

WDoku aus Sicht der Klinik-IT

Für: IT-Leitung, Systemadministration, Informationssicherheitsbeauftragte

Betriebsvarianten, Authentifizierung, Verschlüsselung, Protokollierung und Schnittstellen, dazu die Punkte, die wir selbst noch als offen führen.

Das Wichtigste in Kürze

WDoku läuft entweder in unserer Cloud mit Serverstandort in Deutschland oder auf einem Server in Ihrem Haus. Ohne KIS-Anbindung werden keine Patientendaten gespeichert oder verarbeitet. Bei eigenem Betrieb liefern wir eine virtuelle Appliance mit verschlüsselter Festplatte, die ausschließlich über Ihr VPN administriert wird. Eingehende Verbindungen aus dem Internet in Ihr Kliniknetz braucht WDoku nicht.

Die beiden Betriebsvarianten

Welche Variante Ihr Haus wählt, bestimmt den weiteren Prüfungsgang. Die Unterschiede betreffen den Speicherort, die Rechtsgrundlage der Einsicht und die Frage, wer welche Daten sehen kann.

	WDoku Cloud (App)	Eigener Server (Appliance)
Wo liegen die Daten	Rechenzentrum in Deutschland	In Ihrem Haus
Patientendaten im System	Werden nicht gespeichert oder verarbeitet	Nur bei optionaler KIS-Anbindung, verlassen das Haus nicht
Leistungs-KIS-ID und ICD-Codes	Nur bei optionaler KIS-Anbindung	Nur bei optionaler KIS-Anbindung
Rechtsgrundlage der Einsicht	Einwilligung des Arztes (Art. 6 Abs. 1 lit. a)	Weiterbildungsverhältnis (Art. 6 Abs. 1 lit. b/f)
Handhabe des Arztes	Widerruf, wirkt sofort	Widerspruch nach Art. 21, wirkt sofort
Uhrzeiten für Befugte	Nur mit eigener Einwilligung	Nur mit eigener Einwilligung
Verantwortlicher nach DSGVO	WDoku für das Nutzerkonto, die Klinik für gelieferte Daten	Die Klinik

Wie die Daten fließen

Für die Bewertung zählt weniger, wo die Software läuft, als welche Daten verarbeitet werden und wer sie lesen kann.

WDoku Cloud

Rechenzentrum in Deutschland, Betrieb durch uns.

- Die Ärztin oder der Arzt erfasst die Leistung in App oder Browser.
- Der Eintrag geht über TLS in die Cloud, verschlüsselt gespeichert.
- Weiterbildungsbefugte lesen nur, was für ihre Abteilung freigegeben ist.
- Ohne KIS-Anbindung keine Patientendaten und keine Gesundheitsdaten: verarbeitet werden OPS-Codes, Zeitstempel und Saalbezeichnungen.
- Mit der optionalen KIS-Anbindung liefert Ihr Haus zusätzlich die Leistungs-KIS-ID und die ICD-Codes des Eingriffs. Name, Geburtsdatum und Adresse überträgt WDoku Connect nicht.
- Die Leistungs-KIS-ID erreicht die WDoku-Cloud nur als Hash, gebildet mit einem Schlüssel, der Ihr Haus nie verlässt.
- Der Weg zur Ärztekammer bleibt der Export durch den Arzt selbst.

Eigener Server (Appliance)

Virtuelle Maschine in Ihrem Netz, Wartung über Ihr VPN.

- App und Browser der Ärztinnen und Ärzte sprechen mit der Appliance in Ihrem Haus.
- Das KIS liefert optional Leistungsdaten per JSON oder CSV an dieselbe Appliance: die Leistungs-KIS-ID und die ICD-Codes des Eingriffs, wie in der Cloud-Variante.
- Weiterbildungsbefugte lesen auf Grundlage des Weiterbildungsverhältnisses; ein Widerspruch des Arztes wirkt sofort.
- Patientenbezogene Felder bleiben im Haus und verlassen Ihr Netz nicht, die Leistungs-KIS-ID und die ICD-Codes eingeschlossen.
- Die Leistungs-KIS-ID bleibt hier im Klartext: sie verlässt Ihr Netz nicht, und für den Abgleich mit Ihrem KIS muss sie lesbar sein. Gehasht wird nur, was in die Cloud geht.
- Wir erreichen das System nur über Ihr VPN, nicht aus dem öffentlichen Netz.
- Die Sicherung liegt bei Ihnen, verschlüsselt mit Ihrem eigenen Schlüssel.
- Der Weg zur Ärztekammer bleibt auch hier der Export durch den Arzt selbst.

