LANDES-
ZAHNÄRZTEKAMMER
BRANDENBURG
Körperschaft des
öffentlichen Rechts

Informationsblatt

Organisatorische und technische Maßnahmen zum Datenschutz

Organisatorische Maßnahmen

Bereich	***Maßnahmen***
Empfangsbereich	➢ Verhinderung der Bildschirmeinsicht ➢ kennwortgeschützter Bildschirmschoner aktivieren ➢ Passwörter einrichten ➢ Diskretionszone einrichten (z.B. Schild „Bitte Abstand halten“) ➢ keine Dokumente liegen lassen ➢ keine Patientennamen bei telefonischen Gesprächen nennen (z.B. bei der Terminvergabe)
Wartezimmer	➢ möglichst geschlossener Raum ➢ im täglichen Betrieb Wartezimmertür geschlossen halten
Unbeaufsichtigtes Behandlungszimmer	➢ keine Karteikarten von vorher behandelten Patienten liegen lassen ➢ an Monitoren → keine offenen Karteikarten oder Röntgenbilder (kennwortgeschützter Bildschirmschoner)
Kommunikation innerhalb der Praxis	➢ bei interne Gesprächen zw. Mitarbeitern über eine Behandlung des Patienten → keine Patientennamen nennen, da es andere Patienten hören könnten

Rechtsgrundlagen des Datenschutzes und weitere Hinweise finden Sie im aktuellen Datenschutzleitfaden, den Sie downloaden können unter www.lzkb.de → Zahnarzt → Berufsrecht → Datenschutz → Datenschutz und Datensicherung in der Zahnarztpraxis.

Technische Maßnahmen (Software)

Bereich	***Maßnahmen***
Datensicherung	➢ Installation Sicherungssystem (Backup) ➢ Speichermedien (CD, DVD, USB, Festplatten, Bankschließfächer) ➢ Datensicherungen sollen verschlüsselt sein ➢ Lagerung außerhalb der Praxisräume (z.B. Tresor) ➢ Erstellung und Dokumentation von einem Sicherungs- und Wiederherstellungsplan ➢ diebstahlgeschützt und wassergeschützt ➢ Rücksicherung kontrollieren
Fremde Wechseldatenträger	➢ erst durch Virenprogramm überprüfen lassen ➢ privat mitgebrachte Wechselmedien von Mitarbeitern untersagen (Empfehlung)
Passwörter	➢ Bekanntgabe nur an zugriffsberechtigte Mitarbeiter ➢ Empfehlung → jeder Mitarbeiter eigenes Passwort ➢ Bei Ausscheiden des Mitarbeiters → sofortige Passwortsperre ➢ regelmäßige Änderung → Empfehlung alle 3 Monate ➢ länger als 7 Zeichen (Groß/-Kleinbuchstaben, Zahlen, Sonderzeichen) ➢ sollte nicht im Wörterbuch stehen und keine Namen oder Geburtsdaten enthalten
Nutzung E-Mail Programm	➢ Virenschutzprogramm nötig ➢ Anti-Spam-Software ➢ Anti- Phishing-Software ➢ Personal Firewall ➢ Empfehlung → Erstellung einer „Email – Richtlinie“ → jeder weiß dann wie mit E-Mails umgegangen werden muss
Fernwartung	➢ Praxis erteilt Freigabe für den Zugriff ➢ Mitverfolgung am Bildschirm der durchgeführten Tätigkeiten der Firma ➢ Auftragsdatenverarbeitungsvertrag notwendig → siehe www.zqms.de ➢ Protokollierung Umfang und Zeitpunkt der Wartungsarbeiten + Name des Techniker

Technische Maßnahmen (Hardware)

Bereich	***Maßnahmen***
Praxisinternes Netzwerk	➢ Internet nur über Router mit Firewall ➢ Bei WLAN → Praxisnetzwerk von normalem Netzwerk getrennt → VLAN`s + Verschlüsselung (WPA´s –Verfahren) ➢ PVS-System (Konnektor + VPN Verbindung) ➢ Empfehlung Beratung durch IT
Entsorgung Patientenunterlagen (Aktenvernichtung)	➢ nach DIN 66399 + DIN 32757 ➢ Zuordnung der Gesundheitsdaten Schutzklasse 3* + mind. Sicherheitsstufe 4** ➢ Entsorgung von PC´s → Zertifizierte Entsorgungsfirma, die gegen Entgelt Datenträger unlesbar macht & dafür Haftung übernimmt ➢ wenn extern → Auftragsdatenverarbeitungsvertrag erforderlich
Anforderung an der Hardwarekomponente (PC)	➢ Server im abschließbaren Raum oder Schrank → keine Nutzung als Arbeitsplatz ➢ USB Eingänge + CD/DVD Laufwerke gesichert ➢ abhängig von Praxisgröße und Art ➢ aktuelles Betriebssystem ➢ Betreuung durch Fachfirma empfohlen

*Schutzklasse 3 → sehr hoher Schutzbedarf für besonders vertrauliche & geheime Daten

**Sicherheitsstufe 4 → besonders sensible & vertrauliche Daten sowie personenbezogene Daten, die einem erhöhten Schutzbedarf unterliegen