inSuite

Arzt- und Praxissoftware
der 3. Generation

IT-Informationen zur inSuite

Technologie, Datenschutz & DSGVO

DocCirrus

www.doc-cirrus.com

Unsere Mission

Mit unserer Software wollen wir die Gesundheitsversorgung verbessern - für Ärzte wie Patienten.

Durch unsere offene Plattform wollen wir allen Beteiligten die Möglichkeit moderner Vernetzung und Zusammenarbeit unter höchsten Sicherheitsstandards bieten.

Mit innovativen Partnern und Technologien wollen wir alle Vorteile der Digitalisierung zum Wohle von Ärzten und Patienten nutzbar machen.

Ihr Doc Cirrus Team

DocCirrus

Wir sind die Technologieplattform für das Gesundheitswesen der Zukunft.

Inhalt

Sehr geehrte/r Interessent/in,

diese Broschüre dient Ihrer Erstinformation. Wenn Sie vollständige, tagesaktuelle und für den Betrieb praktische Anleitungen und Informationen benötigen, dann zögern Sie nicht, uns zu kontaktieren. Wir wünschen viel Spaß beim Erkunden der inSuite-Technologie.

Das Ziel: Patientendaten schützen und KBV-Empfehlungen beachten

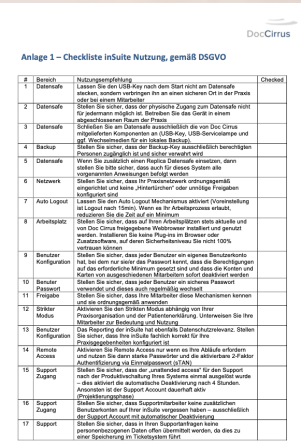
Um dem aller Infos zu Grund liegenden Ziel, dem Schutz der Patientendaten, gerecht zu werden, stellen wir hinsichtlich der digitalen Einhaltung der DSGVO unseren Kunden einen detaillierten Maßnahmen- und Empfehlungskatalog zur Verfügung, den Sie mit der inSuite einfach und flexibel umsetzen können.

Die Kassenärztliche Bundesvereinigung hat dazu umfassende Informationen veröffentlicht:

- https://www.kbv.de/media/sp/Praxisinformation_Datenschutz_DSGVO.pdf
- https://www.kbv.de/media/sp/Praxisinformation_Datenschutz_Checkliste.pdf

Diese Vorgaben sind nicht einfach umzusetzen. Je nach dem, welches AIS bzw. welche Arztsoftware Sie für die Erhebung und Bearbeitung von Patientendaten verwenden, kann das einfach bis schwierig sein und sogar teilweise am Rande der Unmöglichkeit liegen.

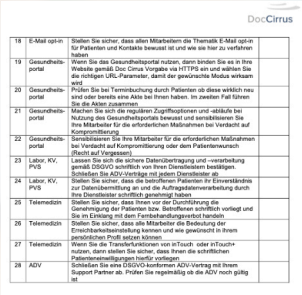
Unsere Kunden haben dazu eine detaillierte Empfehlungsliste erhalten, die Ihnen dabei hilft, die KBV-Anweisungen adäquat umzusetzen.



DocCirrus

Anlage 1 – Checkliste inSuite Nutzung, gemäß DSGVO

#	Bereich	Nutzungsempfehlung	Checked
1	Datensafe	Lassen Sie den USB-Key nach dem Start nicht am Datensafe stecken, sondern verbringen ihn an einen sicheren Ort in der Praxis oder bei einem Mitarbeiter.	
2	Datensafe	Stellen Sie sicher, dass der physische Zugang zum Datensafe nicht für jedermann möglich ist. Betreiben Sie das Gerät in einem abgeschlossenen Raum der Praxis	
3	Datensafe	Schließen Sie am Datensafe ausschließlich die von Doc Cirrus mitgelieferten Komponenten an (USB-Key, USB-Servicelampe und ggf. Wechselmedien für ein lokales Backup).	
4	Backup	Stellen Sie sicher, dass der Backup-Key ausschließlich berechtigten Personen zugänglich ist und sicher verwahrt wird	
5	Datensafe	Wenn Sie zusätzlich einen Replica Datensafe einsetzen, dann stellen Sie bitte sicher, dass auch für dieses System alle vorgenannten Anweisungen befolgt werden	
6	Netzwerk	Stellen Sie sicher, dass Ihr Praxisnetzwerk ordnungsgemäß eingerichtet und keine „Hintertürchen" oder unnötige Freigaben konfiguriert sind	
7	Auto Logout	Lassen Sie den Auto Logout Mechanismus aktiviert (Voreinstellung ist Logout nach 15min). Wenn es Ihr Arbeitsprozess erlaubt, reduzieren Sie die Zeit auf ein Minimum	
8	Arbeitsplatz	Stellen Sie sicher, dass auf Ihren Arbeitsplätzen stets aktuelle und von Doc Cirrus freigegebene Webbrowser installiert und genutzt werden. Installieren Sie keine Plug-Ins im Browser oder Zusatzsoftware, auf denen Sicherheitsniveau Sie nicht 100% vertrauen können.	
9	Benutzer Konfiguration	Stellen Sie sicher, dass jeder Benutzer ein eigenes Benutzerkonto hat, das nur er zusammen mit dem Passwort kennt, dass die Berechtigungen auf das erforderliche Minimum gesetzt sind und dass die Konten und Karten von ausgeschiedenen Mitarbeitern sofort deaktiviert werden.	
10	Benuter Passwort	Stellen Sie sicher, dass jeder Benutzer ein sicheres Passwort verwendet und dieses auch regelmäßig wechselt.	
11	Freigabe	Stellen Sie sicher, dass Ihre Mitarbeiter diese Mechanismen kennen und sie ordnungsgemäß anwenden	
12	Strikter Modus	Aktivieren Sie den Strikten Modus abhängig von Ihrer Praxisorganisation und der Patientenerklärung. Unterweisen Sie Ihre Mitarbeiter zur Bedeutung und Nutzung	
13	Benutzer Konfiguration	Das Reporting der inSuite hat ebenfalls Datenschutzrelevanz. Stellen Sie sicher, dass Ihre inSuite fachlich korrekt für Ihre Praxisgegebenheiten konfiguriert ist	
14	Remote Access	Aktivieren Sie Remote Access nur wenn es Ihre Abläufe erfordern und nutzen Sie dann starke Passwörter und die aktivierbare 2-Faktor Authentifizierung via Einmalpasswort (sTAN).	
15	Support Zugang	Stellen Sie sicher, dass der „unattended access" für den Support nach der Produktivschaltung Ihres Systems einmal ausgelöst wurde – dies aktiviert die automatische Deaktivierung nach 4 Stunden. Ansonsten ist der Support Account dauerhaft aktiv (Projektierungsphase).	
16	Support Zugang	Stellen Sie sicher, dass Supportmitarbeiter keine zusätzlichen Benutzerkonten auf Ihrer inSuite vergeben haben – ausschließlich der Support Account mit automatischer Deaktivierung	
17	Support	Stellen Sie sicher, dass in Ihren Supportanfragen keine personenbezogenen Daten offen übermittelt werden, da dies zu einer Speicherung im Ticketsystem führt	



DocCirrus

18	E-Mail opt-in	Stellen Sie sicher, dass allen Mitarbeitern die Thematik E-Mail opt-in für Patienten und Kontakte bewusst ist und wie sie hier zu verfahren haben	
19	Gesundheits-portal	Wenn Sie das Gesundheitsportal nutzen, dann binden Sie es in Ihre Website gemäß Doc Cirrus Vorgabe via HTTPS ein und wählen Sie die richtigen URL-Parameter, damit der gewünschte Modus wirksam wird	
20	Gesundheits-portal	Prüfen Sie bei Terminbuchung durch Patienten ob diese wirklich neu sind oder bereits eine Akte bei Ihnen haben. Im zweiten Fall führen Sie die Akten zusammen	
21	Gesundheits-portal	Machen Sie sich die regulären Zugriffsoptionen und -abläufe bei Nutzung des Gesundheitsportals bewusst und sensibilisieren Sie Ihre Mitarbeiter für die erforderlichen Maßnahmen bei Verdacht auf Kompromittierung	
22	Gesundheits-portal	Sensibilisieren Sie Ihre Mitarbeiter für die erforderlichen Maßnahmen bei Verdacht auf Kompromittierung oder dem Patientenwunsch (Recht auf Vergessen)	
23	Labor, KV, PVS	Lassen Sie sich die sichere Datenübertragung und –verarbeitung gemäß DSGVO schriftlich von Ihren Dienstleistern bestätigen. Schließen Sie ADV-Verträge mit jedem Dienstleister ab	
24	Labor, KV, PVS	Stellen Sie sicher, dass die betroffenen Patienten Ihr Einverständnis zur Datenübermittlung an und die Auftragsdatenverarbeitung durch Ihre Dienstleister schriftlich genehmigt haben	
25	Telemedizin	Stellen Sie sicher, dass Ihnen vor der Durchführung die Genehmigung der Patienten bzw. Betroffenen schriftlich vorliegt und Sie im Einklang mit dem Fernbehandlungsverbot handeln	
26	Telemedizin	Stellen Sie sicher, dass alle Mitarbeiter die Bedeutung der Erreichbarkeitseinstellung kennen und wie gewünscht in Ihrem persönlichen Profil setzen können	
27	Telemedizin	Wenn Sie die Transferfunktionen von inTouch- oder inTouch+ nutzen, dann stellen Sie sicher, dass Ihnen die schriftlichen Patientenerweiterungen hierfür vorliegen	
28	ADV	Schließen Sie eine DSGVO-konformen ADV-Vertrag mit Ihrem Support Partner ab. Prüfen Sie regelmäßig ob die ADV noch gültig ist	