WDoku erhebt selbst keine Patientendaten. Mit der optionalen KIS-Anbindung liefert Ihr Haus die Leistungs-KIS-ID, Zeitstempel, Saal, die beteiligten Ärztinnen und Ärzte und die OPS-/ICD-Codes des Eingriffs. Name, Geburtsdatum und Adresse überträgt WDoku Connect nicht. Die Leistungs-KIS-ID erreicht die WDoku-Cloud nur als Hash, gebildet mit einem Schlüssel, der Ihr Haus nie verlässt. Einen Klartextwert weist die Cloud ab. Ohne diesen Schlüssel können auch wir die Zuordnung zu einer Person nicht herstellen. Anonym sind die Daten damit nicht: Ihr Haus hält den Schlüssel, bleibt Verantwortliche, und die Kategorie im Auftragsverarbeitungsvertrag entfällt dadurch nicht.

Was Sie bereitstellen müssen

- Cloud: nichts. Die Ärztinnen und Ärzte nutzen App oder Browser, eine KIS-Anbindung ist optional.
- Eigener Server: eine virtuelle Maschine für die Appliance (Auslieferung als OVA), ein DNS-Eintrag und ein VPN-Zugang für unsere Wartung. Die Festplatte ist mit LUKS verschlüsselt, für den Notfall existiert ein dokumentiertes Break-Glass-Verfahren.
- TLS-Zertifikat: die Appliance wird mit einem selbstsignierten Zertifikat ausgeliefert, das ist der Provisionierungs-Standard. Ihre IT kann im Admin-Web ein eigenes, CA-signiertes Zertifikat hinterlegen. Für die Nutzung mit der Mobile-App ist ein öffentlich vertrauenswürdigen Zertifikat nötig, weil iOS im WebView kein selbstsigniertes akzeptiert.
- Erreichbarkeit: Klinik-VMs sind ausschließlich über VPN erreichbar, nicht aus dem öffentlichen Netz.

Die Appliance im Detail

Für den Betrieb im eigenen Haus liefert die Appliance ihr Sicherheitskonzept mit. Die folgenden Eigenschaften sind Bestandteil der Auslieferung, keine Zusatzoptionen.

- Firewall mit Default-Deny in beide Richtungen: eingehend sind nur die Anwendung, das Admin-Web und SSH aus dem Klinik-Netz erreichbar. Ausgehend ist eine kurze Allowlist von WDoku-Zielen sowie DNS und NTP erlaubt, alles andere wird verworfen.
- Verwaltung ohne Root-Alltag: ein Admin-Web auf einem eigenen Port, nur aus Ihrem Klinik-Netz erreichbar, dazu ein Admin-CLI in der Hypervisor-Konsole für Erstinstallation und Diagnose. Beide arbeiten mit klar begrenzten Rollen.
- Jede Verwaltungsaktion landet in einem Protokoll, das auf Betriebssystem-Ebene nur angehängt werden kann. Nachträgliches Ändern oder Löschen einzelner Einträge ist damit ausgeschlossen.
- Updates sind fail-closed: die Appliance prüft die Signatur gegen einen bei der Einrichtung verankerten

Schlüssel und lehnt alles ab, was nicht passt. Downgrades auf ältere Stände werden verweigert, ein fehlgeschlagenes Update kehrt automatisch zum vorherigen Stand zurück.

- Private Schlüssel bleiben im Haus: das TLS-Zertifikat entsteht über ein CSR-Verfahren. Die Appliance erzeugt den Schlüssel lokal, wir signieren nur; der private Schlüssel verlässt Ihr Haus zu keinem Zeitpunkt.
- Einmalige Geheimnisse je Installation: Schlüssel und Passwörter werden pro Appliance erzeugt. Ein kompromittiertes System gefährdet keine andere Installation.

Die vollständige Beschreibung von Betrieb, Administration und Update-Verfahren steht im Bereich Klinik-IT und Betrieb.

