Viele PVS bieten auch die Funktion der Privatabrechnung, Abrechnung nach UV-GOÄ oder von Selbstzahler-Leistungen (IGeL) an, so dass sämtliche anfallenden Leistungen einer Praxis erfasst und abgerechnet werden können.

8.2 Umgang mit (digitalen) Patientendaten

Sämtliche patientenbezogenen Daten und Informationen, vom Arztkontakt über den Gesundheitszustand bis zur Krankengeschichte oder künftige Behandlungen/Therapien, sind vertraulich zu behandeln. Patientendaten dürfen grundsätzlich nur mit Zustimmung des Patienten oder auf gesetzlicher Grundlage weitergegeben werden.

Die Geheimhaltungspflicht besteht gegenüber jedermann, d. h. auch gegenüber Familienangehörigen des Patienten sowie gegenüber Familienangehörigen des Praxisteams (Schweigepflichterklärung!).

Außer allen Praxismitarbeitern sollen auch externe Personen (z.B. EDV-Support-Mitarbeiter), die Zugang zur personenbezogenen Daten haben, und das Reinigungspersonal die Datenschutzregelungen der Praxis kennen und die Datenschutzerklärungen unterschreiben.

Laut Bundesdatenschutzgesetz muss in Praxen mit mehr als neun Mitarbeitern, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ein Datenschutzbeauftragter schriftlich festgelegt werden (§ 4 Beauftragter für den Datenschutz, BDSG). Daten und Aufzeichnungen sind in abschließbaren Schränken in Räumen aufzubewahren, die ausreichend gegen Brand und Diebstahl geschützt sind.

Was bedeutet das für die Praxis?

- Berücksichtigung der datenschutzrechtlichen Vorschriften
- Bestellung eines betrieblichen Datenschutzbeauftragten
- Aus- und Weiterbildung eines Mitarbeiters in der Praxis

Natürlich können diese Verantwortlichkeiten delegiert und extern eingekauft werden.

Anhand einer Datenschutz-Risikoanalyse lassen sich Problemfelder in diesem Bereich mit Handlungsbedarf im eigenen Praxisumfeld erkennen:

- Telefongespräche:
  Patienten im Wartebereich können mithören.
- Gespräche am Empfang:
  Patienten im Wartebereich können mithören.
- Ablage von Rezepten:
  Rezepte können von unberechtigten Personen eingesehen oder gar entwendet werden.
- Ablage von Patientenakten:
  Bei Ablage im Empfangsbereich können Akten entwendet oder eingesehen werden.
- Umgang mit Taxifahrern:
  Taxifahrer erhalten vertrauliche Informationen über Patienten.
- Schreibarbeiten im Empfangsbereich:
  Die Bildschirme können von anwesenden Patienten eingesehen werden.
- Ablage im Archiv:
  Das Archiv wird nicht verschlossen.
- Vernichtung von Daten:
  Daten werden nicht unkenntlich gemacht.
- Unberechtigtes Erfassen von Patientendaten:
  Es wurde unterlassen, die Zustimmung des Patienten einzuholen.

- Datenfernwartung:
  Unberechtigter Zugriff auf vertrauliche Daten.
- Verwendung persönlicher Dateien auf Praxiscomputern:
  Unberechtigte Nutzung von Praxiscomputern.

Achtung: Vorsicht im Umgang mit mobilen Datenträgern wie USB-Sticks, CD-ROM und DVD: Schadsoftware kann in das Praxisverwaltungssystem eingespielt werden und Daten können leicht entwendet werden!

8.2.1 Schutz vor Einsichtnahme und Zugriff

Es ist beim Umgang mit Patientendaten das informelle Selbstbestimmungsrecht des Patienten zu beachten. Unbefugte Dritte dürfen weder im Empfangsbereich noch in den Behandlungsräumen Einblick oder gar Zugriff auf Patientenakten erhalten. Papiergebundene Akten dürfen in keinem Fall so bereitgelegt werden, dass andere Patienten Kenntnis nehmen können. Bildschirme sind so aufzustellen, dass nur Arzt und Praxispersonal diese einsehen können, ggf. sind EDV-Arbeitsplätze auch zu sperren, um die Einsichtnahme durch wartende Patienten zu verhindern.

8.2.2 Aufbewahrungsfristen

Alle ärztlichen Unterlagen sind grundsätzlich für die Dauer von 10 Jahren nach Abschluss der Behandlung aufzubewahren, soweit keine anderen gesetzlichen Regelungen greifen.

Nach Ablauf der Aufbewahrungsfristen sind die Aufzeichnungen mittels eines Aktenvernichters der Sicherheitsstufe 3[26] oder 4 nach DIN 32757 zu vernichten.

[26] Sicherheitsstufe 3 ist empfohlen für vertrauliches Schriftgut und bedeutet bei Streifenschnitt: max. 2 mm Streifenbreite, bei Kreuzschnitt max. 4 mm Breite auf max. 60 mm Partikellänge, aber bei Kunststoffen (wie Identifikationskarten oder Mikrofilm) max. 1 mm² Partikelfläche. Sicherheitsstufe 4 wird für geheim zu haltendes Schriftgut empfohlen und bedeutet bei Kreuzschnitt max. 2 mm Breite auf max. 15 mm Partikellänge, aber bei Kunststoffen (wie Identifikationskarten oder Mikrofilm) max. 0,5 mm² Partikelfläche.