Das Ziel: Patientendaten schützen und KBV-Empfehlungen beachten

Mit der inSuite vom Start weg bestens aufgestellt

Der Einsatz der inSuite als modernes und sicheres Praxisverwaltungssystem der 3. Generation ist nämlich bereits ein wesentlicher Bestandteil Ihrer Datenschutz-Maßnahmen.

Grundsätzlich ist es so, dass Praxen und Anwender die alleinige Verantwortung für ihr Handeln und die Konsequenzen, wenn sie die Nutzungsvorgaben bewusst oder fahrlässig missachten. Aus diesem Grund ist die inSuite von A- Z nach dem Prinzip „Privacy by Design and Default“ entwickelt worden. Bedeutet: Der Datenschutz ist allein durch die Technikgestaltung und datenschutzfreundliche Voreinstellungen in großem Umfang gewährleistet.

Im Rahmen der DSGVO erlangen sie jedoch neue Bedeutung. Unser **„Privacy by Design“** greift den Grundgedanken auf, dass sich der Datenschutz am besten einhalten lässt, wenn ein frühzeitiges Ergreifen technischer und organisatorischer Maßnahmen möglich ist.

Unsere Kunden haben auch dank **„Privacy by Default“** (Datenschutz durch datenschutzfreundliche Voreinstellungen) sehr überschaubaren Aufwand, weil die Werkeinstellungen datenschutzfreundlich ausgestaltet und voreingestellt sind. Wir wollen Nutzer schützen, die weniger technikaffin sind und z.B. dadurch nicht geneigt sind, die datenschutzrechtlichen Einstellungen ihren Wünschen und Pflichten gem. DSGVO entsprechend anzupassen. Die inSuite wurde daher unter diesen Aspekten konzipiert und nach aktuellstem Wissen entwickelt.

Datenschutzgrundverordnung (DSGVO) in der inSuite

Mit der folgenden Auswahl an funktionalen Aspekten stellen Sie als inSuite- Kunde einen sicheren, maßgeschneiderten Datenschutz her (1/3)

- Mit dem Doc Cirrus Datensafe speichern Sie **personenbezogene** Daten stets lokal
- Die **Speicherung** erfolgt automatisch auf verschlüsselten Festplatten
- Für einen effektiven **Diebstahlschutz** verwenden Sie beim Hochfahren einen USB- Key zum Entschlüsseln der Festplatten
- Der Datensafe ist nicht anfällig für Viren, Trojaner (wie andere Praxissysteme)
- Manuelle und zeitgesteuerte **Backups** sind einfach direkt aus der Software möglich
- Datenprozesse inner- und außerhalb des eigenen Netzwerks können jeweils maximal verschlüsselt werden und durch verschiedene Einstellungen & Maßnahmen zusätzlich abgesichert werden
- In der inSuite können Sie **individuelle Benutzerrollen** und -rechte an jeden angelegten Nutzer(-kontos) vergeben, um sicherzustellen, wer was machen darf und welche Daten sehen und/oder verarbeiten darf
- Über den **Audit-log** sehen Sie stets, wer wann was gemacht hat, wer sich wann wo angemeldet hat und wer wann was für wen freigegeben hat
- Jeder User hat ein eigenes Passwort, da jedem User eine bestimmte Rolle und bestimmte Rechte zugeordnet sind
- Freigegebene Akteneinträge sind automatisch unveränderbar (**Schutz vor einem Regress**)

