Datenschutz Praxis Check

Mein PraxisManager

Weitere Informationen und leicht verständliche Erläuterungen zu den folgenden Datenschutzanforderungen finden Sie unter dem QR-Code. Alternativ können Sie den folgenden Link nutzten:
https://mein-praxis-manager.de/datenschutz-praxis-check.html
Diese Analyse dient der ehrlichen Selbsteinschätzung zur Datenschutzsituation in Ihrer Praxis.

Legende

- ✅ alles ok
- ❗ Handlungsbedarf identifiziert
- ➖ gilt nicht für meine Praxis / Datenverarbeitung wird nicht eingesetzt

✅❗➖ Bestellpflicht Datenschutzbeauftragter

☐☐☐ Besteht für Ihre Praxis eine DSB-Bestellpflicht?
☐☐☐ Wurde Ihr Datenschutzbeauftragter ordnungsgemäß bestellt?

✅❗➖ Auftragsverarbeitungsvertrag (AVV)

☐☐☐ Wurde ein AVV mit Ihrem IT-Dienstleister abgeschlossen?
☐☐☐ Wurde ein AVV mit Ihrem Praxis-Verwaltungssystem-Anbieter abgeschlossen?
☐☐☐ Wurde ein AVV mit Ihrem Provider für Ihre Website abgeschlossen?
☐☐☐ Wurde ein AVV mit Ihrem Provider für Ihre E-Mails abgeschlossen?
Achtung: Free-Mail-Dienste!
☐☐☐ Wurde ein AVV mit Ihrem Provider für Ihre Telematik-Infrastruktur abgeschlossen?
☐☐☐ Wurde ein AVV mit Ihrem Labor (Order-Entry-System) abgeschlossen?
☐☐☐ Wurde ein AVV mit Ihrer privaten Verrechnungsstelle abgeschlossen?
☐☐☐ Wurde ein AVV mit dem Betreiber der Videosprechstunde abgeschlossen?
☐☐☐ Wurde ein AVV mit dem Betreiber Ihrer Telefonanlage abgeschlossen?
☐☐☐ Wurde ein AVV mit dem Betreiber Ihrer digitalen Assistenten abgeschlossen?
☐☐☐ Wurde ein AVV mit dem IT-Dienstleister Ihrer Medizintechnik abgeschlossen?
☐☐☐ Wurde ein AVV mit dem Betreiber Ihrer digitalen Personalakte abgeschlossen?
☐☐☐ Wurde ein AVV mit dem Betreiber Ihrer Zeiterfassung abgeschlossen?
☐☐☐ Wurde ein AVV mit der Plattform zum Dokumentenaustausch mit Ihrem Steuerberater abgeschlossen?

Datenschutz Praxis Check

Mein PraxisManager

Verzeichnis von Verarbeitungstätigkeiten (VVT)

- ☐☐☐ Ist ein VVT für Ihr Praxis-Verwaltungssystem vorhanden?
- ☐☐☐ Ist ein VVT für Ihre medizinischen Softwareanwendungen vorhanden?
- ☐☐☐ Ist ein VVT für die Abrechnung von GKV-Patienten vorhanden?
- ☐☐☐ Ist ein VVT für die Abrechnung von privaten Patienten vorhanden?
- ☐☐☐ Ist ein VVT für den Betrieb Ihrer Praxiswebsite vorhanden?
- ☐☐☐ Ist ein VVT für den Betrieb Ihres Online-Terminbuchungssystems vorhanden?
- ☐☐☐ Ist ein VVT für den Betrieb Ihrer digitalen Assistenten vorhanden?
- ☐☐☐ Ist ein VVT für die Verarbeitung Ihrer digitalen Anamnesebögen vorhanden?
- ☐☐☐ Ist ein VVT für den Betrieb Ihrer Telefonanlage vorhanden?
- ☐☐☐ Ist ein VVT für den Betrieb Ihres Zeiterfassungssystems vorhanden?
- ☐☐☐ Ist ein VVT für den Betrieb Ihrer digitalen Personalakte vorhanden?
- ☐☐☐ Ist ein VVT für den Betrieb Ihres Order-Entry-Systems (Labor) vorhanden?
- ☐☐☐ Ist ein VVT für die Lohnabrechnung Ihrer Mitarbeiter vorhanden?
- ☐☐☐ Liegt eine Dokumentation Ihrer TOMs vor?

Richtlinien für Ihre Mitarbeiter

- ☐☐☐ Ist eine Richtlinie zum Identifizieren von Anrufern vorhanden?
- ☐☐☐ Ist eine Richtlinie zur praktischen Umsetzung des Auskunftsrechts vorhanden?
- ☐☐☐ Ist eine Richtlinie zur Meldung von Datenpannen vorhanden?
- ☐☐☐ Ist eine Richtlinie zur Verwendung der ePA vorhanden?
- ☐☐☐ Ist eine Richtlinie zur Vernichtung von Daten einschließlich der Aufbewahrungsfristen vorhanden?

Praxis – Datenvernichtung

- ☐☐☐ Wurde die Datenvernichtung für Papier gemäß DIN 66399 umgesetzt?
- ☐☐☐ Wurde die Datenvernichtung für Festplatten gemäß DIN 66399 umgesetzt?
- ☐☐☐ Wurde die Datenvernichtung für SSDs und USB-Sticks gemäß DIN 66399 umgesetzt?
- ☐☐☐ Liegt eine Vorlage für ein Vernichtungsprotokoll für elektronische Geräte vor?

