

## **Aktion „Datenschutz in der Arztpraxis“**

### **Selbst-Check**

#### **Empfang**

- Ist sichergestellt, dass der Zutritt zur Praxis nicht unbeaufsichtigt geschieht?
- Wird durch eine ausreichende Diskretionszone, durch organisatorische Maßnahmen und eine entsprechende Gestaltung der Abläufe in der Praxis sichergestellt, dass die Patientinnen und Patienten ihre Anliegen schildern können, ohne dass neugierige Ohren mithören können?
- Werden die Daten der Patientinnen und Patienten (Anschrift, Kassenart, Grund des Besuchs...) so erhoben, dass Unbefugte sie nicht zur Kenntnis nehmen können?
- Kann das Personal Telefongespräche führen, ohne dass zwangsläufig wartende Patientinnen und Patienten dadurch von Daten anderer Personen Kenntnis erlangen?
- Sind Telefaxgeräte und Bildschirme so aufgestellt, dass diese nicht von Unbefugten eingesehen werden können?
- Wird die Patientin bzw. der Patient darauf hingewiesen, dass er einen Anamnesebogen auf freiwilliger Basis individuell ausfüllen kann? Gibt es in Ihrer Praxis einen gesonderten Bereich, wo dieser Bogen ohne Störungen durch andere ausgefüllt werden kann?

#### **Wartebereich**

- Ist der Wartebereich vom Empfang und dem Behandlungsbereich so getrennt, dass wartende Patientinnen und Patienten keine Informationen über andere Patientinnen und Patienten aufnehmen können?

#### **Behandlungsbereich**

- Können Behandlungsräume so abgeschottet werden, dass neugierige Augen und Ohren ausgeschlossen werden?
- Erfolgen vertrauliche Patienten-Gespräche in geschlossenen Räumen?

- Sind Patientendaten in den Behandlungsräumen gegen unbefugte Kenntnisnahme geschützt? Werden Unterlagen vorhergehender Behandlungen sofort an das Vorzimmer/an die Ablage zurückgegeben?

### **Patientenrechte**

- Werden Patientinnen und Patienten auf Wunsch über die Schweigepflicht der Ärzte, Zahnärzte und Psychotherapeuten und ihre Datenschutzrechte informiert?
- Sind Sie darauf vorbereitet, was zu veranlassen ist, wenn eine Patientin/ein Patient von seinem Recht auf Einsicht in die objektiven Aufzeichnungen zu seiner Person Gebrauch macht und/oder Kopien aus der Patientenakte verlangt?
- Wie ist sichergestellt, dass Patientendaten spätestens nach 30 Jahren gelöscht werden?

### **EDV**

- Ist der Zugang zum Computer durch ein Passwort geschützt?
- Ist das Passwort vor fremdem Zugriff geschützt (kein Zettel unter Tastatur, am Bildschirm usw.)?
- Entspricht das Passwort dem aktuellen Sicherheitsstandard (8 Stellen, bestehend aus Buchstaben, Zahlen und Sonderzeichen)?
- Ist vorgesehen, dass das Passwort nach einer gewissen Zeit geändert werden muss (Alterung)?
- Kennt nur das befugte Personal dieses Passwort?
- Wird ein passwortgeschützter Bildschirmschoner mit kurzer Aktivierungszeit eingesetzt?
- Sind Computer mit Patientendaten, die mit dem Internet verbunden sind, ausreichend geschützt? Ist eine Firewall installiert? Gibt es auf dem Rechner eine Virenprüfung und wird ein regelmäßiges, möglichst tägliches Update des Virencanners durchgeführt?
- Wird regelmäßig eine Sicherungskopie der Daten gefertigt (möglichst jeden Tag, mindestens einmal die Woche)?
- Wird das Patientengeheimnis beachtet, wenn Systemverwaltung und Wartung der EDV durch externe Stellen erfolgt (siehe auch Mitteilung in: Deutsches Ärzteblatt 93, Heft 43, 25.10.1996 –91, A-2809 ff.)?