Datenschutzgrundverordnung (DSGVO) in der inSuite

Mit der folgenden Auswahl an funktionalen Aspekten stellen Sie als inSuite- Kunde einen sicheren, maßgeschneiderten Datenschutz her (2/3)

- Ein forcierter **Freigabemodus** bewirkt, dass Drucken von Rezepten, Formularen etc. nur bei vorheriger Freigabe durch einen bestimmten Nutzer (dem Arzt) möglich ist

- Ein **„strikter Modus“** hilft größeren, breiter aufgestellten Einheiten, dass nur jene Benutzer Zugriff auf Akteneinträge, die Betriebsstätten zugeordnet sind, haben, in den auch der Benutzer zugeordnet ist

- Über leistungsstarke, frei konfigurierbare **Reportingmechanismen** (die Benutzerrechte berücksichtigen) ist es möglich, dass nur Nutzer in Betriebsstätte A auch Reports bezogene auf die Daten von Betriebsstätte A sehen

- Der grundlegende Zugang zur inSuite auch von Außen (**mobil** bei Hausbesuchen) kann nutzerbasiert eingeschränkt werden (dazu kann eine **Multifaktor-Authentifizierung** aktiviert werden, vergleichbar)

- Beim Thema **E-Mails an Patienten schicken** können Sie mit der inSuite bei Speicherung der E-Mail-Adresse automatisch den Versand mit der Aufforderung zum **opt-in** durchführen, das System speichert diese patientenseitige Verifizierung

- **Sie schalten** Patienten für Dienste im Gesundheitsportal selbst frei

- Sie können **explizit** Ihren Patienten **erlauben** bzw. technisch unmöglich machen, Termine zu buchen

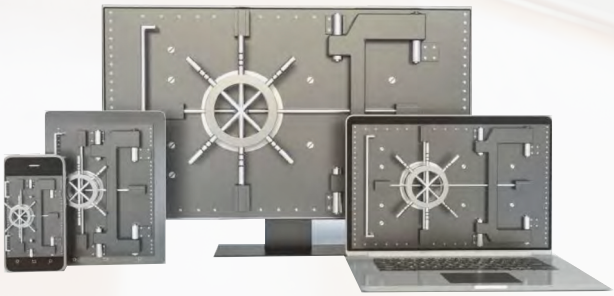
Datenschutzgrundverordnung (DSGVO) in der inSuite

Mit der folgenden Auswahl an funktionalen Aspekten stellen Sie als inSuite- Kunde einen sicheren, maßgeschneiderten Datenschutz her (3/3)

- Bei Gefahren für seine Daten (z.B. sein Smartphone ist von Schadsoftware befallen) können Sie die **Nutzerfreigabe zurücksetzen**, sodass der Patient den Sicherheitsprozess erneut durchführen muss

- Telemedizinische Vorgänge sind über den modernen **Standard WebRTC** abgesichert, alle Videounterhaltungen und sonstigen Datentransfers sind Ende-zu-Ende verschlüsselt (auch hier können auf Nutzer- und Betriebsstättenebene verschiedene Rechte eingeräumt werden)

- Alle Integrationsmöglichkeiten (Labor/LDT, Geräte/GDT, Abrechnung/KVDT/KV- Connect/PadNEXT/PVS-Net, Klinik/HL7, PACS/DICOM, REST/moderne Kopplung mit Drittsystemen, Apps und Solutions) sind im Rahmen aller genannten Sicherheitsmaßnahmen entsprechend mit gesichert bzw. letztere erfordert eine sog. Access Token (eine Art **Sicherheitsschlüssel**)



Grundlegende Fakten zu den Kernkomponenten der inSuite (1/3)

Sicherheitsrelevante Zertifizierungen

- IS0 2008/9001 (Qualitätsmanagement)
- ISO 27001 (IT-Sicherheit),
- KBV-zertifiziert (alle aktuellen Zertifikate finden Sie unter https://www.doc-cirrus.com/ueber-doc-cirrus/auszeichnungen)

ZERTIFIKAT

Hiermit wird bescheinigt, dass

DocCirrus

Doc Cirrus GmbH
Sonnenstraße 62
12133 Berlin
Deutschland

ein Informationssicherheits-Managementsystem
eingeführt hat und anwendet.

