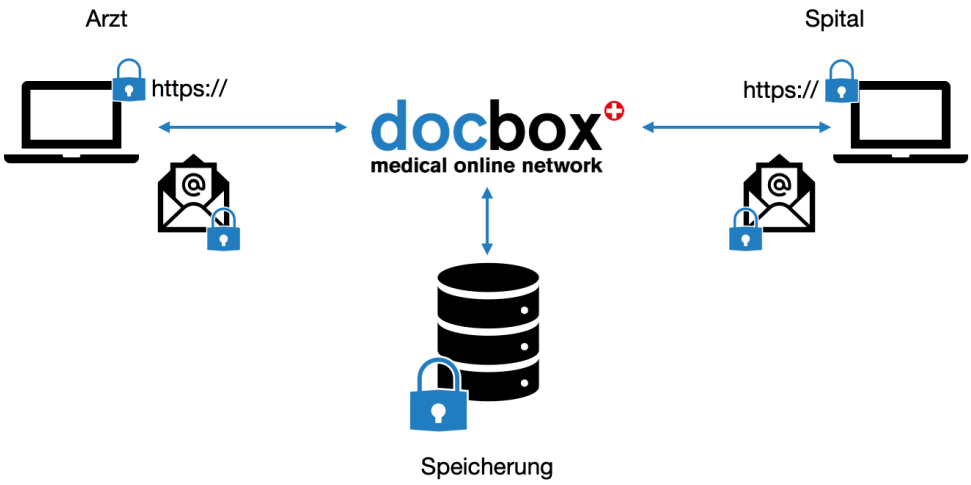
Datensicherheit in der gerichteten Kommunikation

Die Digitalisierung im Schweizer Gesundheitswesen nutzt sowohl den Akteuren als auch dem Patienten, macht die Datensicherheit jedoch zu einem erfolgskritischen Faktor. Das Whitepaper Datenschutz und Sicherheit in der gerichteten Kommunikation zeigt, wie der Transfer von sensiblen Daten über docbox sicher funktioniert.

Zum Schutz der Daten auf docbox werden alle erforderlichen technischen und organisatorischen Massnahmen getroffen.



Organisatorische Massnahmen

- Verträge und AGB (kundenseitig) sowie akzeptierte Lizenzbestimmungen und Datenschutzerklärungen (benutzerseitig) halten Rechte & Pflichten bezüglich Datensicherheit und Datenschutz fest.
- Alle Mitarbeitenden der Visionary AG unterzeichnen eine Datenschutz- und Sicherheitserklärung, in der sie über Rechte und Pflichten aufgeklärt werden. Die Mitarbeitenden werden regelmässig über die Datenschutz- und Sicherheitsbestimmungen informiert und darauf sensibilisiert.

Sicherheit bei der Datenübermittlung

- Die Datenübermittlung erfolgt https-verschlüsselt mit SSL UCC Zertifikaten.
- Bei der Kommunikation zwischen den Systemen (z.B. zwischen Praxis Software und docbox oder zwischen Klinik Software und docbox) kommt zusätzlich ein Client Zertifikat zum Einsatz.
- Username & Passwort authentisieren und autorisieren den Benutzer.
- Patientendatenzugang ausschliesslich nach 2-Faktor-Authetifizierung (aktuell mittels HIN-SSO, Client Zertifikat oder mTAN möglich). Ohne Zusatzfaktor ist ausschliesslich anonymisierter Zugang möglich.
- Der E-Mail Versand mit Patientendaten ausschliesslich an HIN-geschützte E-Mail-Adressen. Ungeschützte E-Mailadressen erhalten ausschliesslich anonymisierte Notifikationen.

Sicherheit bei der Datenspeicherung

- Patientendaten werden auf den docbox Servern verschlüsselt gespeichert.
- Patientendaten werden lediglich zwischengespeichert. Sie werden ein Tag nach Abholung bzw. ein Monat bei Nichtabholung aus docbox automatisch gelöscht
- Technisch ist eine Entschlüsselung der Daten nur durch die Visionary AG Software Entwickler möglich. Alle Mitarbeitenden der Visionary AG haben eine Datenschutzerklärung unterschrieben, welche die Entschlüsselung dieser Daten ohne Bewilligung verbietet und die Nutzung der Daten in docbox regelt.
- Logfiles protokollieren die Datenströme (Transaktionsdaten): welcher Nutzer hat welche Daten über die Schnittstelle „eingestellt“ und „abgerufen“ und wann wurden Daten „gelöscht“. Das Log wird nicht gelöscht. Eine unvorhergesehene Nutzung (gem. VDSG Art. 10 Abs. 1) der Patientendaten ist mit den Daten im Log nicht möglich.

Systemüberwachung

- Überwachung, Unterhalt und Betrieb von Hardware, OS, Webserver sowie den Datenbankserver durch EveryWare AG
- 24 x 7 Reaktions- und Interventionszeit 2 Std. während der Bürozeit / 4 Std. ausserhalb

Systemarchitektur

- Ausfallsicherheit durch Redundanz gewährleistet, mittels load balancing bei den Applikationsservern und Master/Slave-Konfiguration bei den Datenbankservern
- Separate Test- und Produktivsysteme verfügbar

Hosting

- Hosting nach Schweizer Gesetzgebung, aktuell bei EveryWare AG, Zürich.
- SLA Verfügbarkeit von 99.7% über 6 Monate.

Datacenter Sicherheit

- Kontrolle über die docbox Anwendungen und Daten ist vollständig bei Visionary AG.
- Datacenter erfüllt höchste Ansprüche bezüglich Zugangssicherheit, Einbruchsicherheit, Stromversorgung, Klimatisierung, Brandalarmierung, Videoüberwachung und Internetanbindung
- Hochsicherheitszugangsschleusen
- Zwei physisch getrennte Internetanbindungen
- Leistungsfähiges und flexibles, internes Netzwerk mit mehreren Security-Zonen, auf welchem Datastorage- und Backup-Dienste betrieben werden.
- Tägliches Backup der Daten mit Aufbewahrung von 5 Tagesgenerationen und 4 Wochengenerationen.
- Rechenzentrum erfüllt die Richtlinien der FINMA für Bankenoutsourcing