Authentifizierung und Sitzungen

- Passwörter werden mit bcrypt gehasht (Kostenfaktor 12). Altbestände aus SHA1 werden beim Login transparent migriert.
- Die Passworrichtlinie verlangt mindestens acht Zeichen mit Groß- und Kleinbuchstaben sowie Ziffer oder Sonderzeichen und prüft gegen bekannte Datenlecks.
- Die App arbeitet mit JWT: Zugriffstoken 15 Minuten, Refresh-Token 60 Tage mit Rotation bei jeder Erneuerung, maximal drei Geräte je Konto.
- Wird ein bereits widerrufenes Token wiederverwendet, widerruft das System alle Token dieses Kontos und schreibt ein Sicherheitsereignis.
- Im Browser meldet ein Inaktivitäts-Logout nach 15 Minuten ab, mit Countdown ab Minute 10. Das ist für geteilte Stations-PCs gedacht.
- Nach zehn Fehlversuchen sperrt das Konto für 15 Minuten. Zusätzlich greifen Rate-Limits je IP-Adresse, je E-Mail-Adresse und je Netzsegment.
- Die Löschung des eigenen Kontos verlangt eine erneute Passworteingabe.
- Administratoren können Konten sperren. Eine Sperre wirkt sofort bei jedem Request, auch mit noch gültigem Token, widerruft alle Refresh-Token und wird protokolliert.

Verschlüsselung

- Transport: TLS 1.3 erzwungen, HSTS mit Preload.
- Speicherung auf dem Server: AES-256 im Ruhezustand.
- Auf dem Endgerät: die lokale Datenbank der App ist mit SQLCipher verschlüsselt. Der Server bleibt die führende Quelle.
- Die Store-Builds für iOS und Android verbieten unverschlüsselten Verkehr auf Plattformebene (App Transport Security bzw. Network Security Config).
- Betriebsgeheimnisse liegen in einem zentralen Secrets-Management, nicht als Klartext auf den Maschinen. Die Rotation des Signaturschlüssels ist dokumentiert und erprobt.

Rollen, Rechte und Zugriffsprüfung

Es gibt vier Stufen: Arzt (erfasst eigene Leistungen), Weiterbildungsbefugter (zusätzlich Einsicht in freigegebene Stände), Administrator (Benutzer, Gruppen, Kataloge, Importe) und Superadministrator (globale Einstellungen).

Sichtbarkeiten werden immer serverseitig aus den Rollen des angemeldeten Nutzers abgeleitet, nie aus einem Parameter, den der Client mitschickt. Das schließt die Klasse von Fehlern aus, bei der ein manipulierter Request fremde Datensätze liefert.

Einsicht in fremde Daten setzt zusätzlich ein Freigabe-Gate voraus und prüft unabhängig davon die aktive

Protokollierung

- Ein Audit-Protokoll in der Datenbank erfasst rund 35 Ereignisarten: Sicherheitsereignisse, Betroffenenrechte, Rollenlebenszyklus, administrative Aktionen, Installations- und Katalogvorgänge. Aufbewahrung 24 Monate, einsehbar über eine Administrationsansicht mit Filtern.
- Zugriffe von Weiterbildungsbefugten auf fremde Daten werden als eigene Kategorie protokolliert. Die betroffene Ärztin oder der betroffene Arzt sieht diese Zugriffe selbst in der App.
- Erteilung, Widerruf und Widerspruch von Freigaben werden ebenfalls protokolliert.
- Die Änderungshistorie geteilter Leistungen ist technisch schreibgeschützt: Einträge lassen sich nach dem Anlegen weder ändern noch löschen.
- Passwörter, Token, Codes und Sprachaufnahmen erscheinen in Server-Protokollen als [FILTERED]. Ein Regressionstest hält das fest.
- Server-Protokolle werden nach 90 Tagen automatisch gelöscht.

Updates und Lieferkette

- Container-Images sind signiert (cosign) und kommen aus unserer eigenen Registry mit Konten nach dem Least-Privilege-Prinzip.
- Abhängigkeiten werden automatisiert auf bekannte Schwachstellen geprüft. Wie ein Update abläuft, steht unter Updates und Sicherheit.
- Sicherheits- und Datenschutzabschnitte sind fester Bestandteil jeder Funktionsspezifikation, nicht ein nachgelagerter Schritt.
- Interne Sicherheitsreviews laufen mit nachverfolgbaren Befund-Nummern; die Befunde werden als Anforderungen umgesetzt und im Code referenziert.

Datensicherung

Datenbanksicherungen laufen nach einem Generationenschema: alle Stände bis 60 Tage, danach Wochenstände. Nach zwölf Monaten werden Sicherungen endgültig gelöscht. Damit ist eine Konto-Anonymisierung nach spätestens zwölf Monaten auch aus allen Sicherungen verschwunden.

