
Datenempfang aus Messgeräten
und Diabetes-Apps
Omnitest
B. BRAUN
connect
omron
kompatibel mit über 200 Messgeräten
kompatibel mit zahlreichen Diabetes-Apps
ohne die Nachteile von Cloud-Lösungen

Hauptproblem beim digitalen Diabetes-Datenmanagement: wie kommen die Daten zum Arzt ?

Einlesen der Geräte in der Praxis kostet Zeit und ist fehleranfällig.

Patienten „vergessen“ mitunter, das Gerät zum Termin mitzubringen

Benötigte Kabel sind nicht vorhanden/ nicht betriebsbereit

Manche Systeme verfügen über keine Kabelverbindung mehr; Hardware zur Kommunikation per Bluetooth/BLE oder NFC in Praxen/Kliniken vielmals nicht verfügbar oder zugelassen.

Nutzung der von Geräteherstellern/Pharmafirmen angebotenen Cloud-Lösungen birgt massives Problempotential:

- Cloud-Nutzung bringt qua Gesetz erheblichen administrativen Zusatzaufwand mit entsprechenden Kosten, worüber sich viele Ärzte nicht bewusst sind
- Hohe Bußgeldrisiken bei Datenschutzverstoß, die Arzt selbst tragen muss und auf niemanden abwälzen kann
- Übermittlung von Patientendaten an Industrie zur kommerziellen Nutzung ist ethisch wie rechtlich hochproblematisch: Hohes Risiko eines Bruchs der ärztlichen Schweigepflicht sowie damit einhergehender Datenschutzstraftaten!
- Bei Internet-Störung oder Störung des Cloud-Anbieters: kein Zugriff auf die Daten möglich
- In der Cloud liegende Daten unterliegen keinem Beschlagnahmeverbot, Arzt kann ungewollte Nutzung dieser Daten nicht unterbinden: Behandlungsleistung des Arztes wird einfacher überprüfbar, u.a. nach Vorkommnissen (zB Unfall in Hypo)

Risiko DSGVO: erste empfindliche Bußgelder auch im medizinischen Bereich

Haga Hospital, Den Haag (Holland): 460.000,00 EUR Bußgeld !

„Erst kürzlich wurde das größte Krankenhaus in Den Haag, das Haga Hospital, wegen eines Verstoßes gegen die DSGVO mit einem Bußgeld in Höhe von 460.000 Euro belegt. Die niederländische Aufsichtsbehörde hat einen nicht ausreichenden Schutz der Patientendaten bemängelt“
https://www.datenschutz-notizen.de/fehlendes-berechtigungskonzept-im-krankenhaus-ein-bussgeldbewaehrtes-risiko-0823168/

Barreiro Hospital, Portugal: 400.000,00 EUR Bußgeld !

„The Barreiro Hospital in Portugal was fined 400,000 € by the Portuguese Data Protection Authority CNPD (Comissão Nacional de Proteção de Dados) for incompliancy with the EU General Data Protection Regulation (GDPR) by not separating access rights to patents’ clinical data.“

https://www.datenschutz-notizen.de/portuguese-data-protection-authority-imposes-400000-e-fine-on-hospital-4821441/

Krankenhaus in Rheinland-Pfalz: 105.000,00 EUR Bussgeld !

„Der rheinland-pfälzische Datenschutzbeauftragte will die Geldbuße auch als Signal verstanden wissen, im Gesundheitswesen besonders wachsam zu sein.“

https://www.heise.de/newsticker/meldung/DSGVO-Verstoss-Krankenhaus-in-Rheinland-Pfalz-muss-105-000-Euro-zahlen-4604348.html

Baden-Württemberg: 80.000,00 EUR Bußgeld !

Gesundheitsdaten landeten versehentlich im Internet

https://www.esslinger-zeitung.de/region/baden-wuerttemberg_artikel,-eu-datenschutzregeln-machen-viel-arbeit-_arid,2237519.html

Krankenhaus in Bayern: vierstelliges Bussgeld

Vierstelliges Bußgeld, nur weil Klinik einen Schwerbehindertenausweis versehentlich an falschen Patienten aushändigte.

https://www.handelsblatt.com/politik/deutschland/datenschutzgrundverordnung-behoerden-verhaengen-erste-bussgelder-wegen-verstoessen-gegen-dsgvo/23872806.html

Risiko DSGVO: Datenübermittlung in Cloud / an Hersteller von Insulinpumpen/CGM

Viele Patienten nutzen für CGM/Insulinpumpe eine Hersteller-App und laden Daten in dortige Cloud.

