

# **VA Maßnahmen nach § 75c SGB V, Einsatz von Smartphones und Tablets**

## **Übersicht**

Die Informationssicherheit nach § 75c SGB V regelt technische und organisatorische Maßnahmen (TOM) für medizinische Versorgungseinrichtungen wie Krankenhäuser und Kliniken zum Schutz vor Schadensfällen in der IT-Anwendung.

## **Ziel und Zweck**

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zum Einsatz von Smartphones und Tablets in strukturierten Prozessen und Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung, ist die Vereinheitlichung der Abläufe und die Sicherstellung des Prozesses, der geregelt wird und die Gewährleistung der Vollständigkeit sowie der geplanten Ergebnisqualität.

## **Anwendungsbereich**

Diese Anweisung gilt für die Anwendung in der medizinischen Versorgung in Krankenhäusern und Kliniken.

## **Verantwortung**

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- IT-Verantwortliche intern
- Externe IT-Dienstleistende

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

## **Grundsätze**

Die Nutzung von Smartphones und Tablets in der Klinik wird in den IT-Sicherheitsleitlinien und Datenschutzleitlinien generell definiert. Grundsätzlich gilt, dass eine private Nutzung nur über getrennte private Systeme erfolgt. Die Trennung von Klinik- und Privatnutzung ist Bestandteil der arbeitsrechtlichen Vereinbarung mit allen Mitarbeitenden, unabhängig von ihren Rollen und Positionen.

## **Prozesse**

Nutzung von Smartphones und Tablets:

### Schritt 1 / Schutz vor Phishing und Schadprogrammen im Browser

Es müssen immer aktuelle Schutzprogramme vor Phishing und Schadprogrammen im Browser genutzt werden. Siehe spezielle Verfahrensanweisung.

### Schritt 2 / Verwendung der SIM-Karten-PIN

SIM-Karten sollten grundsätzlich durch eine PIN geschützt werden. Die Super-PIN / PUK sind nur durch Verantwortliche anzuwenden.

### Schritt 3 / Sichere Grundkonfiguration für mobile Geräte

Besonders auf allen mobilen Endgeräten sollten die strengsten bzw. sichersten Einstellungen gewählt werden. Auch auf mobilen Geräten muss das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden.

### Schritt 4 / Verwendung eines Zugriffsschutzes

Alle mobilen Geräte sollten mit einem komplexen Gerätesperrcode geschützt werden.

### Schritt 5 / Updates von Betriebssystem und Apps

Damit Schwachstellen vermieden werden, sollten Updates des Betriebssystems und der eingesetzten Apps bei entsprechendem Hinweis auf neue Versionen zeitnah installiert werden. Es ist sinnvoll, einen festen Turnus (z.B. monatlich) festzulegen, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.

### Schritt 6 / Datenschutz-Einstellungen

Zugriffe von Apps und dem Betriebssystem auf Daten und Schnittstellen der mobilen Geräte sollten in den Einstellungen restriktiv auf das Notwendigste eingeschränkt werden.

**Aktualisierung:** nach 12 Monaten

#### **Mitgeltende Dokumente:**

- IT-Sicherheitsrichtlinie nach § 75b & 75c SGB V
- Bundesdatenschutzgesetz (BDSG) Auszug § 64
- Datenschutz-Grundverordnung (DSGVO) Auszug Art. 32
- §§ 135 ff. SGB V QM Richtlinie des GBA (GBA-RI)
- DKG-Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S)
- IT-Sicherheitsregelungen der Trägerschaften (z.B. RKD, EKD)
- BSI Grundschutz/VdS 10000 Standard

- Leitlinie zur IT-Sicherheit
- VA Einsatz von Virenschutz