One DICOMServer

SICHERHEITS- UND DATENSCHUTZKONZEPT

Sicherheitskonzept

Technische und organisatorische Massnahmen zum Schutz von Patientendaten in One DICOMServer 2.0 – Grundlage für Datenschutz-Audit und Freigabe.

Produkt	One DICOMServer
Version	2.0.0
Dokumentstand	04.10.2026
Setup SHA-256	`ee060ebbb14db46cd889f8563e87c4c425959937a77ba648fb4ae151d2716b04`
Hersteller	One DICOMServer · www.dicomserver.ch · info@dicomserver.ch

Dieses Dokument beschreibt die Software One DICOMServer 2.0. Weitergabe an Auditoren, Datenschutzberater und IT-Betreuer der Praxis ist ausdrücklich gestattet.

Inhalt

1. Zweck und Geltungsbereich
2. Systemübersicht und Datenflüsse
3. Bearbeitete Daten und Schutzbedarf
4. Technische Massnahmen
5. Rollen und Berechtigungen
6. Protokollierung (Zugriffsprotokoll)
7. Verfügbarkeit und Wiederherstellung
8. Worksheet und KI-Assistenz
9. Sichere Entwicklung und Prüfung
10. Aufgaben der Praxis (Betreiber)
11. Restrisiken und Grenzen
12. Datenschutzrechtliche Einordnung
13. Anhang: Ports, Dateien, Härtungs-Checkliste

1. Zweck und Geltungsbereich

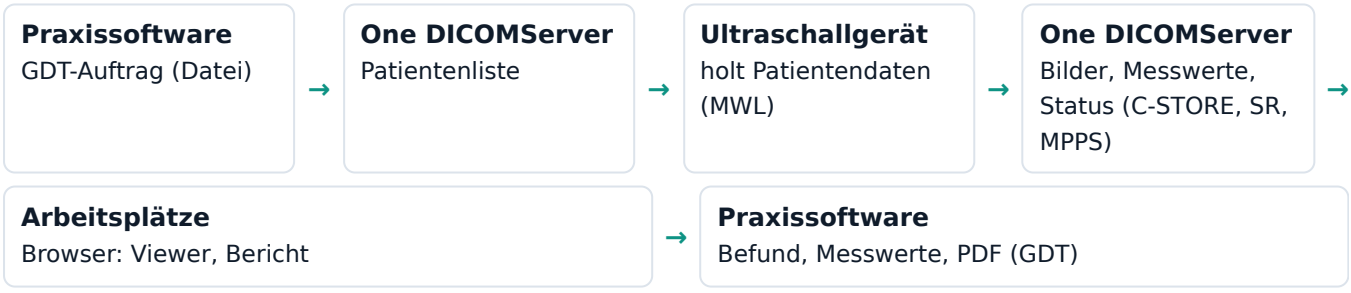
Dieses Dokument beschreibt die Massnahmen, mit denen One DICOMServer 2.0 Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der bearbeiteten Patientendaten schützt. Es richtet sich an Praxisinhaber, Datenschutzberater, IT-Betreuer und Auditoren und dient als Beilage zum Datenschutz- bzw. Informationssicherheitsdossier der Praxis.

Geltungsbereich: Software One DICOMServer (bis Version 1.x „HC-DICOMServer“) ab Version 2.0.0 (Windows-Dienst mit Webinterface), installiert auf einem Windows-10/11-PC im Netz einer Arztpraxis. Nicht Gegenstand sind die angeschlossenen Modalitäten, die Praxissoftware, das Netzwerk sowie das Betriebssystem selbst; für diese werden in Kapitel 10 Anforderungen an den Betreiber formuliert.

Zweckbestimmung: Empfang, Archivierung, Anzeige, Dokumentation und Weitergabe von DICOM-Bilddaten (Schwerpunkt Ultraschall), Bereitstellung der Patientenliste (Modality Worklist) für die Geräte, Erstellung von Befundberichten und Datenaustausch mit der Praxissoftware (GDT). Die primäre Diagnose erfolgt am Untersuchungsgerät bzw. auf einer dafür vorgesehenen Befundstation. Worksheet und die optionale KI-Assistenz (Kapitel 8) sind Hilfsmittel zur Dokumentation und Qualitätssicherung; sie stellen keine Diagnose.