Hohes Risiko für Ärzte/Kliniken:

Auch bei Einladung/Freigabe durch Patient bleibt Arzt „Verantwortlicher“ gem. Art. 4 DSGVO

Cloudnutzung generell nur dann einigermaßen unproblematisch, wenn ein wirksamer (!) Auftragsverarbeitungsvertrag gem. Art. 28 DSGVO mit dem Cloud-Anbieter vorliegt.

Ein wirksamer AV-Vertrag setzt aber u.a. zwingend voraus:

- Cloud-Anbieter darf Daten **nicht für eigene Zwecke** (mit-)nutzen
- Schriftlicher Vertrag zwischen Verantwortlichem (Arzt) und Cloud-Anbieter
- Tatsächliche Weisungsbefugnis des Arztes in Bezug auf die Daten

Cave 1: Arzt haftet für Datenschutzverstöße des Cloud-Anbieters (Art. 82 DSGVO)

Cave 2: „Die Auftragsverarbeitung stellt keine Befugnis im Sinne von § 203 StGB dar.“

„Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der BÄK, Deutsches Ärzteblatt | 09. 03. 2018 | DOI: 10.3238/arztebl.2018.ds01

Cave 3: „Tarnung“ einer unzulässigen Datenverarbeitung als zulässige Auftragsverarbeitung indiziert vorsätzlichen Datenschutzverstoß !

Risiko DSGVO: Datenübermittlung in Cloud / an Hersteller von Insulinpumpen/CGM

Aktuelle Auffassung der deutschen Datenschutzbehörden: Cloud-Nutzung durch Arzt **besonders risikobehaftete Tätigkeit**

16	Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich" im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Arzt nutzt ein Webportal oder setzt eine App an, um mit Patienten mittels Videotelefonie zu kommunizieren und Gesundheitsdaten durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,...) detailliert und systematisch zu erheben und zu verarbeiten.

http://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_MussListe_Version_1.1_Deutsch.pdf

(abgerufen am 12.11.2019)

Cave: Arzt/Klinik muss daher Anforderungen aus Art. 35 DSGVO und § 38 (1) S. 2 BDSG erfüllen.

Datenschutzbehörden haben Bussgeldkonzept veröffentlicht, um Rechtsverstöße bundesweit einheitlich zu ahnden.

Bei Verstössen bzgl. Patientendaten oder Nichtbeachtung der Pflichten aus Art. 35 DSGVO wird selbst eine kleine Einzelpraxis daher mit einem Bussgeld von kaum unter 20.000,00 EUR rechnen müssen.

https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf

(abgerufen am 12.11.2019)

Risiko DSGVO: Datenübermittlung in Cloud / an Hersteller von Insulinpumpen/CGM

Nutzung von cloudbasierten Datenmanagementlösungen bringt somit erhebliche Pflichten und Zusatzkosten:

- Dokumentation im Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Ausführliche Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO und ISO/IEC 29134 (!)
- Gem. § 38 (1) S.2 BDSG **zwingend**: Bestellung eines Datenschutzbeauftragten, unabhängig von Praxisgröße !
- Informationspflicht gem. Art 13 DSGVO auch in Bezug auf die Cloud-Lösung
- Umfassende Aufklärung des Patienten
- Unaufgeforderte, unverzügliche Meldung von Datenpannen (auch des Cloud-Anbieters) innerhalb 72 Stunden an die Aufsichtsbehörde (Art. 33 DSGVO)
- Wohl auch: Pflicht zur vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DSGVO)

Cave 1: Wenn kein wirksamer AV-Vertrag vorliegt, dann muss von jedem Patienten eine selbstbestimmte Einwilligung vorliegen, was eine vorausgegangene und umfassende Aufklärung über die Abläufe voraussetzt.

Cave2: Die obigen Pflichten müssen für jede eingesetzte Cloud-Lösung separat erfüllt werden!

