SECJUR

ISO/IEC 27001 in der Gesundheitsbranche

Die Checkliste für Founder & CEOs: 12 Schritte zur Zertifizierung, von der ersten Bestandsaufnahme bis zum erfolgreichen Audit.

Gesundheits-Startups und Digitalunternehmen im Health-Bereich verarbeiten täglich hochsensible Patientendaten. Gleichzeitig wächst der regulatorische Druck: **DSGVO, §75b SGB V und die NIS-2-Richtlinie** verlangen nachweisbare Informationssicherheit. Kliniken, Krankenkassen und Konzernkunden stellen vor jeder Zusammenarbeit detaillierte Sicherheitsfragebögen, und auch Investoren prüfen in der Due Diligence, ob euer ISMS belastbar ist. **ISO/IEC 27001** ist der internationale Standard, der all das messbar macht: ein strukturiertes Sicherheitsmanagementsystem, das Vertrauen schafft und Türen öffnet.

Diese vier Bereiche entscheiden über euren Erfolg:

BEREICH 01

Gesetzliche Pflichten

§75b SGB V schreibt IT-Sicherheit für Gesundheitsversorger explizit vor. DSGVO und NIS-2 ergänzen das mit konkreten Nachweis- und Meldepflichten. ISO 27001 liefert den Rahmen, um diese Anforderungen strukturiert zu erfüllen.

BEREICH 02

Patientendaten & DSGVO

Gesundheitsdaten zählen zu den sensibelsten personenbezogenen Daten (Art. 9 DSGVO). Ein zertifiziertes ISMS belegt gegenüber Aufsichtsbehörden und Partnern, dass technische und organisatorische Maßnahmen systematisch umgesetzt wurden.

BEREICH 03

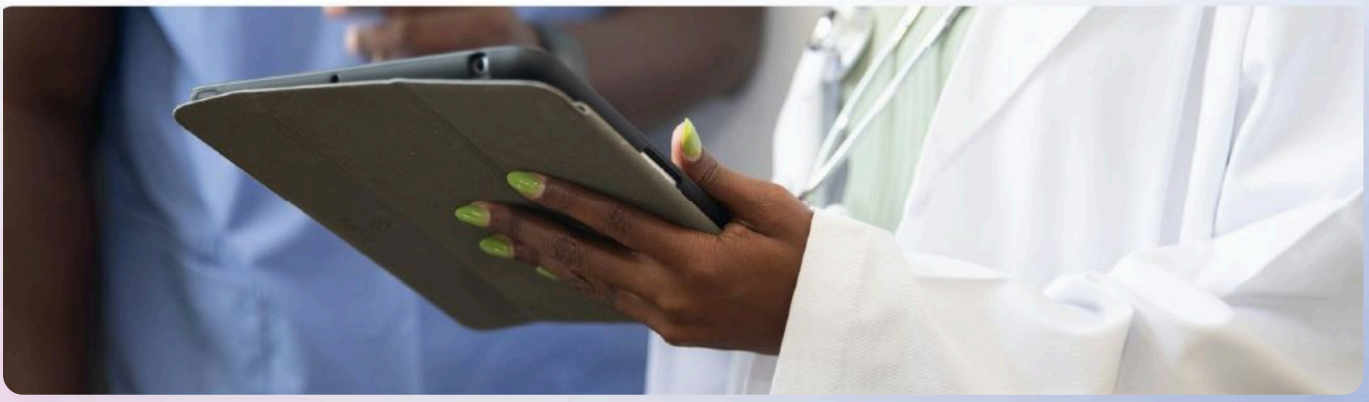
Kunden & Partner

Krankenhäuser, Krankenkassen und Pharmakonzerne verlangen von digitalen Partnern standardisierte Sicherheitsnachweise. Ein ISO-27001-Zertifikat ersetzt unzählige Einzelfragebögen und beschleunigt das Onboarding spürbar.

BEREICH 04

Investoren & Wachstum

Health-VCs und strategische Investoren prüfen in der Tech-Due-Diligence systematisch den Umgang mit Patientendaten und Sicherheitsvorfällen. Ein laufendes ISMS reduziert rote Flaggen und schützt die Bewertung.