2. Systemübersicht und Datenflüsse

One DICOMServer besteht aus einer einzigen ausführbaren Datei, die als Windows-Dienst (`OneDICOMServer`, Konto LocalSystem) läuft. Sie enthält DICOM-Server und -Client, Webserver, Datenbank, Planer (Backup, Export, Aufräumen), die GDT-Anbindung sowie das Worksheet und die KI-Assistenz mit eingebettetem Modell. Es gibt keine weiteren Server-Komponenten, keinen Datenbankserver und keine Cloud-Dienste.



Datenfluss	Protokoll / Weg	Schutz
Gerät ↔ Server: Patientenliste, Statusmeldungen, Vorbefund-Abfragen	DICOM (TCP 104–106) im Praxisnetz	Nur erfasste Geräte, optional an IP-Adresse gebunden; Prüfung des aufgerufenen AE-Titels; Ablehnungen protokolliert
Gerät → Server: Bilder, Loops, Messwerte	DICOM C-STORE	Optional nur erfasste Geräte; Originaldaten unverändert gespeichert
Arbeitsplatz ↔ Server: Bedienung, Bilder, Berichte	HTTPS (TCP 8420)	Anmeldung, Rollen, TLS 1.2/1.3, CSRF-Schutz; ohne Passwort nur am Server-PC
Praxissoftware ↔ Server	GDT-Dateien in einem Austauschordner	Ordnerrechte der Praxis; Netzwerkanmeldung verschlüsselt gespeichert

Server → Export-/Sicherungsziel	Dateien (lokal, USB, NAS)	Ziel in Verantwortung der Praxis (Verschlüsselung empfohlen)
Server → Mailserver	SMTP mit STARTTLS oder TLS	Unverschlüsselter Versand nur an den eigenen PC (Loopback) möglich; Inhalte ohne Patientendaten
KI-Assistenz (optional)	Verarbeitung im Dienst auf dem Server-PC	Keine Übertragung an Dritte; Modell im Programm enthalten; Ergebnisse und Merkmalsvektoren in der lokalen Datenbank
Server → Hersteller	–	Es werden keinerlei Daten an den Hersteller übermittelt. Lizenzprüfung offline.

3. Bearbeitete Daten und Schutzbedarf

Datenkategorie	Beispiele	Schutzbedarf
Gesundheitsdaten (besonders schützenswert)	Ultraschallbilder, Loops, Messwerte, Befundtexte, PDF-Berichte, Untersuchungsart	hoch
Personalien der Patientinnen und Patienten	Name, Geburtsdatum, Geschlecht, Patienten-ID, Grösse/Gewicht, letzte Periode, Warnhinweise	hoch
Daten der Benutzer	Name, Anmeldename, E-Mail-Adresse, Passwort-Hash, Zugriffsprotokoll	mittel
Zugangsdaten zu Drittsystemen	Passwort Mailserver, Netzlaufwerke (Backup, Export, GDT)	hoch
Abgeleitete Daten der Assistenz	Erkannte Ebene, Wahrscheinlichkeiten, Messvorschläge, Merkmalsvektoren der Referenzbilder mit Bezeichnung	hoch (Bezug zu Gesundheitsdaten)
Betriebsdaten	Einstellungen, technische Protokolle	normal

Daraus folgen als Schutzziele: Vertraulichkeit (nur berechtigte Personen und Geräte), Integrität (Originalbilder unverändert, Änderungen nachvollziehbar), Verfügbarkeit (Empfang rund um die Uhr, Sicherung) und Nachvollziehbarkeit (wer hat wann was gemacht).