Risiko DSGVO: Datenübermittlung in Cloud / an Hersteller von Insulinpumpen/CGM

Lösung: Patient schickt Daten ohne Umweg über Dritte, welche kommerziell die Daten nutzen wollen

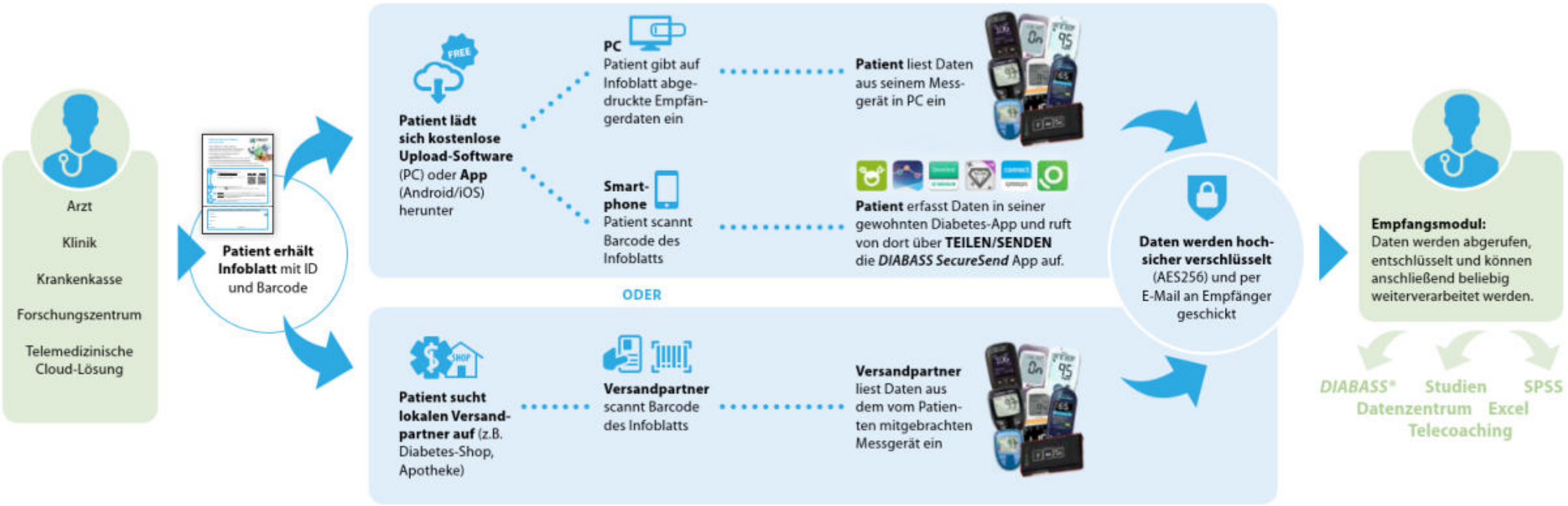
Alternative: Sicher verschlüsselter Datenversand mittels DIABASS SecureSend

Patient schickt die Daten mittels DIABASS SecureSend hochverschlüsselt per eMail

- Kostenlose Übertragungssoftware/App für Patienten
- Übertragungsmodul für PC erlaubt Datenübertragung aus allen Messgeräten
- App erlaubt Datenversand aus diversen Diabetes-Apps

Hochsichere und komfortabel Datenübertragung per DIABASS SecureSend

So einfach funktioniert es:



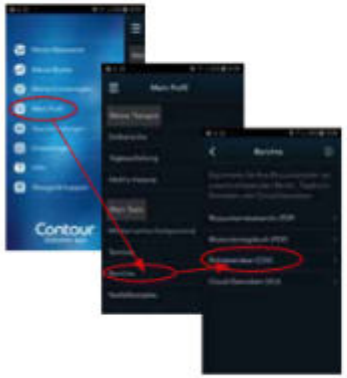
Hochsichere und komfortabel Datenübertragung per DIABASS SecureSend

