtungen und Risiken:**

- ⚠ **Datenschutzfolgeabschätzung** gem. Art. 35 DSGVO bzw. DIN ISO 29134 erforderlich
- ⚠ **Konsultation mit den Behörden** in vielen Fällen unabdingbar (Art. 36 DSGVO)
- ⚠ Verpflichtung zur Bestellung eines **Datenschutzbeauftragten**, auch für kleine Praxen (§ 38 BDSG)
- ⚠ Arzt/Klinik muss meist in die **kommerzielle Nutzung** der Patientendaten einwilligen
- ⚠ **hohes Bussgeldrisiko:** Arzt/Klinik haften für Datenschutzverstöße des Anbieters mit
- ⚠ Arzt/Klinik muss sich um **wirksame Einwilligung** der Patienten bemühen

Die Alternative: *DIABASS®* SecureSend

Ersparen Sie sich die Risiken und Nachteile, die mit dem Einsatz einer Cloud verbunden sind: Lassen Sie sich doch vom Patienten die Daten aus Messgeräten und Diabetes-Apps schicken.

DIABASS® SecureSend bietet hierzu eine **rechtssichere und komfortable Lösung:** Die Daten werden auf dem Computer bzw. Smartphone des Patienten nach höchstem Standard (AES-256) verschlüsselt und dann per E-Mail übermittelt. Durch die „end-to-end" Verschlüsselung ist sichergestellt, dass kein Dritter Einsicht in die Daten hat.

So einfach ist es

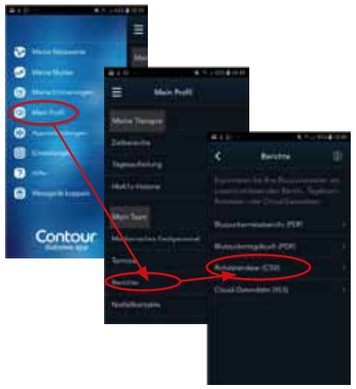
1. Drucken Sie dem Patienten ein Infoblatt mit Zugangsdaten und einer Anleitung.
2. Der Patient liest zu Hause sein Messgerät aus bzw. schickt Daten aus seiner Diabetes-App
3. Sie erhalten eine E-Mail mit einem verschlüsselten Anhang.
4. Die Mail wird automatisch abgerufen, entschlüsselt und in ***DIABASS®*** übernommen

So einfach ist der Datenerhalt aus Diabetes Apps

Beispiel: Contour Diabetes App

Schritt 1

Wechseln Sie in der Contour Diabetes App in das Menü **MEIN PROFIL**, von dort in **BERICHTE.** Klicken Sie dort dann auf **ROHDATENDATEI (CSV).**



Schritt 2

Klicken Sie auf das **TEILEN** Symbol am linken unteren Bildschirmrand. Wählen Sie in der erscheinenden Liste die App ***DIABASS® SecureSend*** aus.

Schritt 3

Die ***DIABASS® SecureSend*** App startet nun automatisch. Wählen Sie beim ersten Start **„ANDERER EMPFÄNGER"** und scannen den vom Arzt erhaltenen Barcode.

Schritt 4

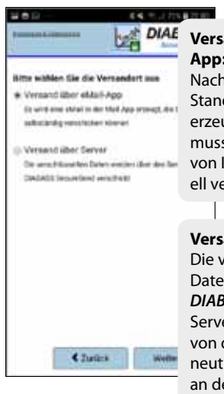
Klicken Sie auf **WEITER**. Es werden nun die vom Barcode gelesenen Versanddaten angezeigt. Wenn die Angaben richtig sind, klicken Sie auf **WEITER**.

Schritt 5

Hier können Sie eine (optionale) Nachricht für den Empfänger eingeben. Klicken Sie dann auf **WEITER**.

Schritt 6

Die Daten sind nun hochsicher verschlüsselt (AES-256) und für die Übermittlung vorbereitet.Wählen Sie nun die Versandart aus und bestätigen mit **WEITER**.



Versand über E-Mail App: Es wird eine Nachricht in Ihrer Standard-Email-App erzeugt, die Nachricht muss anschließend von Ihnen noch manuell versendet werden.

Versand über Server: Die verschlüsselten Daten werden an den ***DIABASS® SecureSend***-Server übermittelt und von dort per E-Mail mit neutralem Absender an den Empfänger weitergeschickt.