3–6 Monate

typische Umsetzungszeit mit Plattform & Expert:innen, statt 12+ Monate im Eigenbau

Art. 9 DSGVO

Gesundheitsdaten als besondere Kategorie, maximale Schutzpflicht, maximale Haftung

§75b SGB V

gesetzliche IT-Sicherheitspflicht für digitale Gesundheitsversorger in Deutschland

SECJUR

Die Checkliste: Schritte 1–6

Von der Vorbereitung bis zur Risikobehandlung: Grundlagen eures Informationssicherheits-Managementsystems.

SCHRITT 01

Scope festlegen

- [ ] Systemgrenzen klar definieren (Systeme, Prozesse, Standorte)
- [ ] Datenkategorien inkl. Patientendaten identifizieren
- [ ] Schnittstellen zu Kliniken, Kassen, Dienstleistern erfassen
- [ ] Ausschlüsse begründen und dokumentieren
- [ ] Scope-Dokument formal verabschieden und versionieren

SCHRITT 02

Management-Commitment

- [ ] Informationssicherheit als Top-Management-Thema positionieren
- [ ] Budget und Ressourcen explizit bereitstellen
- [ ] ISB oder CISO benennen und im Organigramm verankern
- [ ] IS-Ziele mit der Geschäftsführung abstimmen
- [ ] Commitment der Führungsebene intern kommunizieren

SCHRITT 03

IS-Leitlinie verabschieden

- [ ] IS-Leitlinie mit Schutzzielen schriftlich formulieren
- [ ] Schutzziele definieren: Vertraulichkeit, Integrität, Verfügbarkeit
- [ ] Geltungsbereich und Verantwortlichkeiten benennen
- [ ] Geschäftsführung unterzeichnet die Leitlinie formell
- [ ] Kommunikation an alle Mitarbeitenden sicherstellen

SCHRITT 04

Risiken bewerten

- [ ] Asset-Inventar aufbauen: Systeme, Daten, Prozesse erfassen
- [ ] Bedrohungen und Schwachstellen je Asset identifizieren
- [ ] Risikobewertung nach Eintrittswahrscheinlichkeit × Schadenshöhe
- [ ] Healthcare-Risiken priorisieren: Datenpanne, Ransomware, Ausfall
- [ ] Risikoakzeptanzkriterien mit der Geschäftsführung abstimmen

SCHRITT 05

Statement of Applicability

- [ ] 93 Controls aus ISO/IEC 27002 auf Anwendbarkeit prüfen
- [ ] Ausschlüsse mit nachvollziehbarer Begründung dokumentieren
- [ ] Umsetzungsstatus je Control festhalten
- [ ] Verantwortliche und Zieltermine je Control benennen
- [ ] SoA regelmäßig aktualisieren und versionieren

SCHRITT 06

Risikobehandlung planen

- [ ] Behandlungsplan mit konkreten Maßnahmen je Risiko erstellen
- [ ] Strategie je Risiko wählen: akzeptieren, mindern, transferieren
- [ ] Verantwortliche und Umsetzungsfristen benennen
- [ ] Ressourcen (Budget, Tools, Personal) zuordnen
- [ ] Restrisiken durch Management formell akzeptieren lassen

Die Checkliste: Schritte 7–12

Von der Implementierung bis zum Zertifizierungsaudit: euer Weg zur ISO-27001-Zertifizierung.

SCHRITT 07

TOMs implementieren

- [ ] Verschlüsselung für Patientendaten at rest und in transit
- [ ] Zugriffskontrollen nach Need-to-know-Prinzip einrichten
- [ ] Monitoring und Logging für relevante Systeme aktivieren
- [ ] Pseudonymisierung und Rollen-/Rechtekonzept umsetzen
- [ ] Maßnahmennachweis in zentraler Dokumentation festhalten

SCHRITT 08

Lieferanten & AVV steuern

- [ ] Dienstleister mit Zugriff auf Patientendaten identifizieren
- [ ] AVV (Art. 28 DSGVO) mit Auftragsverarbeitern abschließen
- [ ] Sicherheitsanforderungen vertraglich verankern
- [ ] Fernwartungszugänge kontrollieren und protokollieren
- [ ] Bewertung der Dienstleister-Sicherheit regelmäßig wiederholen

