HÄTTEN SIE ES GEWUSST, DASS

AUSGABE 2 | 2

die Sicherheitsbereiche (Punkt 4) bereits in der bestehenden IT-SICHERHEITSRICHTLINIE der Kassenärztlichen Bundesvereinigung gefordert werden? Diese gelten auch für Privatpraxen.

IT-Sicherheitsrichtlinie nach § 390 SGB V (KBV) – Übersicht

1. Zweck und Bedeutung

Die Richtlinie der KBV konkretisiert die gesetzlichen Vorgaben des § 390 SGB V. Sie definiert den technischen und organisatorischen Mindeststandard für Arzt- und Psychotherapiepraxen basierend auf Art. 32 DS-GVO.

- **Ziel:** Systematische Risikominderung zum Schutz sensibler Patientendaten (Art. 9 DS-GVO).
- **Schutzziele:** Vertraulichkeit, Integrität und Verfügbarkeit.

2. Verantwortlichkeiten

- Die Gesamtverantwortung verbleibt immer bei der **Praxisleitung**.
- Aufgaben dürfen an Mitarbeitende oder externe IT-Dienstleister delegiert werden.

3. Risikobasierter Ansatz

Die Sicherheitsanforderungen steigen mit der Praxisgröße und Komplexität:

- **Kategorien:** Kleine, mittlere und Großpraxen.
- **Zusatzregeln:** Gelten für Praxen mit medizinischen Großgeräten.

4. Wichtige Sicherheitsbereiche

Personal & Organisation: Da menschliche Fehler oft Sicherheitsvorfälle auslösen, steht der Mensch als wichtiger Faktor im Fokus.

Sensibilisierung & Schulung: Die Richtlinie fordert den Aufbau einer aktiven Sicherheitskultur durch regelmäßige Aufklärung des Teams. Praxisnahe Trainings müssen aktuelle Bedrohungen durch Fallbeispiele vermitteln.

Netzwerksicherheit: Das Praxisnetzwerk benötigt strikten Schutz vor unbefugten Zugriffen. Patchmanagement: Schnelles Schließen von Sicherheitslücken ist eine der wirksamsten Schutzmaßnahmen.

Endgerätesicherheit: PCs und Laptops brauchen Absicherungen, um den Betrieb bei Defekten oder Ransomware-Angriffen schnell wiederherzustellen.

Mobile Geräte: Smartphones und Tablets bergen Verlust- und Diebstahlrisiken; größere Praxen benötigen verbindliche Nutzungsrichtlinien.

Datenträger und Wechselspeicher: USB-Sticks und externe Speicher sind häufige Einfallstore für Schadsoftware.

E-Mail-Sicherheit: E-Mails sind Hauptangriffswege; Standards müssen je nach Praxisgröße skaliert erfüllt werden.

Apps & Cloud: Apps nur aus offiziellen Stores mit minimalen Rechten nutzen. Cloud-Anbieter für Gesundheitsdaten müssen ein aktuelles C5-Testat besitzen.

Webanwendungen & Großgeräte: Eigene Webdienste und medizinische Großgeräte (wie MRT/CT) benötigen Sondermaßnahmen, da sie oft jahrelang ohne Updates laufen.

Telematikinfrastruktur (TI): Die TI-Anbindung unterliegt separaten, strengen Sicherheitsvorgaben.

Haben wir Ihr Interesse geweckt? Gerne beraten wir Sie und Ihr Team.

Ihr Ansprechpartner: Achim Wolf | T: +49 7223.9669.323 | E: a.wolf@bendergruppe.com
b.e.consult GmbH | Dr.-Rudolf-Eberle-Straße 8-10 | 76534 Baden-Baden

07.2026

Weitere Infos auf: www.bendergruppe.com/be-consult

bender gruppe b.e.consult