4. Technische Massnahmen

4.1 Zugang zum Webinterface

- **Sicherer Grundzustand:** Solange kein Passwort gesetzt ist, ist das Webinterface ausschliesslich am Server-PC selbst erreichbar (Zugriff über Loopback und die eigenen Computernamen). Der Zugriff aus dem Praxisnetz lässt sich erst einschalten, wenn ein Passwort gesetzt *und* HTTPS aktiv ist.
- **Persönliche Benutzer** mit den Rollen Administrator und Mitarbeiter (Kapitel 5). Das erste Passwort erzeugt den Administrator „admin“. Der letzte Administrator kann weder gelöscht noch herabgestuft werden.
- **Passwortregeln:** mindestens 8 Zeichen, Buchstaben und Ziffern. Speicherung als PBKDF2-HMAC-SHA256 mit 600 000 Iterationen und zufälligem Salt; ältere Hashes werden bei der nächsten Anmeldung automatisch auf diese Stärke gebracht.
- **Schutz vor Passwortraten:** pro Absender wachsende Wartezeit nach 5 Fehlversuchen (bis 30 Minuten); feste Antwortzeit und gleiche Rechenzeit auch bei unbekanntem Benutzer (keine Rückschlüsse auf gültige Anmeldenamen).
- **Sitzungen:** zufälliges Token (Cookie `HttpOnly`, `SameSite=Strict`, über HTTPS `Secure`), Ablauf nach 12 Stunden Inaktivität. Passwortänderung oder Zurücksetzen beendet alle Sitzungen des Benutzers.
- **Bestätigung heikler Änderungen:** Passwort entfernen, Fernzugriff einschalten, HTTPS ausschalten, Geräte hinzufügen oder Zugangsregeln lockern, Mailserver- bzw. Netzlaufwerk-Ziel ändern – jeweils nur nach erneuter Eingabe des eigenen Passworts. Ein maskiert übertragenes Passwort kann nicht an ein neues Ziel umgeleitet werden.
- **Passwort vergessen:** 8-stelliger Einmal-Code an die im Benutzer hinterlegte *persönliche* E-Mail-Adresse, 15 Minuten gültig, einmal verwendbar, nach 5 Fehlversuchen ungültig, max. 3 Anfragen pro Stunde und Absender; gleiche Antwort unabhängig davon, ob der Benutzer existiert. Ohne E-Mail: Zurücksetzen nur lokal am Server-PC mit Windows-Administratorrechten (Startmenü „Passwort zurücksetzen“).

4.2 Übertragungssicherheit (Web)

- **HTTPS** mit TLS 1.2/1.3. Beim ersten Einschalten erzeugt One DICOMServer ein ECDSA-P-256-Zertifikat für den Computernamen und die IP-Adressen des PCs. Es ist als eigene Zertifizierungsstelle ausgelegt, damit es auf Praxis-PCs als vertrauenswürdig installiert werden kann, ist aber durch kritische *Name Constraints* und *PathLen 0* auf genau diese Namen und Adressen beschränkt – der Schlüssel kann keine Zertifikate für fremde Websites ausstellen. Ein Zertifikat der Praxis-IT kann stattdessen hinterlegt werden.
- Unverschlüsselte Aufrufe auf demselben Port werden auf https umgeleitet (301).
- **Cross-Site-Schutz:** Zustandsändernde Anfragen benötigen eine eigene Kopfzeile, die fremde Websites nicht senden können; Anfragen mit fremdem Ursprung (`Origin`, `Sec-Fetch-Site`) werden abgewiesen. Content-Security-Policy ohne Inline-Skripte, `X-Frame-Options`, `nosniff`, `Referrer-Policy: no-referrer`.
- **Schutz vor DNS-Rebinding:** Nur IP-Adressen und die Namen dieses Computers werden als Host akzeptiert.

4.3 DICOM-Zugriff der Geräte

- **Patientenliste und Statusmeldungen (MWL, MPPS) sowie Archiv-Abfragen (C-FIND, C-MOVE)** erhalten standardmässig nur Geräte, die unter „Geräte verbinden“ erfasst sind. Ist beim Gerät eine IP-Adresse eingetragen, muss die Anfrage von genau dieser Adresse kommen; ein gefälschter AE-Titel von einem anderen Rechner wird abgelehnt (Status 0x0124).
- Der Empfang von Bildern unbekannter Geräte kann ebenfalls gesperrt werden (empfohlen nach der Einrichtung).
- Abgelehnte Zugriffe erscheinen im Protokoll (gedrosselt) und auf der Geräteseite unter „Neue Geräte“; die Übernahme eines Geräts erfordert die Bestätigung mit dem eigenen Passwort.
- Der eigene AE-Titel des Servers kann nicht als Gerät erfasst werden; AE-Titel, Hostnamen und Ports werden streng geprüft. Die Zahl gleichzeitiger Verbindungen ist begrenzt (64), Verbindungen ohne Aktivität werden nach dem eingestellten Zeitlimit getrennt.
- Der DICOM-Parser ist speichersicher implementiert (Go) und mit Fuzzing gegen fehlerhafte und bösartige Daten geprüft.