SCHRITT 09

Schulungen & Awareness

- [ ] Pflichtschulung zu Informationssicherheit für alle
- [ ] Patientendaten und Schweigepflicht als Healthcare-Fokus
- [ ] Phishing-Simulationen und Awareness-Tests durchführen
- [ ] Incident-Response-Prozess definieren und schulen
- [ ] Schulungsnachweise lückenlos dokumentieren

SCHRITT 10

Interne Audits planen

- [ ] Audit-Jahresprogramm mit Scope und Terminen erstellen
- [ ] Auditoren unabhängig benennen oder extern beauftragen
- [ ] Nichtkonformitäten erfassen, bewerten und priorisieren
- [ ] Korrekturmaßnahmen einleiten und Wirksamkeit prüfen
- [ ] Audit-Berichte vollständig dokumentieren und archivieren

SCHRITT 11

Managementbewertung

- [ ] Jährliche Review-Sitzung mit Geschäftsführung durchführen
- [ ] ISMS-Leistung, Auditberichte und Vorfälle besprechen
- [ ] Risiken und Chancen aktualisiert bewerten
- [ ] Verbesserungsmaßnahmen beschließen und zuordnen
- [ ] Sitzungsprotokoll als formellen Nachweis dokumentieren

SCHRITT 12 · ZIEL

Zertifizierungsaudit bestehen

- [ ] Stage-1-Audit: Dokumentenprüfung durch akkreditierten Auditor
- [ ] Stage-2-Audit: Nachweis der gelebten ISMS-Praxis vor Ort
- [ ] Nichtkonformitäten fristgerecht beseitigen
- [ ] Zertifikat erhalten und kommunizieren
- [ ] Überwachungsaudits jährlich einplanen, Laufzeit 3 Jahre

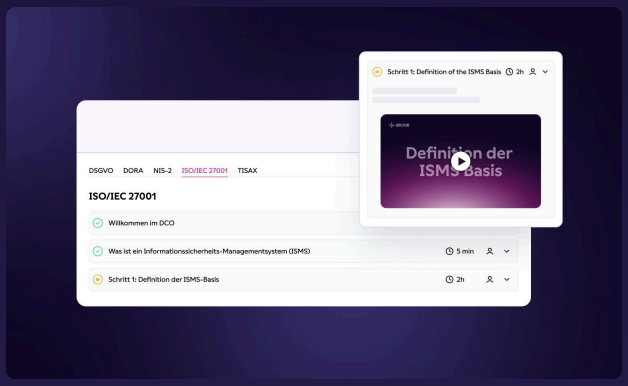
SECJUR

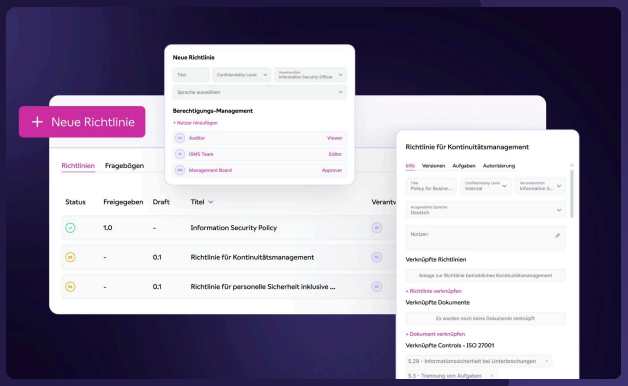
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

Mit der **SECJUR Automatisierungsplattform** und unseren **TÜV-zertifizierten Expert:innen** setzen Sie ISO 27001 in Rekordzeit um:

- Automatisierte Erstellung und Verwaltung Ihres ISMS
- Integriertes Risikomanagement & Lieferantenbewertungen
- Audit-Readiness auf Knopfdruck

Damit sparen Sie hunderte Stunden Aufwand – und sichern sich den entscheidenden Wettbewerbsvorteil bei großen Kundenprojekten.





Mit SECJUR zur automatisierten Compliance

"Als Einrichtung im Gesundheitswesen mussten wir NIS2 verlässlich und prüfungssicher umsetzen. Mit SECJUR haben wir Risikoanalyse, Dokumentation und Behördennachweise zentral abgebildet, ohne unser Tagesgeschäft auszubremsen."

Anonym

Leitung IT-Sicherheit, Gesundheitswesen

VIDEOCLINIC GSK EvoCare. St. Bernhard HOSPITAL HOMECARE die Alltagshelfer viluavitartis

www.secjur.com