PRAXIS-COMPLIANCE & IT-SICHERHEIT

Das Datensicherheits- & DSGVO-Paket

Der Leitfaden für Arztpraxen, Therapeuten & medizinisches Fachpersonal: Rechtssicherer Befundversand, Rezeptionsschutz, PVS-Ransomware-Abwehr und abheftfertige Vorlagen.

> **Fokus:** Strikte Einhaltung der ärztlichen Schweigepflicht (§ 203 StGB / Art. 321 StGB), Art. 9 DSGVO und KBV-Sicherheitsstandards — ohne teure IT-Dienstleisterverträge.

Ausgabe: 1. Praxis-Edition

Zielgruppe: Praxisinhaber, MFA & Therapeuten

1. Rechtlicher Rahmen: Schweigepflicht & Patientengeheimnis

Gesundheitsdaten unterliegen dem höchsten Schutzniveau der Rechtsordnung:

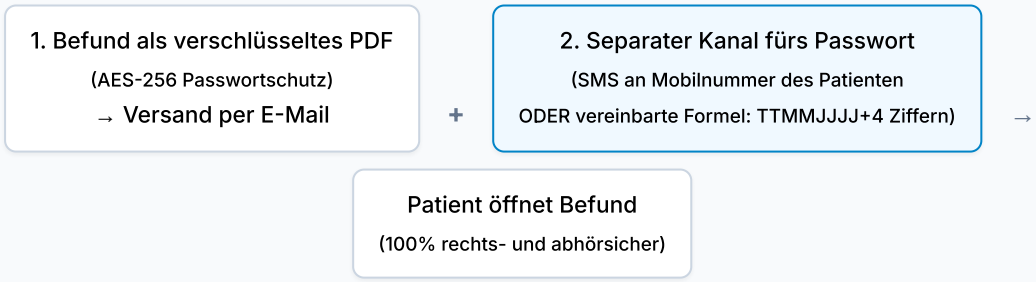
- **Art. 9 DSGVO:** Besondere Kategorien personenbezogener Daten (strikte Verarbeitungs- und Schutzauflagen).
- **Ärztliche Schweigepflicht (§ 203 StGB in DE / Art. 321 StGB in CH):** Verletzungen sind keine Ordnungswidrigkeiten, sondern **Straftaten**, die mit Geldstrafen, Freiheitsstrafen oder Approbationsentzug geahndet werden können.
- **KBV-Sicherheitsrichtlinie (§ 75b SGB V):** Gesetzliche Verpflichtung zur Einhaltung konkreter IT-Mindeststandards für Praxen.

Säule 1: Der rechtssichere digitale Befundversand

Die E-Mail-Haftungsfalle: Laborwerte, Befunde oder Arztbriefe unverschlüsselt per Standard-E-Mail zu versenden, ist ein grober Verstoß gegen das Patientengeheimnis. Selbst eine formlose Einwilligung des Patienten schützt die Praxis im Schadensfall rechtlich nicht ausreichend.

Das praxistaugliche 2-Kanal-Verfahren:

Wenn kein direkter KIM-Anschluss zum Empfänger besteht (z. B. bei Patienten, Physiotherapeuten oder Zuweisern):



1. **Kanal 1 (Befund):** Das PDF wird mit einem Passwort gesichert per Mail versendet.
2. **Kanal 2 (Passwort):** Das Passwort wird *niemals* in derselben Mail versendet. Es wird entweder per SMS an das Patienten-Handy gesendet oder basiert auf einer Vorab-Vereinbarung (z. B. Geburtsdatum des Patienten + letzte 4 Ziffern der Versichertennummer).

Säule 2: Physische Sicherheit an Rezeption & Behandlungsräumen

Die meisten Datenschutzverletzungen entstehen nicht im Internet, sondern durch **wartende Patienten in der Praxis**.

1. Rezeption & Tresen (Schutz vor Schulterblick)

- **Blickschutzfilter (Privacy Filter):** Monitore am Empfang müssen zwingend mit Blickschutzfolien ausgestattet sein. Seitlich wartende Patienten sehen nur ein schwarzes Display.
- **Diskrete Abstandslinie:** Eine deutliche Bodenmarkierung mit mindestens 1,5 bis 2 Metern Abstand verhindert unbefugtes Herantreten.
- **Keine offenen Akten:** Physische Patientenakten, Terminzettel oder Rezepte dürfen niemals mit lesbaren Namen nach oben auf dem Tresen liegen.

