

IT Sicherheit in den Ordinationen	
Organisation, physischer Schutz, Mitarbeiter	

Datenschutz ist mehr als EDV-Sicherheit

Datensicherheit in der Ordination beginnt nicht erst beim Einsatz eines IT-Systems, geeignete Datenschutz- Maßnahmen sind bereits bei der räumlichen Organisation einer Arztpraxis gefordert. Unsere Artikel-Serie der Bundeskurie Niedergelassene Ärzte bietet Ihnen Service und Praxistipps zum Thema IT-Sicherheit.

Eine Serie von DI Michael Nöhammer

Datensicherheit beginnt nicht erst beim Einsatz eines Informationstechnik-Systems. Viele grundlegende Prozesse in einer Ordination haben nichts mit der IT zu tun, trotzdem geht es dabei um sensible Patientendaten. Gerade in diesem Bereich können meist ohne großen Aufwand wesentliche Verbesserungen erzielt und damit die Datensicherheit in der Ordination deutlich erhöht werden.

Örtliche Gegebenheiten

Stellen Sie sicher, dass betriebsfremde Personen (Patienten, Dienstleister) nicht versehentlich oder absichtlich sensible Daten einsehen können:

- Drehen Sie PC-Monitore so, dass nur Sie und Ihre Mitarbeiter die Daten einsehen können;
- Benutzen Sie Bildschirmschoner, die sich nach kurzer Zeit (30 Sekunden) einschalten und verhindern Sie dadurch Einblicke wartender Patienten;
- Behandeln Sie Ausdrucke und ankommende Faxe sorgfältig und lassen Sie diese nicht unbeaufsichtigt liegen;
- Gestalten Sie den Anmeldebereich so, dass die dort geführten Gespräche vertraulich bleiben;
- Minimieren Sie im täglichen Arbeitsablauf die Möglichkeiten zur Einsichtnahme in fremde Daten.

Physischer Zugriff auf Daten

- Halten Sie Ihre Daten verschlossen:
 - o Karteikasten versperren
 - o Server in einen eigenen absperrbaren Raum stellen. Steht kein abgeschlossener Bereich zur Verfügung, sollten PC und Datenserver durch andere geeignete Maßnahmen gegen Diebstahl gesichert werden, zum Beispiel durch spezielle Kabelbefestigungen oder verschweißte Computer-Gehäuse („Cases“);
- Stellen Sie sicher, dass betriebsfremde Personen keinen Zugriff auf Ihre Rechner haben;
- Verschlüsseln Sie Ihre Datensicherungsmedien – Ihr IT-Dienstleister weiß, wie das geht – und/oder versperren Sie diese sicher, um Missbrauch zu verhindern;

- Vergessen Sie nicht auf Daten in Papierform wie Faxe, Briefe, Befunde oder Formulare – auch diese sollten nicht von unbefugten Personen gelesen werden können.

Verträge mit Mitarbeitern und Dienstleistern

Die gesetzlichen Verpflichtungen schreiben vor, dass datenschutzrechtliche Auftraggeber sowie Dienstleister und ihre Mitarbeiter alle Daten aus Datenanwendungen, die ihnen ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung anvertraut oder zugänglich wurden, geheim zu halten haben. Zusätzlich müssen Sie als Ordinationsinhaber festlegen, welche Mitarbeiterinnen und Mitarbeiter auf welche Daten Zugriff haben dürfen. Es empfiehlt sich, nur den unbedingt notwendigen Datenzugriff zu gestatten.

Die Vereinbarungen über Datenzugriff, die Belehrungen über die Verschwiegenheits- und andere Pflichten dokumentieren Sie am besten durch nachweisliche Unterfertigung einer ausgehändigten Vorlage der gesetzlichen Bestimmung. Die Homepage der ÖQMed www.oeqmed.at stellt kostenfrei entsprechende Vorlagen zum Download zur Verfügung.

Praxistipps:	
√	Gestalten Sie Ihre Ordination und den täglichen Ablauf so, dass möglichst wenig Gelegenheit zur Dateneinsicht entstehen kann
√	Sorgen Sie auch ohne IT für Datenschutz
√	Belehren Sie Ihre Mitarbeiterinnen und Mitarbeiter ausführlich und schriftlich