4.4 Datenhaltung

- **Lokal:** Alle Daten liegen auf dem Server-PC bzw. auf von der Praxis gewählten Laufwerken. Keine Cloud, keine Telemetrie, keine Updates im Hintergrund.
- **Datenbank:** eingebettete Datenbank (bbolt) als einzelne Datei `db\hcdicom.db`. Es gibt keinen Datenbankserver, keinen Netzwerkzugang zur Datenbank und deshalb keinen Datenbank-Benutzer und kein Datenbank-Passwort, die verwaltet werden müssten.
- **Dateirechte:** Der Datenordner `C:\ProgramData\One DICOMServer` bzw. nach einem Update von HC-DICOMServer weiterhin `C:\ProgramData\HC-DICOMServer` (Datenbank, Einstellungen, Protokolle, Berichte, Zertifikat) und das Bildarchiv sind bei der Installation auf SYSTEM und Administratoren beschränkt; normale Windows-Benutzer haben keinen Zugriff. Ein fremder, bereits bestehender Speicherordner wird dabei nicht verändert.
- **Passwörter für Drittsysteme** (Mailserver, Netzlaufwerke) werden in `config.json` mit der Windows Data Protection API (DPAPI, an den Computer gebunden) verschlüsselt gespeichert. Eine kopierte Konfigurationsdatei enthält keine lesbaren Passwörter. Im Webinterface werden sie nie im Klartext angezeigt.
- **Originaldaten bleiben unverändert:** Empfangene DICOM-Dateien werden nicht verändert. Korrekturen von Patientendaten werden als Ergänzung in der Datenbank geführt und protokolliert.
- **Export und Weitergabe** (ZIP, JPEG-Export, Senden an Geräte, GDT) erfolgen nur auf Veranlassung eines angemeldeten Benutzers bzw. gemäss Einstellung eines Administrators und werden protokolliert.

4.5 E-Mail

E-Mails (Code für „Passwort vergessen“, Störungsmeldungen) enthalten keine Patientendaten. Der Versand erfolgt nur verschlüsselt (STARTTLS oder TLS, Zertifikat wird geprüft); Kopfzeilen sind gegen Manipulation geschützt; Meldungen werden pro Thema höchstens alle 6 Stunden versendet.

5. Rollen und Berechtigungen

Funktion	Administrator	Mitarbeiter
Dashboard, Patienten & Studien, Viewer, Messungen	ja	ja
Patientenliste: Aufträge anlegen, ändern, erledigen, löschen	ja	ja
Berichte erstellen, PDF/ZIP herunterladen, an Gerät/Praxissoftware senden	ja	ja
DICOM-Import, Patientendaten korrigieren	ja	ja
Eigenes Passwort ändern	ja	ja
Studien, Bilder und Berichte löschen	ja	nein
Geräte verbinden, Einstellungen, Benutzer, Lizenz, Firewall	ja	nein
Praxissoftware (GDT), JPEG-Export, Backup & Wiederherstellung, Berichtvorlagen	ja	nein
Protokoll und Zugriffsprotokoll einsehen und herunterladen	ja	nein
Worksheet ansehen, Bilder analysieren lassen, Referenzbilder hinzufügen	ja	ja
KI-Assistenz ein- und ausschalten, Referenzbilder importieren und entfernen	ja	nein

Die Rollen werden serverseitig für jede Anfrage geprüft; verweigerte Zugriffe werden im Zugriffsprotokoll festgehalten.