So einfach ist der Datenerhalt aus Diabetes Apps

Beispiel: Contour Diabetes App

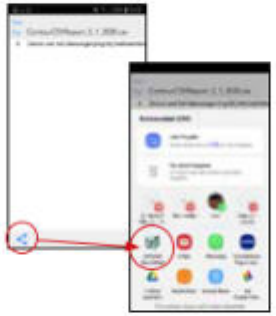
Schritt 1

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

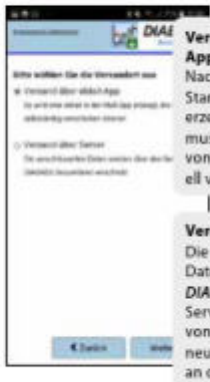
Klicken Sie auf **WEITER**. Es werden nun die vom Barcode gelesenen Versanddaten angezeigt. Wenn die Angaben richtig sind, klicken Sie auf **WEITER**.

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.

Hochsichere und komfortabel Datenübertragung per DIABASS SecureSend

Vorteile für Arzt/Klinik:

- Hochsichere Verschlüsselung (AES-256), allein Arzt kann Daten entschlüsseln
- Datenversand erfolgt per eMail, keine Cloudnutzung erforderlich
- Keine Zusatzanforderungen in Bezug auf DSGVO
- Zeitgewinn, da Patient die Arbeit des Geräteauslesens übernimmt
- Tagesaktuelle Praxisinfo für Patienten möglich (z.B. Hinweis auf Praxisurlaub)
- Datenempfang kann pausiert werden
- eMail-Adresse zum Datenempfang kann von Praxis/Klinik jederzeit geändert werden
- Werbe-/Marketingtool für Praxis: Software/App mit eigenem Praxis-/Kliniklogo
- In Lizenzpreis von DIABASS enthalten

Software/App zum sicheren Datenversand

DIABASS® SecureSend

Liebe Patientin, lieber Patient,

damit wir unseren Termin besser vorbereiten und noch mehr Zeit für das Gespräch mit Ihnen haben, können Sie uns die Werte aus Ihrem Messgerät oder aus zahlreichen Apps vorab zusenden.

Hierzu können Sie die kostenlose Übertragungssoftware bzw. App ***DIABASS® SecureSend*** nutzen.

DIABASS® SecureSend verschlüsselt die Daten bereits auf Ihrem PC/Smartphone („end-to-end") und erlaubt einen direkten Versand an uns, so dass kein Dritter die Daten einsehen kann. Die Verschlüsselung erfolgt nach dem AES-256 Standard, der in zahlreichen Ländern für staatliche Dokumente mit höchstem Geheimhaltungsgrad zugelassen ist.

Ihre Daten können nur bei uns entschlüsselt und Ihnen als Person wieder zugeordnet werden.

1. ***DIABASS® SecureSend*** herunterladen und installieren.

   Software für Windows + Anleitungen

   Unter nachstehendem Link können Sie die PC-Software sowie weitere Anleitungen herunterladen:

   `https://www.diabass.com/ss.php?id=TZRA`

   JETZT BEI Google Play

   Laden im App Store

2. Starten Sie die ***DIABASS® SecureSend*** Software bzw. App.
   Scannen Sie den **unten abgedruckten QR-Code** oder geben Sie die Zugangsdaten manuell ein.

3. **PC Windows:** Lesen Sie Ihr Messgerät/Insulinpumpe mit ***DIABASS® SecureSend*** ein. Alternativ können Sie auch Daten übernehmen, die Sie zuvor aus einer Cloud-Lösung (z.B. Clarity,LibreView, CareLink) heruntergeladen haben.
   Smartphone: Klicken Sie in Ihrer Diabetes-App (z.B. MySugr, Contour Diabetes App) auf **SENDEN** oder **TEILEN** und wählen dann die ***DIABASS® SecureSend*** App aus.

4. Sie können nun noch eine Nachricht für uns eingeben, anschließend werden die Daten hochsicher verschlüsselt und per E-Mail an uns verschickt.

Bildnachweis: © ra2 studio - Fotolia.com

Bitte tragen Sie die nachstehenden Angaben in die *DIABASS® SecureSend* Software/App ein.

Empfänger:	**Musterklinik, 12345-Musterstadt**
Patientencode:	**A331FD**
Vorname:	**Test**
Name:	**SecureSend**
Geburtstag:	**01.01.1955**
Empfänger-ID:	**TZRA**