FMH-IT-Grundschutz-Checkliste für Arztpraxen

Die 11 Minimalanforderungen der FMH zum Abhaken – mit der Prüffrage, die Sie sich in Ihrer Praxis stellen sollten. Stand Oktober 2026.

Die FMH hat 11 Minimalanforderungen zum IT-Grundschutz definiert (Dokumente D1, D2 und D3). Sie sind Empfehlungen, durch das revidierte Datenschutzgesetz (revDSG, seit 1. September 2023) aber faktisch verbindlich: Patientendaten gelten als besonders schützenswerte Personendaten, und die Verantwortung liegt bei der Praxisinhaberin bzw. dem Praxisinhaber. Jeder Punkt, den Sie nicht klar mit «Ja» beantworten können, ist eine Lücke.

Die 11 Anforderungen

- ☐ **1. Verantwortlichkeiten und Vorgaben**
  Gibt es eine schriftliche IT-Sicherheitsrichtlinie mit klaren Zuständigkeiten (Datenschutz, IT, Notfall), die das ganze Team kennt und jährlich aktualisiert wird?

- ☐ **2. Mitarbeitende sensibilisieren und schulen**
  Wurden alle Mitarbeitenden in den letzten 12 Monaten zu Phishing, Passwörtern und dem Umgang mit Patientendaten geschult?

- ☐ **3. Zugriffe auf Daten regeln**
  Hat jede Person ein eigenes Benutzerkonto mit Rechten nach Rolle («need to know»)? Werden Konten bei Austritten sofort deaktiviert?

- ☐ **4. Passwörter und Authentifizierung**
  Werden starke, eindeutige Passwörter (Passwort-Manager) verwendet und ist die Zwei-Faktor-Authentifizierung für E-Mail, Praxissoftware und Cloud aktiv?

- ☐ **5. Schutz vor Schadsoftware**
  Ist auf allen Geräten ein zentral verwalteter, aktueller Virenschutz mit Ransomware-Erkennung aktiv?

- ☐ **6. Firewall und Netzwerk**
  Schützt eine professionelle Firewall den Internetzugang? Sind Praxis-Computer, medizinische Geräte und WLAN in getrennten Netzen? Externe Zugriffe nur per VPN?

- ☐ **7. Software aktuell halten**
  Werden Betriebssysteme, Praxissoftware und Programme regelmässig und überwacht aktualisiert?

- ☐ **8. Daten regelmässig sichern**
  Läuft täglich ein automatisches Backup nach der 3-2-1-Regel (eine Kopie ausser Haus) – und wurde die Wiederherstellung in den letzten Monaten getestet?

- ☐ **9. Verschlüsselung**
  Sind Laptops und Computer verschlüsselt (FileVault bzw. BitLocker) und werden Patientendaten nur verschlüsselt versendet (z. B. HIN-Mail)?

- ☐ **10. Externe Dienstleister verpflichten**
  Gibt es mit allen externen Dienstleistern mit Datenzugang einen schriftlichen Vertrag zur Auftragsbearbeitung?

- ☐ **11. Notfallplan**
  Gibt es ein Notfallblatt auf Papier (Kontakte, erste Schritte, manueller Tagesplan) – und wurde der Ernstfall einmal geübt?

Auswertung

Alle 11 mit Ja: sehr gute Basis – lassen Sie die Umsetzung einmal jährlich unabhängig prüfen. **8 bis 10:** die Lücken gezielt schliessen, meist mit überschaubarem Aufwand. **Weniger als 8:** Handlungsbedarf – besonders bei Backup (8), Virenschutz (5) und Notfallplan (11), weil diese im Ernstfall über die Arbeitsfähigkeit der Praxis entscheiden.

FMH IT-Grundschutz-Check von Compu-Trade – CHF 985.– exkl. MwSt.
Wir prüfen alle 11 Anforderungen vor Ort, dokumentieren den Stand und zeigen, was zu tun ist. Compu-Trade betreut über 50 Arzt- und Zahnarztpraxen in der Deutschschweiz. Mehr:
www.compu-trade.ch/fmh-it-check-arztpraxis · Telefon 034 411 11 33 · info@compu-trade.ch

Grundlage: FMH-Empfehlungen zum IT-Grundschutz für Arztpraxen (D1–D3) und revDSG. Die Checkliste ersetzt keine Rechtsberatung. Ausführliche Erklärung aller Punkte: www.compu-trade.ch/single-post/it-sicherheit-arztpraxis-fmh-schweiz