6. Protokollierung (Zugriffsprotokoll)

- **Inhalt:** jede Änderung und jede Ausgabe von Patientendaten – z.B. Studie geöffnet, ZIP/PDF/DICOM heruntergeladen, Bericht gespeichert, Patientendaten korrigiert, Studie/Bild gelöscht, an Gerät oder Praxissoftware gesendet, Auftrag gespeichert – sowie Anmeldungen (erfolgreich/abgelehnt), Benutzer- und Einstellungsänderungen, verweigerte Zugriffe und DICOM-Abfragen der Geräte (Patientenliste, Archivsuche, Abruf).
- **Format:** Zeit, Aktion, betroffenes Objekt (eindeutige Kennung, keine Patientennamen), Ergebnis, Benutzer und Computer-Adresse bzw. Gerät.
- **Manipulationserkennung:** Jede Zeile trägt eine Prüfsumme (SHA-256) über ihren Inhalt und die Prüfsumme der vorherigen Zeile. Änderungen oder Löschungen einzelner Zeilen werden in der Ansicht „Zugriffsprotokoll (Monat)“ als „verändert ab Zeile …“ angezeigt.
- **Aufbewahrung:** Monatsdateien `logs\audit-JJJJ-MM.log`, 2 Jahre; technische Protokolle 60 Tage. Steuerzeichen in protokollierten Werten werden neutralisiert (kein Einschleusen gefälschter Zeilen).

7. Verfügbarkeit und Wiederherstellung

- Betrieb als Windows-Dienst mit automatischem Start und Neustart nach Fehlern; der Empfang läuft unabhängig von angemeldeten Benutzern.

- **Energiesparmodus:** One DICOMServer verhindert Standby und Ruhezustand am Netzbetrieb und prüft dies bei jedem Start und alle 6 Stunden (auch nach Windows-Updates).
- **Automatische Sicherung** nach Zeitplan auf USB-Festplatte, zweite Festplatte oder NAS: inkrementell, mit mehreren Datenbank-Versionen; verpasste Sicherungen werden nachgeholt. Wiederherstellung über das Webinterface; der vorherige Stand bleibt erhalten.
- **Überwachung:** Speicherplatz (Warnung unter 5 GB), belegte Ports, nicht erreichbare Export-/GDT-Ziele, fehlgeschlagene Sicherungen – Anzeige im Dashboard und auf Wunsch per E-Mail.
- Einstellungen werden atomar mit Vorgängerversion gespeichert; eine beschädigte Konfigurationsdatei wird automatisch aus der Vorgängerversion wiederhergestellt. Einstellungen lassen sich exportieren und importieren (ohne Passwörter).

8. Worksheet und KI-Assistenz

8.1 Funktion und Zweckbestimmung

Das **Worksheet** stellt die vom Gerät gesendeten Messwerte (DICOM Structured Report) geordnet dar und ergänzt sie um Gestationsalter, Perzentilen (INTERGROWTH-21st), Referenzbereiche (u.a. ASE/EACVI 2015/2016) und berechnete Werte. Die optionale **KI-Assistenz** umfasst: Plausibilitätsprüfung der Messwerte, Erkennung fetaler Standardebenen, automatische Messvorschläge für Kopfumfang, Abdomenumfang und Femurlänge mit Vergleich zum Gerätewert sowie den Vergleich mit einer praxiseigenen Referenzbibliothek.

Zweckbestimmung: Hilfsmittel zur Dokumentation und Qualitätssicherung. Die Funktionen stellen keine Diagnose, geben keine Therapieempfehlung und ersetzen nicht die ärztliche Beurteilung. Massgebend sind die Messungen am Untersuchungsgerät und die Befundung durch die Ärztin bzw. den Arzt. Die Assistenzfunktionen sind nicht als Medizinprodukt zertifiziert.

8.2 Datenschutz und Datensicherheit

- **Lokale Verarbeitung:** Das Modell (SonoNet-32, Baumgartner et al., IEEE TMI 2017, Lizenz Apache 2.0; Gewichte im Programm eingebettet) und alle Berechnungen laufen im Dienst auf dem Server-PC, ohne Internetverbindung. Es werden keine Bilder, Messwerte oder Ergebnisse übertragen, und es findet kein Training mit Praxisdaten statt.
- **Gespeicherte Daten:** Ergebnisse der Bildanalyse (Ebene, Wahrscheinlichkeiten, Messvorschlag) und die Referenzbibliothek (Bezeichnung, Merkmalsvektor, Verweis auf das Bild, Benutzer, Zeitpunkt) liegen in der lokalen Datenbank und unterliegen denselben Zugriffs-, Sicherungs- und Löschregeln wie die übrigen Daten. Merkmalsvektoren von Referenzbildern enthalten keine Personalien und lassen sich unter Einstellungen → KI-Assistenz entfernen.
- **Voreinstellung und Berechtigung:** Standardmässig ausgeschaltet. Nur Administratoren können die Assistenz einschalten; dabei wird bestätigt, dass die Hinweise nur als Hilfsmittel dienen. Benutzer und Zeitpunkt der Bestätigung werden gespeichert und im Zugriffsprotokoll festgehalten. Bei ausgeschalteter Assistenz lehnt der Server Analyseanfragen ab.
- **Protokollierung:** Anzeigen des Worksheets, Bildanalysen, Hinzufügen, Import und Entfernen von Referenzbildern werden im Zugriffsprotokoll geführt.

