

Fax und Brief:

Sicherheit ohne Elektronik

Auch bei nichtelektronischen Medien gilt der Datenschutz. Regeln Sie deshalb in Ihrer Ordination, wer

- Briefe öffnen
- eingegangene Faxnachrichten abholen
- schriftlich vorliegende Befunde einscannen

darf und wie die Schriftstücke weiter behandelt werden. Das betrifft z.B. deren Einsortieren in die Patientendokumentation, Ablage oder Vernichtung. Stellen Sie eine korrekte Entsorgung der Papierdokumente mit sensiblen Patientendaten sicher, z.B. durch die Beauftragung einer dafür zertifizierten Firma.

WLAN, Bluetooth, Mobilfunk

Denken Sie bei der Absicherung Ihres IT-Systems auch an drahtlose Netzwerke. Diese bringen zwar ein Plus Bequemlichkeit, eröffnen allerdings Personen ohne physische Anwesenheit in der Ordination die Möglichkeit, auf Patientendaten zuzugreifen.

Ein WLAN (Wireless Local Area Network) ermöglicht Datenübertragung per Funk, die Reichweite beträgt etwa 30 Meter, die Datenübertragungsrate beträgt meistens 54 Mbit/s oder mehr. Der typischer Einsatz von WLAN erfolgt bei Notebooks, Tablets, Smartphones oder Spielkonsolen. Sichern Sie WLAN Netze immer mit der aktuellsten Technologie ab (derzeit WPA2), verwenden Sie „starke Passwörter“ und wechseln Sie diese regelmäßig.

Schalten Sie das WLAN ab, sobald Sie es nicht benötigen.

Bluetooth ermöglicht Funkkommunikation mit geringer Reichweite von maximal 10 Meter.

Es wird typischer Weise bei Headsets (Kopfhörern) eingesetzt. Sollten Sie Bluetooth nicht benötigen, deaktivieren Sie es.

Falls Sie Mobilfunk einsetzen, verwenden Sie für den Datenzugriff ein Virtual Private Network (VPN), eine verschlüsselte Datenverbindung über das Internet.

Internet: offen oder nicht?

Sie haben in Ihrer Ordination – sofern Sie über einen ecard-Anschluss

verfügen – zwei Möglichkeiten einer Internetanbindung: Internet über GIN/Peeringpoint und Internet über privaten Anbieter.

Internet über GIN/Peeringpoint

Mehrwertdienste sind Dienste, die Sie aus ihrer Ordination ohne Internetzugang direkt über den Anschluss des Gesundheits-Informations-Netzes (GIN) nutzen können und die keinen Bezug zur Sozialversicherung haben. Beispiele dafür sind Befundübertragung, Internet, Zahlssysteme/Bankomat, Fernwartung, Softwareupdates etc. Das GIN ist ein Hochsicherheitsnetz zur Kommunikation im Gesundheitswesen. Nur berechtigte Teilnehmer wie Ärzte, Heime, Krankenanstalten, Apotheken oder Rettungsorganisationen haben Zugang zum GIN.

Sie können Internet als Mehrwertdienst über das GIN bzw. den Peeringpoint – einen Netzwerkknoten, der das GIN mit vielen anderen Netzen (Sozialversicherung, Krankenhäuser, Bundesbehörden) verbindet – beziehen. Dadurch wird Ihnen von einem Mehrwertdienstanbieter ein überwachtes Internet geliefert, wodurch gewisse Sicherheitselemente aktiviert sind:

- Es ist kein Zugriff von außen auf Ihre Ordination möglich.
- Definierte Ports (Kommunikationskanäle im Netzwerk) sind freigeschaltet, die Ordination kann damit nicht (versehentlich/durch Virus) als Anbieter von Inhalten auftreten.
- Ein Virenschutz für Stationen ist integriert.
- Bei Verwendung mitgelieferter Mailadressen gibt es einen Viren/Spamschutz.

Vorteilhaft ist, dass Sie keinerlei zusätzliche Infrastruktur benötigen, ein Nachteil ist die Bandbreitenbeschränkung auf die GIN Bandbreite.

Internet über privaten Anbieter

Selbstverständlich ist die Internetanbindung über einen privaten Anbieter möglich, wodurch Sie in den Genuss einer höheren Bandbreite kommen. Allerdings ist zu bedenken, dass Ihre Ordination netzwerkmäßig umgebaut (Kosten) und die Trennung zwischen Ordinationsbe-



reich und öffentlichem Bereich (Internetzugriff) korrekt ausgeführt werden muss. Das kann nur durch einen Dienstleister geschehen, der Ihnen die korrekte Ausführung im Sinne des DSGVO bestätigen muss.

Datensicherheit bei Tablet, Smartphone & Co

So sehr in manchen Fällen ein bequemer Zugriff auf Patientendaten wünschenswert ist, sollten Sie doch eine Reihe von Gesichtspunkten berücksichtigen:

- Der Zugriff von mobilen Geräten aus erfolgt im Allgemeinen drahtlos, ein Mithören ist technisch leicht machbar (siehe Kapitel WLAN).
- Am mobilen Gerät können lokale Daten zurückbleiben. Das ist problematisch bei der Benutzung durch mehrere Personen (Familie) oder bei Weitergabe oder Diebstahl des Geräts. Eine Abhilfe bietet hier eine benutzerbezogene Festplattenverschlüsselung.
- Können Sie garantieren, dass keine unerwünschten Apps mitlesen und die Daten im Internet gespeichert und verwendet werden?

Praxistipps:

- Schließen Sie mit allen Dienstleistern, die Zugriff auf Ihr System haben, entsprechende Dienstleistungsverträge ab, die auch die Verschwiegenheitspflicht nach DSGVO 2000 beinhalten
- Stellen Sie sicher, dass bei Datenweitergabe an Dritte alle gesetzlich vorgesehenen Maßnahmen eingehalten werden und lassen Sie sich diese Einhaltung schriftlich bestätigen
- Regeln Sie die Behandlung von Papierdokumenten schriftlich in den Verträgen mit Ihren Mitarbeitern
- Setzen Sie drahtlose Netzwerke nur dann ein, falls Sie sie unbedingt benötigen. Sie stellen eine kaum zu kontrollierende Möglichkeit dar, auf Patientendaten zuzugreifen
- Falls Sie Internet verwenden, ist das Internet per Peeringpoint das sicherste
- Der Zugriff von mobile Geräten aus auf Patientendaten ist derzeit als potentiell unsicher zu bewerten