Geltungsbereich:
Entwicklung und Betrieb innovativer und sicherer eHealth-Dienste für die Gesundheitsbereiche

Erklärung zur Anwendbarkeit „Statement of Applicability" Version 73 vom 26.05.2019

Durch ein Audit, dokumentiert in einem Bericht, wurde der Nachweis erbracht, dass das Managementsystem die Forderungen des folgenden Regelwerks erfüllt

ISO / IEC 27001 : 2013

Zertifikat-Registrier-Nr. 5050443 ISMS13
Gültig ab 2019-08-17
Gültig bis 2022-08-16
Zertifizierungsdatum 2019-08-17

IAF
DAKKS

DQS GmbH

Markus Becker
Head of Division

Hauptsitz: DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main
Administration Berlin: DQS GT GmbH, Gustav-Heinemann-Ufer 74, 50968 Köln

Produkttechnische Grundprinzipien

- Security-by-design & Security-by-default
- Ease-of-use
- Web first
- Open interfaces/Offene Schnittstellen Standard compliance

Grundlegende Fakten zu den Kernkomponenten der inSuite (2/3)

Kernkomponente I:
Der Doc Cirrus Datensafe (Private Cloud)

- Datensafe arbeitet mit **verschlüsseltem** Filesystem und auch die Backups sind verschlüsselt; Zugriff hat nur, wer über einen der beiden mitgelieferten Schlüssel **(USB-Keys)** und Backup Key verfügt; diesen USB-Schlüssel also nur beim Startvorgang am Datensafe einstecken, danach abziehen und an sicherem Ort verbringen
- Zwei bis vier Festplatten im **RAID-Verbund** mit Benachrichtigung bei Ausfall einer Platte
- **Backup** mittels externer Festplatte, Netzwerk-Share oder als Online-Dienst (inBackup), direkt aus der inSuite steuerbar
- Optional **Replikation**: weiterer Datensafe an zweitem Standort wird automatisch synchronisiert und dient als Ersatzsystem bei Totalverlust des primären Datensafes (Desaster Recovery)
- Integrierter **Kommunikationsserver** mit Schnittstellen wie LDT, GDT, HL7, REST etc.
- Der Datensafe benötigt selbst keine externe **Netzwerkadresse** und sollte auch keine bekommen (siehe auch Informationen bzgl. Sicherheitshinweise für den Betrieb)
- **Integriertes 24/7 Remote Monitoring** aller Doc Cirrus Datensafes. Wir reagieren, wenn etwas nicht in Ordnung ist.

	Datensafe	Virtualisiert
Zustand Festplatten (Lesefehler etc.)	✔	⛔
Zustand Datenspiegelung (RAID) der Festplatten	✔	⛔
Prozessabbrüche durch Kernel (Speichermangel/Speicherfehler)	✔	✔
Auslastung Datenpartitionen	✔	✔
Auslastung CPU	✔	✔
Auslastung Arbeitsspeicher	✔	✔
Auslastung LOAD	✔	✔
Auslastung I/O	✔	✔
Auslastung Netzwerkkommunikation	✔	✔
Fehler bei autom. Backup Archivprüfungen	✔	⛔
Mailversand via internem Mailserver	✔	✔
Gültigkeit Datensafe Zertifikate	✔	✔
SSH Dienst nicht aktiv	✔	✔
inSuite Dienst nicht aktiv	✔	✔
MongoDB Dienst nicht aktiv	✔	✔
Zustand Replikation (Delay, Status)	✔	✔
Verfügbare Firmware Updates (Dell)	✔	⛔
Zustand Netzteile (Dell)	✔	⛔
Backup (Initialisierung und Erstellung)	✔	⛔
Virusscanning (Samba Shares)	✔	✔

Grundlegende Fakten zu den Kernkomponenten der inSuite (3/3)

Kernkomponente II:
Das Doc Cirrus Rechenzentrum (Public Cloud)

- Rechenzentrum in Berlin, deutscher Anbieter, ebenfalls ISO 27001 zertifiziert
- Sealed Cloud Prinzip, d.h. zu keinem Zeitpunkt werden sensitive Patientendaten gespeichert, sondern ausschließlich Ende-to- Ende-verschlüsselt durchgeleitet
- Patienten-Portal eingebettet in die Website der Praxis für Online-Patienten-Dienste
- Zuweiser-/Partner-Portal analog

Kernkomponente III:
Client = Browser

- Die Anwendung der inSuite erfolgt nur über Firefox, Chrome & Co.
- Der User muss nach Updates nur den Browsercache leeren, kein sonstiger Update-Stress

Google Chrome*
(Neuste Version)

Mozilla Firefox*
(Neuste Version)

Apple Safari
(Neuste Version)