2. Behandlungs- und Sprechzimmer

- **Die 60-Sekunden-Autolock-Regel:** Verlässt der Arzt das Zimmer, sperrt der Rechner nach maximal 60 Sekunden automatisch.
- **Tastaturkürzel als Reflex:** Beim Verlassen des Raumes immer `Windows-Taste + L` (oder `Ctrl + Cmd + Q` auf Mac) drücken.
- **Strikte Router-Trennung:** Das Praxis-WLAN (für PVS, Kartenterminals) muss im Router strikt vom Patienten-Gäste-WLAN getrennt sein. Gäste dürfen unter keinen Umständen Zugriff auf IP-Adressen der Praxisrechner haben.

Säule 3: Ransomware-Schutz fürs Praxisverwaltungssystem (PVS)

> **Achtung vor Netzlaufwerken:** Standard-Backups auf dauerhaft angeschlossene USB-Festplatten oder Praxis-Server werden von modernen Erpressungstrojanern sofort mitverschlüsselt!

Das manipulationssichere 3-Medien-Rotationsprinzip:

1. **3 externe Festplatten anschaffen:** Beschrifte sie mit `Platte 1 (Mo/Di)`, `Platte 2 (Mi/Do)` und `Platte 3 (Wochenende)`.
2. **Tägliche Routine beim Praxisschluss:**
   - PVS-Sicherung auf die Tagesplatte starten.
   - **Entscheidend:** Die Festplatte nach der Sicherung **physisch vom PC abziehen**.
   - Die Wochenendplatte wird freitags von der Praxisleitung mit nach Hause genommen (Schutz vor Einbruch, Brand oder Wasserschaden in der Praxis).

3. **Vollverschlüsselung:** Alle Backup-Platten sind mit BitLocker oder FileVault verschlüsselt. Geht eine Platte verloren, sind die Patientendaten unlesbar.

PRAXIS-VORLAGE: VERPFLICHTUNGSERKLÄRUNG ZUM PATIENTENGEHEIMNIS

Gültig für: MFA, Aushilfen, Reinigungspersonal und externe IT-Betreuer gemäß § 203 StGB / Art. 321 StGB & DSGVO

Praxisinhaber / Praxis: _____
Mitarbeiter / Auftragnehmer: _____ **Geburtsdatum:** _____

1. VERPFLICHTUNG ZUR VERSCHWIEGENHEIT
Der/die Unterzeichnende wird hiermit ausdrücklich über die Pflicht zur absoluten Verschwiegenheit über alle personellen, geschäftlichen und vor allem medizinischen Belange (Patientendaten, Diagnosen, Behandlungen) belehrt.

2. STRAFRECHTLICHE RELEVANZ
Es ist bekannt, dass die unbefugte Offenbarung von Patientendaten nach § 203 StGB (bzw. Art. 321 StGB) mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bedroht ist. Diese Pflicht gilt zeitlich unbegrenzt – auch nach Beendigung des Arbeitsverhältnisses.

3. PRAXIS-SICHERHEITSVORSCHRIFTEN
- Bildschirme sind beim Verlassen des Arbeitsplatzes sofort zu sperren.
- Passwörter dürfen weder notiert noch an Dritte weitergegeben werden.
- Patientendaten dürfen nicht auf private Speichermedien oder Smartphones kopiert werden.

Ort, Datum: _____

Unterschrift Mitarbeiter/in: _____ **Unterschrift Praxisleitung:** _____

PRAXIS-NOTFALLPLAN: SOFORT-MASSNAHMEN BEI IT-AUSFALL & RANSOMWARE

VERDACHT AUF VERSCHLÜSSELUNGSTROJANER / HACKERANGRIFF:
(Symptome: Geänderte Dateiendungen, Lösegeldforderungen, gesperrter PVS-Server)

[ ] SCHRITT 1: SOFORT DAS NETZWERKKABEL ZIEHEN!
Ziehe sofort das Netzwerkkabel am betroffenen PC ab. Deaktiviere das WLAN. PC NICHT ausschalten oder neustarten (wichtig für spätere IT-Forensik).

[ ] SCHRITT 2: WEITERE RECHNER TRENNEN
Schalte die übrigen Arbeitsplatz-PCs im Netzwerk ab. Trenne sofort alle angeschlossenen externen Festplatten.

[ ] SCHRITT 3: PRAXISLEITUNG ALARMIEREN
Name Praxisleitung: _____ Telefon: _____

[ ] SCHRITT 4: IT-NOTFALLKONTAKT ANRUFEN
IT-Dienstleister / Betreuer: _____ Notfallnummer: _____

[ ] SCHRITT 5: GESETZLICHE 72-STUNDEN-MELDUNG VORBEREITEN
Bei Verdacht auf Datenabfluss muss die zuständige Landesdatenschutzbehörde innerhalb von 72 Stunden informiert werden.