

IT-Sicherheitsrichtlinie nach § 390 SGB V – Checkliste zur Umsetzung

Die aktualisierte IT-Sicherheitsrichtlinie wurde am 1. Juli 2025 veröffentlicht und trat am 2. Juli 2025 in Kraft. Die neuen bzw. geänderten Anforderungen sind **ab dem 2. Januar 2026 verpflichtend** umzusetzen und betrifft die Praxisleitung einschließlich aller Mitarbeiter einer Zahnarztpraxis, welche sich ständig mit der Datenverarbeitung befassen.

Die Checkliste „**Medizinische Großgeräte**“ dient als Ergänzung zur Checkliste „**Praxis bis 5 Personen**“ oder „**Mittlere Praxis bis 20 Personen**“. Diese benötigen Sie bei der Nutzung von medizinischen Großgeräten sowie zur Umsetzung der Anlagen 4. Weitere detaillierte Hinweise finden Sie auf der Website der KZBV sowie in der o. g. Richtlinie.

Hinweis:

- ① *Es besteht Handlungsbedarf*
- ✓ *Alle IT-Sicherheitsanforderungen erfüllt*
- ⊗ *Nicht für die Zahnarztpraxis zutreffend*

Praxisnummer:	
Praxisname:	
☰	
☎	

Anlage	Nr.	Anforderung	Erläuterung	
4	1	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen	Es muss sichergestellt werden, dass nur zuvor festgelegte berechnete Mitarbeitende auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten zugreifen können. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Passwörter müssen gewechselt werden. Der Wechsel muss dokumentiert und das Passwort sicher hinterlegt werden. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Benutzerkonten sollten gewechselt werden.	
		Umsetzung		
		Festlegung berechtigter Mitarbeiter für den Zugriff auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten:	Mitarbeiter festgelegt Dokumentation der Berechtigungen	
		Änderung der herstellerseitig gesetzten Passwörter:	Passwörter geändert Passwörter sicher dokumentiert	
		Änderung der standardmäßig eingerichteten bzw. herstellerseitig gesetzte Benutzerkonten:	Benutzerkonto geändert Änderung dokumentiert	
Anlage	Nr.	Anforderung	Erläuterung	
4	2	Nutzung sicherer Protokolle für die Konfiguration und Wartung	Für die Konfiguration und Wartung von medizinischen Großgeräten müssen sichere Protokolle genutzt werden. Die Daten müssen beim Transport vor unberechtigtem Mitlesen und Veränderungen geschützt werden.	
		Umsetzung		
		Nutzung sicherer Protokolle für die Konfiguration und Wartung:	Nutzung eines sicheren Protokolls für die Konfiguration Nutzung eines sicheren Protokolls für die Wartung	
		Schutz beim Transport vor unberechtigtem Mitlesen und Veränderungen:	Schutz beim sicheren Transport gewährleistet	

Anlage	Nr.	Anforderung	Erläuterung
4	3	Protokollierung	Es muss festgelegt werden: - welche Daten und Ereignisse protokolliert werden sollen, - wie lange die Protokolldaten aufbewahrt werden und - wer diese einsehen darf. Generell müssen alle sicherheitsrelevanten Systemereignisse protokolliert und bei Bedarf ausgewertet werden.
		Umsetzung	
		Festlegung, welche Daten und Ereignisse protokolliert werden:	Daten und Ereignisse festgelegt Festlegung in den Unterlagen dokumentiert
		Festlegung, wie lange die Protokolldaten aufbewahrt werden:	Zeitraum der Aufbewahrung der Protokolldaten festgelegt Festlegung in den Unterlagen dokumentiert
		Festlegung, wer diese einsehen darf:	Berechtigung für die Einsicht festgelegt Festlegung in den Unterlagen dokumentiert
Anlage	Nr.	Anforderung	Erläuterung
4	4	Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen	Alle nicht genutzten Dienste, Funktionen und Schnittstellen der medizinischen Großgeräte müssen soweit möglich deaktiviert oder deinstalliert werden.
		Umsetzung	
		Deaktivierung/Deinstallation aller nicht genutzten Dienste, Funktionen und Schnittstellen.	Deaktivierung/Deinstallation nicht genutzter Dienste durchgeführt Deaktivierung/Deinstallation nicht genutzter Funktionen durchgeführt Deaktivierung/Deinstallation nicht genutzter Schnittstellen durchgeführt Deaktivierung/Deinstallation dokumentiert
Anlage	Nr.	Anforderung	Erläuterung
4	5	Deaktivierung nicht genutzter Benutzerkonten	Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert werden.
		Umsetzung	
		Deaktivierung nicht genutzter/unnötiger Benutzerkonten:	Deaktivierung nicht genutzter Benutzerkonten durchgeführt Deaktivierung dokumentiert
Anlage	Nr.	Anforderung	Erläuterung
4	6	Netzsegmentierung	Medizinische Großgeräte sollten von der weiteren IT getrennt werden. Insbesondere sollten ferngewartete medizinische Großgeräte in einem eigenen Netzwerksegment eingebunden werden.
		Umsetzung	
		Trennung medizinischer Großgeräte von der weiteren IT:	Trennung von der IT durchgeführt In eigenes Netzwerk eingebunden Einrichtung dokumentiert

Ort:

Datum:

Praxisstempel/Unterschrift: