

IT-Sicherheitscheck für Arztpraxen

Verständliche Checkliste für die Praxisleitung - ohne unnötiges IT-Fachchinesisch

So nutzt du die Checkliste: Markiere bei jeder Frage Ja, Nein oder Unsicher. Jeder Punkt mit Nein oder Unsicher gehört auf deine To-do-Liste. Bei Unklarheiten kann dein IT-Ansprechpartner die Frage direkt prüfen.

1. Internet, WLAN und Zugänge

Prüffrage	Ja	Nein	Unsicher
Ist unsere Praxis zusätzlich zum normalen Internetrouter gegen Angriffe aus dem Internet geschützt?			
Ist das Patienten-WLAN so getrennt, dass darüber kein Zugriff auf Praxisgeräte oder Patientendaten möglich ist?			
Hat jede Person im Team eigene Zugangsdaten statt eines gemeinsam genutzten Logins?			
Kann jede Person nur auf die Daten und Programme zugreifen, die sie für ihre Arbeit wirklich benötigt?			

2. Datensicherung und Notfall

Prüffrage	Ja	Nein	Unsicher
Werden unsere Praxisdaten jeden Tag automatisch und geschützt gesichert?			
Gibt es mindestens eine Datensicherung, die bei einem Angriff auf die Praxis-IT nicht ebenfalls betroffen wäre?			
Haben wir bereits getestet, ob sich unsere gesicherten Daten im Notfall wirklich wiederherstellen lassen?			
Gibt es einen schriftlichen Plan dafür, wen wir bei einem IT-Ausfall anrufen und wie der Praxisbetrieb weiterläuft?			

3. Geräte und Updates

Prüffrage	Ja	Nein	Unsicher
Bekommen alle Computer, Server, Tablets und anderen Praxisgeräte regelmäßig Sicherheitsupdates?			
Ist auf allen relevanten Geräten ein aktueller Schutz vor Schadsoftware eingerichtet?			
Sind die Daten auf Laptops und mobilen Geräten so geschützt, dass sie bei Verlust nicht einfach ausgelesen werden können?			
Werden Geräte, für die es keine Sicherheitsupdates mehr gibt, nicht mehr im Praxisbetrieb eingesetzt?			

4. Team und Passwörter

Prüfrage	Ja	Nein	Unsicher
Gibt es klare Regeln für sichere Passwörter, und nutzt niemand dasselbe Passwort für mehrere wichtige Systeme?			
Sind wichtige Zugänge zusätzlich zum Passwort mit einer zweiten Sicherheitsabfrage geschützt?			
Weiß unser Team, wie gefälschte oder gefährliche E-Mails erkannt werden und wie im Verdachtsfall zu reagieren ist?			
Werden die Mitarbeitenden regelmäßig zur sicheren Nutzung der Praxis-IT geschult?			

5. Datenschutz und Nachweise

Prüfrage	Ja	Nein	Unsicher
Ist geklärt, ob unsere Praxis einen Datenschutzbeauftragten benötigt, und ist bei Bedarf eine Person benannt?			
Haben wir schriftlich festgehalten, welche personenbezogenen Daten wir verarbeiten und wofür?			
Bestehen mit Dienstleistern, die Patientendaten verarbeiten, die erforderlichen Datenschutzvereinbarungen?			
Können wir anhand unserer Unterlagen nachweisen, welche Sicherheitsmaßnahmen in der Praxis umgesetzt sind?			

6. Telematikinfrastruktur und Kommunikation

Prüfrage	Ja	Nein	Unsicher
Ist unsere Anbindung an die Telematikinfrastruktur aktuell und funktioniert sie zuverlässig?			
Werden vertrauliche medizinische Nachrichten über den dafür vorgesehenen sicheren Kommunikationsweg KIM versendet?			
Ist das E-Rezept im Praxisalltag eingerichtet und wird es sicher genutzt?			

Dein Ergebnis

So wertest du aus: Zähle alle Kreuze bei „Nein“ und „Unsicher“ zusammen. Das ergibt deine offenen Punkte.

Offene Punkte: _____ von 23

- **0 offene Punkte** Stark aufgestellt. Weiter so, und einmal im Jahr neu prüfen.
- **1 bis 4 offene Punkte** Solide Basis mit Lücken. Geh die offenen Themen gezielt an.
- **5 oder mehr offene Punkte** Deutlicher Handlungsbedarf. Lass deine Praxis-IT bald prüfen.

Schon ein einziges Nein oder Unsicher bei Backup, Firewall oder Updates kann im Ernstfall teuer werden.

Mehr als ein Kreuz bei Nein oder Unsicher? Lass uns sprechen.

Die Experten von riomar gehen die offenen Punkte mit dir gemeinsam durch und geben dir Ratschläge zur Verbesserung.

Ruf uns an: +49 (0) 611 950 06 599