8.3 Transparenz und Massnahmen gegen Fehlinterpretation

- Jede Anzeige der Assistenz ist mit „Hilfsmittel“ gekennzeichnet und mit dem Hinweis „ersetzt nicht die ärztliche Beurteilung“ versehen; Hinweise nennen ihre Quelle (Referenz bzw. „KI-Assistenz (Bildanalyse)“).
- Messvorschläge werden im Bild als Kontur angezeigt, damit das Ergebnis überprüft werden kann; die Sicherheit der Messung und die Wahrscheinlichkeit der Ebene werden angegeben.
- Gerätewerte werden nie überschrieben. Hinweise der Assistenz werden nicht automatisch in Berichte oder an die Praxissoftware übernommen.
- Gegenprüfung nur in eindeutigen Fällen: keine Gegenprüfung bei Mehrlingen, ohne Kalibrierung keine Längenangabe, BPD/OFD (abweichende Messkonvention) werden nicht verglichen.

8.4 Grenzen

Die Erkennung der Standardebenen ist für fetale Ultraschallbilder des 2./3. Trimenons trainiert und kann bei anderen Darstellungen (1. Trimenon, 3D/4D, Doppler, Farbe, ungewöhnliche Schnittführung) falsch sein. Die Bildmessung ist eine klassische Konturanpassung und kann bei Schatten, angrenzenden Strukturen oder ungünstiger Bildqualität abweichen. Die Referenzbibliothek ist nur so gut wie die von der Praxis gewählten Referenzbilder. Die Software wurde mit Beispielbildern und synthetischen Daten geprüft; eine klinische Validierung an Praxisdaten liegt nicht vor.

9. Sichere Entwicklung und Prüfung

- Implementierung in Go (speichersicher); eigene DICOM-Implementierung; als einzige Fremdbibliotheken die quelloffenen Pakete bbolt (Datenbank) und golang.org/x/sys (Windows-Schnittstellen), beide im Quellcode mitgeliefert, sowie die Modellgewichte von SonoNet-32 (Apache 2.0, eingebettet; die Inferenz ist eigenständig in Go implementiert und gegen die Referenzimplementierung geprüft). Keine Laufzeit-Downloads.
- Reproduzierbarer Build; die SHA-256-Prüfsumme des Setups wird auf der Website veröffentlicht.
- Automatisierte Tests bei jedem Release: Unit- und Integrationstests (Go, mit Race-Detector), Fuzzing aller Parser für DICOM, Netzwerkprotokoll, GDT, Messwerte, Worksheet und Bilddekodierung (14 Fuzz-Ziele), Prüfung der KI-Inferenz gegen die Referenzimplementierung, 112 End-to-End-Prüfungen der Oberfläche (Desktop und Handy), 34 Netzwerktests gegen eine unabhängige DICOM-Implementierung (pynetdicom), HTTPS-Prüfungen. Ergebnisse siehe Testprotokoll 2.0.
- Für Version 2.0 wurden zwei unabhängige Sicherheitsprüfungen des Quellcodes durchgeführt; alle Befunde wurden behoben und durch Tests abgesichert.

