

Auszüge, Herausstellungen und Kommentierung durch InfoPresent e.K.

## Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis\*

### 5.3 Externe elektronische Kommunikation

Die sicherste Möglichkeit, Patientendaten zu schützen, ist es,

- den Rechner mit Patientendaten von dem Rechner zu trennen, über den die Internetverbindung hergestellt werden soll (sog. Standalone-Gerät).

**Kommentar.** Durch Einsatz der QP Toolbar läuft die komplette Praxisverwaltung auf einem externen verschlüsseltem USB-Laufwerk, welches nach Beenden des Praxisprogramms vom PC physisch getrennt werden kann.

- Soweit eine Verbindung mit dem Praxisrechner erfolgt, sollten die Patientendaten auf dem Praxiscomputer verschlüsselt gespeichert und eine hochwertige, regelmäßig gewartete und aktualisierte Firewall verwendet werden.

**Kommentar:** Durch Einsatz der QP Toolbar wird die Praxis-EDV auf einem externen Laufwerk betrieben und ist dort mit AES 256 Bit verschlüsselt. Sicheres Passwort wird durch den Arzt eingegeben. Als Firewall kann u.a. Zonealarm genutzt werden.

Auf diese Weise kann verhindert werden, dass Dritte unbemerkt eine Verbindung aufbauen, Schaden stiftende Programme in dem Praxiscomputer installieren und/oder den Datenbestand ausspähen, verändern oder löschen. Es wird empfohlen, den in der Anlage (vgl. Kapitel 3 der Technischen Anlage) dargestellten technischen Vorgaben zu folgen. Kann dies nicht sichergestellt werden, so sind Patientendaten auf einem Praxiscomputer zu speichern, der über keinen Internetanschluss verfügt.

- Übermittelt der Arzt Dokumente über ein öffentliches Datennetz (Internet), so sollte er sicherstellen, dass der Zugriff Unbefugter auf die Dokumente ausgeschlossen ist. Die zu übermittelnden Daten müssen daher durch ein hinreichend sicheres Verfahren verschlüsselt werden (vgl. Kapitel 5 der Technischen Anlage).

**Kommentar:** Die Verbindung beider Rechner zur Realisierung der interaktiven Schulung und des Helpdesks erfolgt über eine 256-Bit AES Verschlüsselung über das Internet. Ein zertifiziertes Sicherheitsprotokoll über alle durchgeführten Aktionen wird erstellt und steht dem Praxisinhaber nach Sitzungsende zur Verfügung.

Zusätzlich wird das Training entweder nur auf dem Rechner von InfoPresent durchgeführt oder auf einer zweiten Installation des Praxisverwaltungsprogramms auf dem Praxisrechner mit Musterpatienten.

- .....

### 6. Weitere Grundsätze beim Einsatz von EDV in der Arztpraxis

Der Einsatz von EDV-Technik in der Praxis des niedergelassenen Arztes erfordert nicht nur die Beachtung der aufgezeigten rechtlichen Rahmenbedingungen, sondern macht es auch erforderlich, dass der organisatorische Ablauf den Besonderheiten des Einsatzes dieses Mediums Rechnung trägt. Auch durch die Beachtung dieser organisatorischen Hinweise kann dazu beigetragen werden, den in § 10 Abs. 5 der MBO aufgestellten Anforderungen Genüge zu tun. Im Einzelnen sollte der Arzt Folgendes beachten:

- Zur Sicherung der Patientendaten sind täglich Sicherungskopien auf

geeigneten externen Medien zu erstellen.

- .....
- Die (Fern-)Wartung von EDV-Systemen in Arztpraxen ist dann zulässig, wenn das System die Möglichkeit bietet, dass die einzelnen Maßnahmen durch den Arzt autorisiert und überwacht werden können. Es handelt sich hierbei um eine Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch Externe gem. § 11 Abs. 5 BDSG. Dabei sind die für die Datenverarbeitung im Auftrag geltenden Grundsätze gem. § 11 Abs. 1 bis Abs. 4 BDSG zu beachten.  
**Kommentar:** Der Praxisinhaber muss jede Instanz der Zugriffsart auf seinen Rechner bestätigen oder untersagen durch Drücken eines Buttons. Er legt fest, ob nur auf dem Rechner von InfoPresent oder auch auf seinem PC trainiert oder gewartet wird. Darüber hinaus ist der Arzt der zu Trainierende und damit ob seiner ständigen Anwesenheit vor dem PC in der Lage, eine umfassende Überwachung durchzuführen.
- Der Arzt ist weiterhin für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Er hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Er hat sich also vor der Auftragserteilung zu vergewissern, dass der Auftragnehmer in der Lage und Willens ist, die erforderlichen Sicherungsmaßnahmen auszuführen. In dem schriftlich abzuschließenden Auftragsverhältnis müssen sich der Auftragnehmer und seine Mitarbeiter zur Verschwiegenheit verpflichten. Die im Rahmen der (Fern-) Wartung durchgeführten Maßnahmen sowie der Name der Wartungsperson sind zu protokollieren (vgl. Kapitel 10 der Technischen Anlage).  
**Kommentar:** Der Helpdesk ist als Serviceleistung im Rahmen der VIP-Hotline Bestandteil der QP Toolbar. Die jährliche Lizenz wird auf Basis eines Vertrages vergeben. Zusätzlich erhält der Praxisinhaber nach jeder Trainings- und Helpdesk-Sitzung eine Patientendatenschutzerklärung und das zertifizierte Sicherheitsprotokoll und das Helpdeskprotokoll wird ihm zugänglich gemacht.
- .....
- Auszumusternde Datenträger müssen unter Beachtung des Datenschutzes (z. B. durch mehrfaches Überschreiben mittels geeigneter Software) fachgerecht unbrauchbar gemacht werden.  
**Kommentar:** Die QP Toolbar enthält ein Software-Modul zum sicheren Löschen von Dateien und Verzeichnissen nach 7 Verfahren (höchste Sicherheit: Gutman-Verfahren) und die Möglichkeit, freien Speicherplatz mehrfach zu überschreiben.
- .....
- Der Arzt sollte beim Abschluss von EDV-Verträgen und in jedem einzelnen Wartungs- oder Reparaturfall darauf achten, dass die genannten Vorschriften eingehalten werden.  
**Kommentar:** Die Voraussetzungen dazu sind mit vorstehenden technisch-organisatorischen Maßnahmen geschaffen.

Kommentierung: InfoPresent e. K., Helpdesk - Betreiber für psychotherapeutische Praxen