21 Informationssicherheit und Datenschutz

Qualitätsmanagement-Richtlinie

§ 3 Grundelemente
- Informationssicherheit und Datenschutz

Die Felder Datenschutz und Informationssicherheit werden gerne sofort mit Computern und technischen Systemen assoziiert. Dies ist in der Regel richtig, allerdings gibt es in der Vertragspraxis Informationen und Daten, die nicht technisch transportiert, bereitgestellt oder gelagert werden. Denken Sie nur an das zu schützende Gespräch mit dem Patienten oder dessen Karteikarte. Deshalb sollten Sie bei Informationssicherheit und Datenschutz neben den digitalen Daten und Systemen auch die „herkömmlichen" bzw. analogen Daten und Systeme im Blick haben. Eine sehr gute Problemanalyse gibt der KBV-Selbstcheck „Mein Praxis-Check – Informationssicherheit" auf www.kbv.de.

Für den Datenschutz und die Informationssicherheit gibt es gesetzliche Grundlagen, bereichsspezifische Gesetze und Empfehlungen. Diese sind u. a. im Bundesdatenschutzgesetz (BDSG), den Datenschutzgesetzen der Länder, dem Strafgesetzbuch (StGB), dem Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten, der Musterberufsordnung (MBO) sowie den Empfehlungen der Bundesärztekammer zur Schweigepflicht, Datenschutz und Datenverarbeitung geregelt.

Unter Informationssicherheit bezeichnet man die Sicherheit von informationsverarbeitenden und -lagernden (technischen oder nicht-technischen) Systemen zur Gewährleistung der Verfügbarkeit und Vertraulichkeit. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, insbesondere Systemausfall (Festplattenschaden oder Brand im Aktenraum), Systemmissbrauch (digitaler oder analoger Datendiebstahl) und Sabotage.

Folgende Punkte müssen in der Arztpraxis geregelt werden:

- Beachtung der Grundsätze der ärztlichen Schweigepflicht (Umfang, Einschränkungen, www.bundesaerztekammer.de/richtlinien/empfehlungenstellungnahmen/schweigepflichtdatenschutz)
- Regelung der ärztlichen Dokumentation (Art und Umfang, Einsichtnahme durch Patienten, Aufbewahrungspflichten)
- Einsatz und Schulung eines betrieblichen Datenschutzbeauf-

tragten, wenn mehr als neun Mitarbeiter regelmäßig mit Praxisdaten umgehen
- Information aller Mitarbeiter über die Schweigepflicht und über die Datenschutzbestimmungen (bei Neueinstellung, schriftliche Dokumentation erforderlich, eine regelmäßig Auffrischung durchzuführen – z. B. jährlich – ist ratsam)
- Regelung interner Vorgaben zum Datenschutz und zur Datenübermittlung (EDV, Sicherungsmedien, Post, Telefon, Fax, E-Mail)
- Schutz der PC und Monitore vor Zugriff von Dritten (z. B. Sichtschutz vor Dritten, Passwortregelungen, Passwortsicherheit von mind. 8 Stellen, Passwortänderungen, Bildschirmschoner mit kurzer Aktivierungszeit)
- Schutz von Karteikarten oder patientenbezogenen Daten (Befunde, Briefe, sonstige Dokumente) in abschließbaren Schränken
- Sicherung von elektronischen Daten in regelmäßigen Abständen (z. B. Tag, Woche, Monat, Quartal) und Schutz vor Einbruch und Feuer
- Überwachung der Diskretion an der Patientenrezeption (Diskretionszone)
- Überwachung der Diskretion beim Telefonieren und Sprechen (Empfang, Wartebereich, Sprechzimmer und Behandlungsräume)
- Regelung des Zugriffs- und Einsichtsrechts von Dritten auf die Praxisdaten
- Löschung und Vernichtung von personenbezogenen Daten (Schredder etc.)
- Kontrolle der Einhaltung der Datenschutzbestimmungen und praxisinternen Regelungen

Im Rahmen von Teambesprechungen können diese Punkte besprochen und in Form verbindlicher und schriftlicher Regelungen dokumentiert werden. Die Einhaltung ist für das gesamte Team verbindlich. Dies wird regelmäßig geprüft. Hierzu bieten die Ärztekammern regelmäßig Fortbildungen an.

„KPQM schützt vor Gefahren.“