Datenschutz Praxis Check

Mein PraxisManager

IT-Dokumentation

- ☐☐☐ Ist eine vollständige IT-Dokumentation für alle Praxis-IT-Installationen vorhanden?
- ☐☐☐ Befinden sich alle Passwörter für Ihre IT-Systeme in Ihrer Praxis?
- ☐☐☐ Ist ein vollständiges IT-Inventarverzeichnis für Ihre Praxis vorhanden?
- ☐☐☐ Ist ein aktueller Netzwerkplan für alle IT-Systeme vorhanden?

Datenschutzinformation für Ihre Patienten

- ☐☐☐ Ist in Ihrer Praxis eine leicht zugängliche Datenschutzinformation für Ihre Patienten vorhanden?

Website

- ☐☐☐ Ist die Datenschutzerklärung auf Ihrer Website vorhanden und mit nur einem Klick erreichbar?
- ☐☐☐ Beschreibt die Datenschutzerklärung die Datenverarbeitung bei Ihrer Online-Terminvergabe?
- ☐☐☐ Beschreibt die Datenschutzerklärung die Datenverarbeitung bei Ihrer Videosprechstunde?
- ☐☐☐ Beschreibt die Datenschutzerklärung die Datenverarbeitung für Ihren Messenger?
- ☐☐☐ Beschreibt die Datenschutzerklärung die Datenverarbeitung bei Ihrer digitalen Patientenaufklärung?
- ☐☐☐ Können Patienten über Ihr Kontaktformular medizinische Daten bereitstellen? Ohne vollständige verschlüsselte Übertragung ist dies jedoch unzulässig.

Online-Terminbuchung

- ☐☐☐ Ist Ihre Datenschutzerklärung von jedem einzelnen Schritt der Terminbuchung mit nur einem Klick erreichbar?
- ☐☐☐ Beschreibt die Datenschutzerklärung die Datenverarbeitung bei der Online-Terminbuchung mit entsprechendem Inhalt?
- ☐☐☐ Enthält die E-Mail zur Online-Terminbuchung keinen medizinischen Kontext?
- ☐☐☐ Enthält die SMS zur Online-Terminbuchung keinen medizinischen Kontext?

Datenschutz Praxis Check

Mein PraxisManager

✅❗➖ Social Media Account

☐☐☐ Ist Ihre Datenschutzerklärung auf Ihrem Social Media Account mit nur einem Klick erreichbar?
☐☐☐ Beschreibt Ihre Datenschutzerklärung die Datenverarbeitung auf Ihrem Social Media Account?
☐☐☐ Haben Sie eine Strategie zur Verhinderung der unbefugten Kontaktaufnahme mit medizinischen Daten erfolgreich umgesetzt?

✅❗➖ Diskretion an Ihrer Anmeldung

☐☐☐ Ist in Ihrer Praxis bei der Anmeldung eine diskrete Kommunikation gegeben?
☐☐☐ Ist in Ihrer Praxis bei der Anmeldung ein diskreter Patientenaufruf möglich?

✅❗➖ Einwilligungserklärung

☐☐☐ Entsprechen alle Einwilligungserklärungen den vorgestellten Prüfungskriterien?
☐☐☐ Gibt es eine organisatorische und technische Lösung für Patienten, die der Einwilligung widersprochen haben?
☐☐☐ Haben Sie einen sicheren Prozess, der die Widersprüche Ihrer Patienten zur Speicherung in der ePA dokumentiert und den entsprechenden Datenupload sicher verhindert?

✅❗➖ Kommunikation

☐☐☐ Gibt es in Ihrer Praxis eine Kommunikation per E-Mail mit Mitarbeiterdaten an Ihr Lohnbüro?
☐☐☐ Gibt es in Ihrer Praxis eine Kommunikation per E-Mail mit medizinischen Patientendaten?
☐☐☐ Gibt es in Ihrer Praxis eine Kommunikation per SMS mit medizinischen Patientendaten?
☐☐☐ Gibt es in Ihrer Praxis eine Kommunikation per Fax mit medizinischen Patientendaten?
☐☐☐ Gibt es in Ihrer Praxis eine Kommunikation per Messenger mit medizinischen Patientendaten?

Videoüberwachung

☐☐☐ Hat Ihr Datenschutzbeauftragter die Videoüberwachung mit einer Datenschutzfolgeabschätzung analysiert und genehmigt?

Verantwortung auf alle Mitarbeiter übertragen

☐☐☐ Hat jeder Mitarbeiter in Ihrer Praxis eine schriftliche Verpflichtung zum Datenschutz und zur ärztlichen Schweigepflicht unterzeichnet?

☐☐☐ Wird jeder Mitarbeiter in Ihrer Praxis mindestens einmal pro Jahr geschult und werden die Nachweise schriftlich aufbewahrt?

Haben Sie Fragen zum Ausfüllen des Fragebogens oder zur korrekten Umsetzung des Datenschutzes in Ihrer Praxis? Kontaktieren Sie mich gern im Rahmen einer kostenlosen Erstberatung.

Matthias Boden

IT-Security-Beauftragter (TÜV®)
Datenschutzbeauftragter (TÜV®)

+49 351 27180437
kontakt@boden-it.de