Die Sicherungen werden asymmetrisch verschlüsselt. Hinterlegt Ihre Klinik einen eigenen öffentlichen Schlüssel, kann nur noch Ihr Haus diese Sicherungen entschlüsseln, wir dann nicht mehr. Das ist so gewollt.

Schnittstelle zum KIS

Es gibt zwei Wege, und beide kommen ohne proprietäre Treiber aus: eine JSON-Schnittstelle mit einem Token, das Ihrer Klinik gehört, oder CSV-Dateien.

Wo Ihr KIS keine passende Exportfunktion mitbringt, übernimmt WDoku Connect den lesenden Zugriff.

Die Übertragung ist Server zu Server, alle Schreibvorgänge sind auf den Teilbaum Ihrer Klinik begrenzt.

Was wir selbst als offen führen

Diese Punkte stehen in unserem internen Restrisiko-Register. Wir nennen sie hier, weil eine IT-Abteilung sie ohnehin erfragt und eine Liste ohne offene Punkte unglaublich ist.

- Der letzte externe Penetrationstest liegt bei der virtuellen Appliance und stammt aus 2022. Eine Wiederholung ist vorgesehen. Als aktueller Nachweis taugt er nicht.

Häufige Fragen

Brauchen wir eine eigene virtuelle Maschine?

Nur beim Betrieb im eigenen Haus. Die Cloud-Variante braucht auf Ihrer Seite keine Infrastruktur.

Muss WDoku von außen in unser Netz hinein?

Nein. Die Wartung der Klinik-Appliance läuft über Ihr VPN. Eingehende Verbindungen aus dem Internet in Ihr Netz sind nicht erforderlich.

Wer administriert das System im Alltag?

Benutzer, Rollen und ihre hauseigenen Kataloge verwaltet Ihr Haus selbst über eine Administrationsoberfläche. Die offiziellen Weiterbildungskataloge der Landesärztekammern hält WDoku automatisch aktuell. Betriebssystem- und Anwendungsupdates der Appliance übernehmen wir über den Wartungszugang.

Was passiert, wenn ein Update fehlschlägt?

Die Appliance kehrt automatisch zum vorherigen Stand zurück. Jedes Update ist signiert und wird vor der Installation geprüft; Downgrades auf ältere, möglicherweise verwundbare Stände lehnt das System ab.

Welche Verbindungen baut die Appliance nach außen auf?

Ausschließlich ausgehende, zu einer kurzen Allowlist von WDoku-Zielen sowie DNS und NTP. Die Firewall verwirft alles andere in beide Richtungen. Einen Fernzugriff durch uns gibt es nur über den VPN-Zugang, den Ihr Haus kontrolliert.

Kommen Patientendaten in die Cloud?

Name, Geburtsdatum und Adresse überträgt WDoku Connect nicht, in keiner Betriebsart. Ohne KIS-Anbindung verarbeitet WDoku darüber hinaus keine Gesundheitsdaten: erfasst werden OPS-Codes, Zeitstempel und Saalbezeichnungen. Mit der optionalen Anbindung liefert Ihr Haus zusätzlich die Leistungs-KIS-ID und die ICD-Codes des Eingriffs. Die Leistungs-KIS-ID erreicht die WDoku-Cloud nur als Hash, gebildet mit einem Schlüssel, der Ihr Haus nie verlässt. Einen Klartextwert weist die Cloud ab. Ohne diesen Schlüssel können auch wir die Zuordnung zu einer Person nicht herstellen. Anonym sind die Daten damit nicht: Ihr Haus hält den Schlüssel, bleibt Verantwortliche, und die Kategorie im Auftragsverarbeitungsvertrag entfällt dadurch nicht.

Was passiert bei einem Ausfall?

Ein externes Monitoring prüft die Erreichbarkeit. Die Wiederherstellung aus einer Sicherung ist praktisch erprobt, das Vorgehen ist in einem Runbook beschrieben.

Diese Unterlage online, mit Verweisen auf die übrigen Rollen:
wdoku.de/homepage/einfuehrung/it-und-sicherheit

Diese Unterlage beschreibt den technischen und organisatorischen Stand von WDoku. Sie ist keine Rechtsberatung. Ob und wie Mitbestimmung, Datenschutz-Folgenabschätzung oder Vergaberecht im Einzelfall greifen, hängt vom konkreten Einsatz und von Ihrer Trägerschaft ab.

WDoku Marketing GmbH · Dr. Alfred-Neff-Str. 15 · 75015 Bretten · HRB 745718 Amtsgericht Mannheim · USt-IdNr. DE 357614122 · support@wdoku.de · wdoku.de