## **Datenübermittlung**

- Achten Sie darauf, dass bei der Übermittlung von Patientendaten die Empfänger nicht mehr Informationen erhalten, als diese zur Erfüllung ihrer spezifischen Aufgaben benötigen?
- Prüfen Sie, bevor Sie Anfragen von Dritten direkt beantworten, ob die Auskünfte, Berichte oder Bescheinigungen nicht auch über die Patientin/den Patienten schriftlich weitergegeben werden können?
- Achten Sie darauf, dass Privatärztliche Verrechnungsstellen nur dann rechtswirksam beauftragt werden können, wenn die Patientin bzw. der Patient zuvor schriftlich eingewilligt hat?
- Können Sie gesetzlich Krankenversicherten auf Anfrage Auskunft geben, welche Daten für welche Zwecke an die Kassenärztliche Vereinigung weitergegeben werden?
- Informieren Sie die Patientinnen und Patienten über mit- und nachbehandelnde Ärzte (auch Laborärzte) und holen Sie zumindest mündlich von Ihren Patientinnen und Patienten die Einwilligung in die Weitergabe von Daten ein?<sup>1</sup>
- Vergewissern Sie sich bei Anforderung von Patientenunterlagen durch vor-, mit- und nachbehandelnde Ärzte, Zahnärzte und Psychotherapeuten davon, dass diese Anforderung durch eine Einwilligung der Patientin/des Patienten gedeckt ist?
- Haben Sie sichergestellt, dass in Ihrer Praxis bei Zweifeln über die Zulässigkeit vor der Übermittlung von Patientendaten - etwa an den Arbeitgeber - eine rechtliche Klärung erfolgt (z.B. über die Ärzte-/Psychotherapeuten-/Zahnärztekammer, den Landesbeauftragten für den Datenschutz Niedersachsen oder eine Anwältin/einen Anwalt)?

## **Praxisverwaltung**

- Sind Karteikarten und Patientenakten vor dem Zugriff Unbefugter geschützt?
- Werden Karteikarten etc. am Empfang oder in den Behandlungsräumen immer nur so bereit gelegt, dass eine entsprechende Aufsicht gewährleistet ist?
- Sind abschließbare Aktenschränke vorhanden? Werden diese nach Dienstschluss verschlossen?
- Haben Sie Vorkehrungen getroffen, dass Ihre Praxis, insbesondere die Räume, in denen sich Patientendaten/Abrechnungsdaten befinden, ausreichend gegen Einbruch geschützt sind?

---

<sup>1</sup>Bei einer Übermittlung von Patientendaten an die beim Hausarzt geführte zentrale Dokumentation bzw. bei einer Übermittlung aus dieser Dokumentation an Ärzte oder andere Leistungserbringer ist gem. § 73 SGB V sogar eine schriftliche Einwilligung erforderlich.

- Ist sichergestellt, dass das Reinigungspersonal keinen Zugang zu Patientendaten hat, und wird es auf Vertraulichkeit verpflichtet?
- Ist die Aufbewahrung von Altakten sicher organisiert?
- Erfolgt eine sichere Vernichtung von Patientendaten (keine Daten in den Hausmüll)? Werden auch die elektronischen Datenträger sicher gelöscht?
- Wird bei der Versendung von Patientendaten per Fax sichergestellt, dass ausschließlich berechnigte Dritte beim Empfänger Kenntnis von diesem Fax erhalten (z.B. Ankündigung beim Empfänger, regelmäßige Kontrolle von programmierten Nummern)?
- Sind Mitarbeiterinnen und Mitarbeiter über ihre Befugnisse und gesetzlichen Pflichten zur Wahrung des Datengeheimnisses ausreichend (schriftlich) informiert?  
Ein Muster für eine Verpflichtungserklärung zur Wahrung des Datengeheimnisses gem. § 5 BDSG kann im Internetauftritt des Bundesbeauftragten für den Datenschutz – [www.bfd.bund.de/dsvonaz/verpflichtung.pdf](http://www.bfd.bund.de/dsvonaz/verpflichtung.pdf) – heruntergeladen werden.
- Haben Sie einen betrieblichen Datenschutzbeauftragten bestellt? - Eine solche Bestellung ist erforderlich, wenn mindestens fünf Arbeitnehmer automatisiert Patientendaten verarbeiten.

Stand: 15.06.2004