

Technische Beschreibung Jalomed®

Erläuterung zu Grundlagen und Funktion des Jalomed-Systems (allgemein):

Jalomed hilft die gesetzlich verankerten gesundheitsdatenspezifische Vorgaben aus den § 630f BGB (Patientengesetz) und § 199 BGB, sowie Leitlinien, Expertenstandards, IV-Vertragsvorgaben, Registerteilnahmen einzuhalten und den Auftraggeber z.B. vor einem Löschen von Daten innerhalb der gesetzlich verankerten Aufbewahrungsfrist zu schützen. Im Falle von Regressen durch Kostenträger hilft eine korrekt geführte Dokumentation diese mittels „Outcome Management ist der dokumentierte Nachweis der therapeutischen und wirtschaftlichen Wirksamkeit einer eingesetzten Therapie“ zu widerlegen.

Funktion:

- Die Software ist ein offline-fähiger Client und kann als Einzelplatzversion oder in einer Vernetzung betrieben werden.
- Dateneingabe und -ausgabe geschieht nur über die Jalomed-Client-Software.
- Zugang zur Client-Software über userspezifische DSGVO-konforme Zugangsdaten.
- Eingegebene Daten werden in der Client-Software verschlüsselt abgelegt. Sollte ein vernetztes Arbeiten gewünscht sein, werden bei bestehender Online-Verbindung neu hinzugekommene Daten mit der Jalomed-Zentralen Datenbank (verschlüsselte Verbindung) synchronisiert. Diese Jalomed-Zentrale Datenbank dient als Kommunikationsplattform.

Aufbau der Datenstruktur:

Das Jalomed-System speichert die Daten von Patienten-/Bewohnern in jeweils einer eigenen Patientendatenbank. Diese patienteneigene-Datenbank kann auch dem Patienten übergeben werden und der Patient könnte mit einer Jalomed-Client-Software seine Daten einsehen.

Datenstruktur Betriebssystem:

Von einem Patienten können beliebig viele Dateninstanzen erzeugt werden, die parallel und gleichzeitig auf Windows-Betriebssystemen (ab Win2000) in JalomedFlex® offline bearbeitet werden können. Mit Bereitstellung eines Remote-Desktop kann auch auf Tablet/PC mit den Betriebssystemen Android, Mac OSX, (IOS) gearbeitet werden. Die Daten in einer Dateninstanz können in einzelne Organisationseinheiten gegliedert werden, um sie mit unterschiedlichen Berechtigungen abzusichern.

Die Dateninstanz eines Patienten kann auch zur sicheren Kommunikation zwischen Patient und Einrichtung (Praxis, Krankenhaus, Wundzentrum) eingesetzt werden.

Sicherheit:

Alle Dateninstanzen sind intern verschlüsselt und werden über eine SSH-Verbindung zusätzlich verschlüsselt übertragen. Es besteht sowohl eine Ende-zu-Ende Verschlüsselung als auch eine Übertragungsverschlüsselung.

Datenausgabe und Berichte:

Analog zu den Dokumentationsinhalten werden die Berichtsinhalte gegliedert und zusammengestellt.