

Checkliste TI – Datenschutz sicherstellen

Im laufenden Betrieb der TI in der Praxis ist zu gewährleisten, dass der Datenschutz stetig sichergestellt ist.

Das heißt: Nur, wenn die zugelassenen Komponenten der TI bestimmungsgemäß integriert und betrieben werden, besteht Haftungsausschluss des Praxisinhabers.

Zur Sicherstellung des Datenschutzes in der Praxis gilt Folgendes:

Konnektor:

- nur mit **aktuell zugelassenen** Firmware-Versionen betreiben
- verfügbare Firmware-Updates des Konnektor-Herstellers unmittelbar installieren
- an einem sicheren/geschützten Ort aufstellen
- AGBs und Besondere Geschäftsbedingungen des Vertriebspartners beachten
- Rückgabe / Entsorgung:
 - Konnektoren und eHealth-Kartenlesegeräte **zwingend** an den Hersteller / Vertriebspartner **zurückgeben**
 - Rückgabe ausschließlich über die „**sichere Lieferkette**“ **gemäß DSGVO** organisieren
 - Rückgabe ggf. eigenständig veranlassen
 - Geräte **in keinem Fall weiterverkaufen** (eBay o.ä.)
 - Übernahmeverträge ausschließlich mit TI-Vertriebspartner schließen

SMC-B / eHBA:

- nach dem Ende der Zertifikatsgültigkeit unbrauchbar machen (in mehrere kleine Stücke zerschneiden)
- bei Aufgabe der vertragszahnärztlichen Tätigkeit – **Sperrung der SMC-B veranlassen** (bei KZV Sachsen oder Kartenanbieter)
- **eHBA** am Ende der Praxis-Sprechzeit aus dem eHealth-Kartenlesegerät entnehmen und an einem **sicheren/geschützten** Ort aufbewahren
- PIN und PUK geheim halten, nicht zusammen mit Karten aufbewahren

eHealth-Kartenterminal:

- **BSI-Siegel** auf den Kartenslots für SMC-B und gSMC-KT aufbringen
- verfügbare **Updates** unmittelbar **installieren**
- an einem sicheren/geschützten Ort aufstellen
- Rückgabe und Entsorgung: siehe Ausführungen zu Konnektor

KIM-Fachdienst:

- Updates unmittelbar nach Verfügbarkeit installieren

Passwörter:

- sicher verwahren
- nur autorisierten Mitarbeitern zur Verfügung stellen
- **nach Ausscheiden** eines Mitarbeiters **neu vergeben**

Die vorgenannten Maßnahmen ersetzen keine Sicherheitssysteme für das Praxisnetzwerk. Es gelten weiter zusätzlich die IT-Sicherheitsrichtlinie sowie Empfehlungen zu Schweigepflicht, Datenschutz und Datenverarbeitung, mit denen Sie sich vertraut machen sollten.