Microsoft Edge
(Neuste Version)

Grundlagen & Systemarchitektur der Doc Cirrus Technologie (1/2)

- **Hybrid Cloud, Sealed Cloud:** Daten werden ausschließlich lokal im Datensafe gespeichert, von hier kommt auch die Anwendung, also die "Software", bei lokalen Zugriffen (oder aus der Doc Cirrus Cloud bei Zugriffen von außerhalb der Praxis)
- **Webbasiertes System**, HTML5-fähiger Browser als Client
- **Responsives Design**, d.h. für alle Auflösungen und Endgeräte optimiert
- **Single-Page-App Aufbau** für „Desktop Feeling“ im User Interface
- Servertechnologie Node.js und NoSQL- Datenbank, **Betriebssystem Linux mit zusätzlicher Härtung**
- **Auto-Update-Funktion** ohne Benutzerinteraktion, d.h. das System wird automatisch aus der Doc Cirrus Cloud aktualisiert
- Gesamtsystem ist **plug & play** und hinsichtlich Datenschutz optimiert
- Standardzugriff erfolgt **via SSL**, d.h. inkl. Transportverschlüsselung
- Für Zugriffe von außerhalb der Praxis greift zusätzlich eine **Ende-zu-Ende-Inhaltsverschlüsselung auf Basis AES-256**
- Asynchrone Ende-zu-Ende-Verschlüsselung möglich

Grundlagen & Systemarchitektur der Doc Cirrus Technologie (2/2)

- Keine zentrale PKI, sondern **Peer-to-Peer Schlüsselaustausch mit Multifaktorbestätigung**
- Zusätzlich kann man als Praxisbetreiber Zugriffe von außen generell verbieten oder mit der bereits genannten **Multifaktor-Authentifizierung** belegen, um das Sicherheitsniveau noch weiter zu steigern
- Telemedizinische Funktionen (z.B. Telekonsile oder Video-Sprechstunden) basieren auf **verschlüsseltem Peer-to- Peer-Protokoll WebRTC**
- **Lokaler und globaler Signalisierungs- und Präsenzdienst** für Telefonate, Audio-Video- Konferenzen, Telekonsile und Online Sprechstunden – auch einrichtungsübergreifend
- Durch Anwender konfigurierbare intra- und intersektorale Netzwerke inkl. Aktentransfer mit **Ende-to-Ende-Verschlüsselung**
- **Übersichtlicher Audit Log**, das jegliche Veränderungen und Zugriffe im System sicher protokolliert
- **Freigabeprinzip**, d.h. Abrechnung, Ausdruck und Weitergabe von Dokumenten/Formularen an Dritte nur nach elektronischer Freigabe durch den/die verantwortlichen Arzt/Ärzte

Sicherheitshinweise & Rechtesystem für den inSuite-Betrieb

Sicherheitshinweise für den Betrieb

- Es wird der Betrieb des Datensafes hinter der Firewall des Internetrouters einer Praxis empfohlen
- Standardeinstellung wählen, d.h. keine zusätzlichen Portfreischaltungen o.ä.
- Für detaillierte Informationen zum Betrieb des Doc Cirrus Datensafes halten wir einen technische Broschüre für die Inbetriebnahme des Datensafes für unsere Kunden vor. Dort finden Sie alle Fakten zu den den Themen:

  - Zugriffssteuerung und VPN
  - Zugriff der inSuite via Internet
  - Firewall-Einstellungen
  - SSL und Nutzung der inSuite im Browser
  - Nutzung von WLAN im inSuite-Kontext

  Die Broschüre finden Sie hier:

  https://www.doc-cirrus.com/images/downloads/datensafe-kundenbroschuere.pdf

Administratorrechte

- Der Datensafe ist eine Appliance, d.h. auf Betriebssystemebene nicht zugänglich und erlaubt keine Installation von Drittsoftware
- Zugriff auf das System ist ausschließlich über die Benutzeroberfläche und die veröffentlichten Schnittstellen möglich
- Verschiedene Rechte, Rollen und Gruppen für Anwender verfügbar
- Sollte zu einem späteren Zeitpunkt ein Systemwechsel gewünscht sein, so stellt Doc Cirrus die Daten des Systems auf Wunsch in einem marktüblichen und maschinenlesbaren Exportformat für die Migration zum Pauschalpreis zur Verfügung

Sicherheit bei externem Zugriff

Die gesamte Struktur hat aufgrund der Architektur ein sehr hohes Sicherheitsniveau, wenn sie so betrieben wird, wie wir es empfehlen:

