

## **Das IT-Sicherheitskonzept**

Das Gesetz verpflichtet Ärztinnen und Ärzte zu einem IT-Sicherheitskonzept, dem schriftlichen Protokoll aller Datensicherheits-Maßnahmen. In diesem Bericht unserer Serie zur Datensicherheit in Arztpraxen können Sie sich darüber informieren, worauf Sie dabei achten müssen.

Eine Serie von DI Michael Nöhammer

Ärztinnen und Ärzte sind gesetzlich verpflichtet, alle Datensicherheits-Maßnahmen schriftlich zu protokollieren. Die gesamte Dokumentation wird in unserem Zusammenhang als IT-Sicherheitskonzept bezeichnet. Dieses kann bzw. muss beispielsweise folgendes enthalten:

- Dokumentation der Aufgabenverteilung der der daraus resultierenden Datenverwendung je Mitarbeiter
- Dokumentation der Zutrittsberechtigung zu den Räumlichkeiten der Ordination je Mitarbeiter
- Unterzeichnete Belehrung über Datenschutzvorschriften
- Unterzeichnete Aufteilung der Zugriffsberechtigung auf Daten und Programme je Mitarbeiter
- Informationen über Datensicherungsmaßnahmen und Datensicherungen.

Die enthaltenen Dokumente müssen laufend aktualisiert werden.

### **So steht es im Gesetz**

Das Gesundheitstelematikgesetz (GTelG) 2012 formuliert dies im § 2 so: „IT-Sicherheitskonzept“: Summe aller Datensicherheitsmaßnahmen eines Gesundheitsdiensteanbieters, die zum Schutz von personenbezogenen Daten, insbesondere von sensiblen Daten, notwendig und angemessen im Sinne des § 14 Datenschutzgesetz (DSG) 2000 sind. Im § 8 Abs. 1 ist weiters zu lesen: Gesundheitsdiensteanbieter haben auf Basis eines IT-Sicherheitskonzeptes alle gemäß § 14 DSG 2000 und den Bestimmungen dieses Bundesgesetzes getroffenen Datensicherheitsmaßnahmen zu dokumentieren. Aus dieser Dokumentation muss hervorgehen, dass sowohl der Zugriff als auch die Weitergabe der Daten ordnungsgemäß erfolgt und die Daten Unbefugten nicht zugänglich sind.

Mit dem IT-Sicherheitskonzept können Sie im Anlassfall nachweisen, dass Sie die Ihnen „unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit“ (DSG 2000) zumutbaren Maßnahmen getroffen haben.

Zusätzlich fordert das GTelG im § 8 Abs. 3: Die Dokumentation gemäß Abs. 1 ist auf Verlangen des Bundesministers für Gesundheit diesem zu übermitteln.

***Diese Dokumentation dient daher Ihrem Schutz und der Sicherheit Ihrer Mitarbeiter!***

## **So kommen Sie zu einem IT-Sicherheitskonzept**

Als ersten Schritt sollten Sie alle relevanten Dokumente sammeln und diese an einem Ort (in einem Ordner) sicher aufbewahren. Die Österreichische Ärztekammer wird im Lauf des Jahres 2014 eine Vorlage zur Verfügung stellen, die ein minimales IT-Sicherheitskonzept darstellt. Mithilfe dieser Vorlage können Sie überprüfen, ob Ihre Dokumentation vollständig ist und Sie können ggf. Ihre Unterlagen erweitern. Sollten Sie IT Systeme oder Programme betreiben, die durch die Vorlage nicht abgedeckt sind, so sind diese ebenfalls sinngemäß zu dokumentieren.

Wichtig: Alle Dokumente sind immer auf dem aktuellen Stand zu halten!

## **Kontrolle des IT-Sicherheitskonzepts**

Aus heutiger Sicht ist es ausgeschlossen, dass Dritte in Ihrer Ordination das IT-Sicherheitskonzept einsehen oder überprüfen können. Im Anlassfall (Gerichtliches Verfahren, ...) kann von Ihnen allerdings verlangt werden, das IT-Sicherheitskonzept vorzulegen, damit dieses inhaltlich geprüft werden kann. Sofern Sie ELGA verwenden, kann das Bundesministerium für Gesundheit ohne Anlassfall Einsicht in das IT-Sicherheitskonzept verlangen, ein Besuch in der Ordination aus diesem Anlass ist aber nicht vorgesehen.

<b>Praxistipps</b>	
√	Sammeln Sie alle relevanten Dokumente
√	Überprüfen Sie laufend die Unterlagen auf Vollständigkeit und Aktualität