10. Aufgaben der Praxis (Betreiber)

	Massnahme
☐	Server-PC mit aktuellem, unterstütztem Windows, automatischen Updates, Virenschutz und Windows-Konto mit Passwort betreiben; Festplatte mit BitLocker verschlüsseln.
☐	Im Webinterface ein Passwort setzen und für jede Person einen eigenen Benutzer mit persönlicher E-Mail-Adresse anlegen; gemeinsame Zugänge vermeiden; Benutzer austretender Mitarbeitender sofort löschen.
☐	HTTPS einschalten, sobald andere Geräte zugreifen; das Zertifikat auf den Praxis-PCs installieren oder den Fingerabdruck einmalig prüfen.
☐	Nach der Einrichtung „Bilder auch von Geräten annehmen, die nicht in der Liste stehen“ ausschalten und bei jedem Gerät die IP-Adresse eintragen; die Geräte erhalten feste IP-Adressen.
☐	Die Ports 104–106 und 8420 nur im Praxisnetz freigeben, nie ins Internet weiterleiten. Geräte und Server möglichst in einem eigenen Netzsegment betreiben.
☐	Automatische Sicherung einrichten, Sicherungsmedium verschlüsseln (z.B. BitLocker To Go), eine Kopie ausser Haus aufbewahren, die Wiederherstellung mindestens jährlich testen.
☐	E-Mail-Versand einrichten (Passwort vergessen, Störungsmeldungen).
☐	Zugriffsprotokoll monatlich herunterladen, prüfen und gemäss Aufbewahrungsfrist archivieren.
☐	Bildschirmsperre an allen Arbeitsplätzen; Tablets und Handys mit Gerätesperre, nur im Praxis-WLAN.
☐	Austauschordner für GDT und Exportziele auf die nötigen Konten beschränken.
☐	KI-Assistenz nur einschalten, wenn alle Benutzer über den Charakter als Hilfsmittel informiert sind; Referenzbilder sorgfältig auswählen und beschriften.
☐	Updates von One DICOMServer zeitnah installieren (Hinweise auf www.dicomserver.ch).

11. Restrisiken und Grenzen

Thema	Beschreibung	Massnahme / Empfehlung
DICOM unverschlüsselt	Die DICOM-Kommunikation mit den Geräten erfolgt – wie bei den meisten Modalitäten üblich – ohne TLS.	Betrieb nur im Praxisnetz, Netzsegmentierung, IP-Bindung der Geräte.
Prüfsummenkette des Zugriffsprotokolls	Die Kette erkennt Änderungen einzelner Zeilen. Wer Administratorrechte auf dem Server-PC hat, könnte eine Monatsdatei vollständig neu berechnen.	Zugriffsprotokoll monatlich exportieren und ausserhalb des Servers aufbewahren; Windows-Administratorkonten restriktiv vergeben.
Lesende Listenansichten	Das Öffnen einer Studie und jede Datenausgabe werden protokolliert, das blosse Anzeigen der Studien- und Patientenliste nicht.	Rollen und persönliche Benutzer nutzen.

Mitarbeiter-Rechte	Mitarbeitende dürfen Aufträge der Patientenliste löschen (Arbeitsabläufe am Empfang).	Löschungen sind im Zugriffsprotokoll nachvollziehbar.
Eigenes Zertifikat	Ohne Installation des Zertifikats zeigt der Browser beim ersten Aufruf eine Warnung.	Zertifikat installieren oder Fingerabdruck prüfen; alternativ Zertifikat der Praxis-IT hinterlegen.
DPAPI im Maschinenkontext	Gespeicherte Passwörter sind an den Computer gebunden; Prozesse mit Administratorrechten auf diesem PC können sie entschlüsseln.	Schutz des Server-PCs (Kapitel 10). Bei Umzug auf einen neuen PC sind die Passwörter neu einzugeben.
Sicherungen	Die Software verschlüsselt Sicherungen nicht selbst.	Verschlüsseltes Sicherungsmedium verwenden.
KI-Assistenz: Fehlerkennung	Ebenenerkennung, Messvorschläge und Plausibilitätshinweise können falsch positiv oder falsch negativ sein; das Fehlen eines Hinweises bedeutet nicht, dass die Messung korrekt ist.	Standardmässig aus, Kennzeichnung als Hilfsmittel, Kontur zur Kontrolle, keine Übernahme in Berichte; Schulung der Benutzer.
KI-Assistenz: Gewöhnung	Risiko, sich auf die Gegenprüfung zu verlassen (Automation Bias).	Organisatorisch: Messung am Gerät bleibt massgebend; Hinweise als Anlass zur Kontrolle, nicht als Ergebnis.
Zwei-Faktor-Anmeldung	Nicht vorhanden.	Zugriff nur aus dem Praxisnetz; starke Passwörter.

12. Datenschutzrechtliche Einordnung

Die Praxis ist Verantwortliche im Sinne des Bundesgesetzes über den Datenschutz (DSG). One DICOMServer unterstützt insbesondere

- **Datensicherheit (Art. 8 DSG, Art. 1–6 DSV):** Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit durch die in Kapitel 4–7 beschriebenen Massnahmen; Protokollierung gemäss Art. 4 DSV.
- **Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 7 DSG):** Zugriff standardmässig nur lokal, Patientenliste nur für erfasste Geräte, keine Übermittlung an Dritte, verschlüsselte Übertragung.
- **Keine Auftragsbearbeitung durch den Hersteller:** Der Hersteller hat keinen Zugriff auf die Daten der Praxis; eine Fernwartung findet nur statt, wenn die Praxis sie ausdrücklich veranlasst.
- **Berufsgeheimnis (Art. 321 StGB):** Die Daten verbleiben im Verantwortungsbereich der Praxis.
- **Automatisierte Auswertung:** Die KI-Assistenz trifft keine automatisierten Einzelentscheidungen im Sinne von Art. 21 DSG; sie liefert Hinweise für die behandelnde Person, die über deren Verwendung entscheidet.

Dieses Dokument beschreibt die technischen Eigenschaften der Software und ersetzt keine rechtliche Beurteilung im Einzelfall. Die Gesamtbeurteilung (inkl. Bearbeitungsverzeichnis, Datenschutz-Folgenabschätzung, Netzwerk und Organisation) obliegt der Praxis.

13. Anhang

Ports

Port (Standard)	Dienst	Richtung
104/TCP	DICOM: Bilder (C-STORE), Verbindungstest, Archiv-Abfragen (C-FIND/C-MOVE), Storage Commitment	eingehend aus dem Praxisnetz
105/TCP	DICOM: Patientenliste (MWL), Statusmeldungen (MPPS)	eingehend aus dem Praxisnetz
106/TCP	DICOM: Messwerte (SR), optional	eingehend aus dem Praxisnetz
8420/TCP	Webinterface (HTTPS)	eingehend, nur bei erlaubtem Fernzugriff freigegeben
Port der Geräte	DICOM-Versand an Geräte/PACS, Storage-Commitment-Rückmeldung	ausgehend
587 bzw. 465/TCP	Mailserver (optional)	ausgehend

Dateien und Ordner

Ort	Inhalt	Zugriff
`C:\Program Files\One DICOMServer`	Programm	Windows-Standard
`C:\ProgramData\One DICOMServer\config.json` (nach Update von 1.x: `…\HC-DICOMServer\`)	Einstellungen, Benutzer (Passwort-Hashes), verschlüsselte Fremdpasswörter	SYSTEM, Administratoren
`…\db\hcdicom.db`	Datenbank (inkl. Ergebnisse der Assistenz und Referenzbibliothek)	SYSTEM, Administratoren
`…\storage` oder gewählter Ordner	DICOM-Originaldateien	SYSTEM, Administratoren
`…\logs`	Protokolle, Zugriffsprotokolle	SYSTEM, Administratoren
`…\tls`	Zertifikat und privater Schlüssel für HTTPS	SYSTEM, Administratoren

Härtungs-Checkliste (Kurzfassung)

1. Einstellungen → Zugriff & Passwort: Passwort setzen, Benutzer anlegen, HTTPS einschalten.
2. Geräte verbinden: alle Geräte mit IP-Adresse erfassen; „Bilder … nicht in der Liste“, „Patientenliste … nicht erfasste Geräte“ und „Vorbefunde … nicht erfasste Geräte“ ausschalten.
3. Einstellungen → E-Mail: Versand einrichten, „Bei Problemen eine E-Mail senden“ einschalten.
4. Backup: Sicherung auf verschlüsseltes Medium einrichten, Testwiederherstellung.
5. Einstellungen → System: Energiesparmodus verhindern (Standard) und Datenbank prüfen.
6. Einstellungen → KI-Assistenz: nur bei Bedarf einschalten; Benutzer über den Charakter als Hilfsmittel informieren.