- Gute Passwortqualität jedes Users – wird im System mit „grün“ visualisiert
- 2-Faktor-Anmeldung aktivieren – erfordert bei jeder Anmeldung von außen eine mTAN, d.h. einen Einmalcode, den der Mitarbeiter als SMS bekommt und der dann zusätzlich zum Benutzernamen und Passwort für die externe Anmeldung erforderlich ist
- USB-Schlüssel wird nur beim Startvorgang am Datensafe eingesteckt und danach abgezogen und sicher verbracht
- Auf den Endgeräten jeweils die aktuellsten Browser verwenden
- Firewall im Praxisnetzwerk sollte bis auf die benötigten Ports abgeriegelt sein, insbesondere für Zugriffe von außen nach innen

Für den selektiven Zugang einzelner Mitarbeiter von außen gibt es zwei Optionen:

- Bei aktivierter 2-Faktor-Anmeldung: Aktivierung des Remote Login nur mit Einmalpasswort (sTAN), Handynummern nur bei den Usern hinterlegen, die Remote Login auch nutzen dürfen
- Parallel Nutzung der Gruppenberechtigungen

Sicherheit bei Backups

1) Automatischer Backup-Dienst auf dem Doc Cirrus RZ – kostenpflichtige Erweiterung

2) Manuelles Backup über externe Festplatte(n) gemäß folgender Policy (Empfehlung):

- Man sollte mindestens zwei, besser mehrere Festplatten für das Backup verwenden. Jede Platte muss einmalig initialisiert werden und sollte mit einem Aufkleber gekennzeichnet werden (z.B. mit 1, 2, 3). Man steckt eine der Platten an und lässt sie über Nacht am Datensafe. Gegen 21 Uhr wird das Backup automatisch auf die Platte übertragen. Morgens dann Platte abziehen und die nächste Platte anstecken. Die abgezogene Platte mitnehmen und an einem anderen Ort aufbewahren - usw. Hat man einen Plattenwechsel doch einmal vergessen, so ist dies kein Problem – die Sicherung kommt damit problemlos klar.

- Auch die Platten sind im Falle eines Diebstahls insofern geschützt als ein Dieb mit ihr nichts anfangen könnte, wenn er nicht gleichzeitig auch den entsprechenden Backup Key hat – analog zum silbernen USB-Key, der die gleiche Funktion für die Platten im Datensafe übernimmt

- Auch wenn der automatische Backup-Dienst (s.o.) später im Einsatz ist, macht es Sinn zumindest eine Backup- Festplatte dauerhaft am Datensafe zu belassen. Dann besteht nämlich die Möglichkeit der Rücksicherung, wenn der Standort längere Zeit ohne Internet sein sollte – weil die Rücksicherung aus dem Doc Cirrus RZ ja eine Internetverbindung erfordert.

Backup Keys für Entschlüsselung der verschlüsselten Backup-Datei an einem sicheren Ort verwahren

Alternativ zur externen Festplatte kann als Zielmedium auch ein Netzwerk-Share eingerichtet werden. Für die Sicherung dieses Mediums ist natürlich dann wiederum eine eigene Policy wie die oben dargestellte notwendig

inSuite-Vorteile auf einen Blick

Hochsichere Online-Patientenservices, wie Termine und Sprechstunden verschlüsselt auf Ihrer modernen Website

Wartungsfreies System mit Top-Datenschutz: Automatische Updates & Softwarepflege, Monitoring, Backups & Ende-zu-Ende-Verschlüsselung

Geräte-Wahlfreiheit: Nutzen Sie die inSuite unabhängig vom Ort (Praxis, Hausbesuch) sowie parallel & sicher auf Mac, Tablet, PC & mobil auf Smartphone (iOS, Android)

Automatische, vollständige, nutzerbasierte & **revisionssichere Dokumentation** (mit 1-Click-Doku, Cave, eigene Workflows & Regeln uvm.)

Zeit- & kostensparende Abrechnung (GKV, ASV, PKV etc.) auch mit ASV und diversen Spezialverträgen

Standortübergreifende & **intersektorale Zusammenarbeit im Team** (individuell konfigurierbar dank einfachem Rollen- & Rechtemanagement)

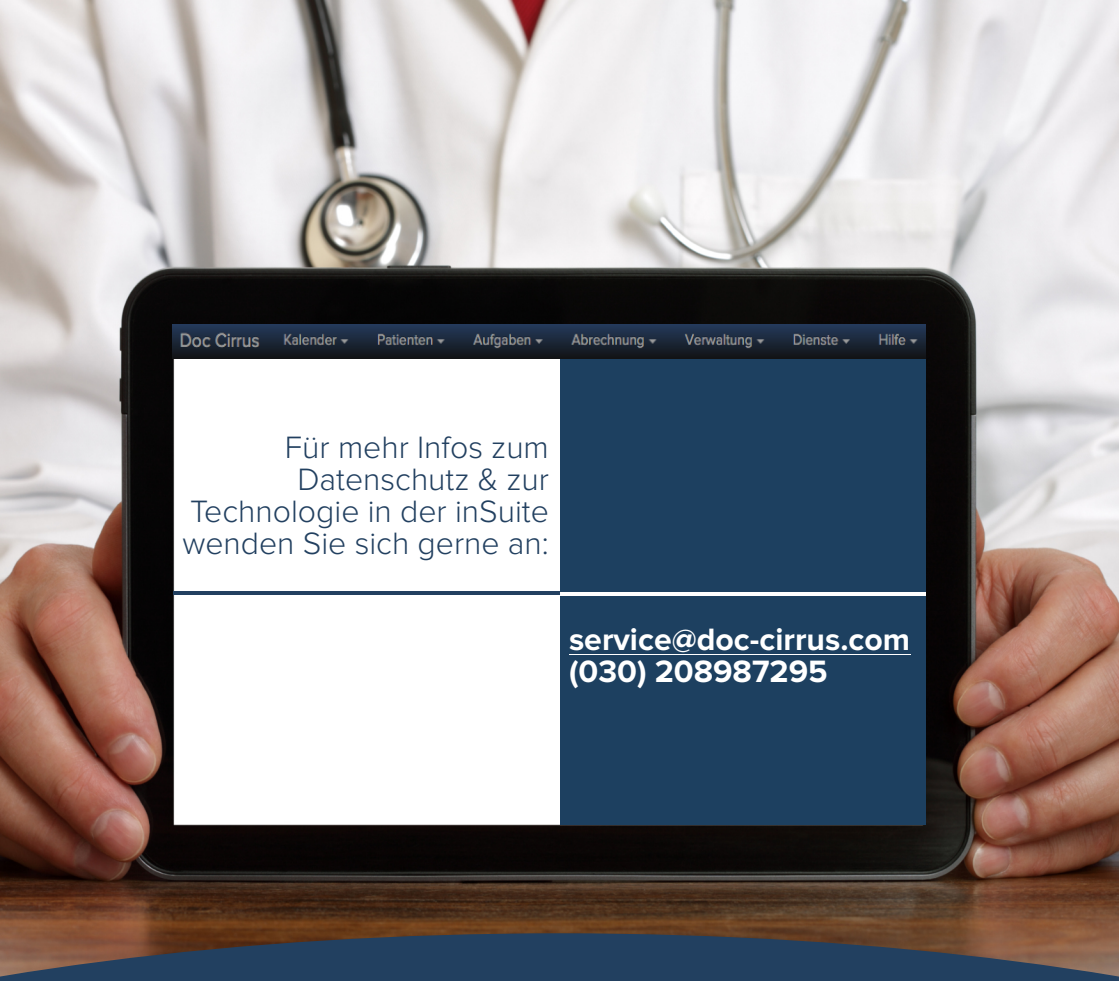
Daten aus Apps, Fitnesstrackern & Medizingeräten direkt in die ärztliche Akte (z.B. EKG, Herzschrittmacher, Patientenapps etc.)

Integrierte Telemedizin (Videosprechstunde, Telekonsile, Tumorkonferenzen, Partnernetzwerk) optimal vorbereitet auf das E-Health-Gesetz

inSuite

Ein KBV-zertifiziertes Komplettsystem (AIS/PVS) für alle medizinischen Leistungserbringer

Webbasiertes & topmodernes Arzt- & Praxissystem | ISO-zertifizierter, modernster Datenschutz mit 360°-IT-Sicherheits- & Bedienkonzept | Für Praxen, Fachärzte, Therapeuten, MVZs & Netzwerke | Intelligentes Hard- & Softwaresystem | Alle Arbeitsplätze & alle nichtärztlichen Nutzer immer inkl. | Faire Monatsgebühr pro Arzt



(030) 208987295
(030) 208987299 (Fax)

www.doc-cirrus.com

Doc Cirrus GmbH
Pohlstraße 20
10785 Berlin