

Organisationen des EDV-Einsatzes in der Arztpraxis

Technische und organisatorische Maßnahmen nach § 9 BDSG

- 3.1 Zugangskontrolle
- 3.2 Datenträgerkontrolle
- 3.3 Speicherkontrolle
- 3.4 Benutzerkontrolle
- 3.5 Zugriffskontrolle
- 3.6 Übermittlungskontrolle
- 3.7 Eingabekontrolle
- 3.8 Auftragskontrolle
- 3.9 Transportkontrolle
- 3.10 Organisationskontrolle

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 § 15 Abs. 4 der MBO aufgestellten Anforderungen Genüge zu tun. Im einzelnen sollte der Arzt folgendes beachten: Der Arzt muß während der vorgeschriebenen Aufbewahrungsfristen (in der Regel zehn Jahre - § 15 Abs. 1 MBO) in der Lage sein, auch nach einem Wechsel des EDV-Systems oder der Programme innerhalb angemessener Zeit die EDV-mäßig dokumentierten Informationen lesbar und verfügbar zu machen.

Die Wartung einer EDV-Anlage oder jeglicher Fehlerbeseitigung vor Ort darf grundsätzlich nur mit Testdaten erfolgen. Im Notfall, z. B. bei Systemstillstand in einer spezifischen Patientendatenkonstellation, muß der Einblick Dritter in Originaldaten auf besondere Ausnahmefälle eingeschränkt bleiben. Das Wartungspersonal ist zu beaufsichtigen und schriftlich auf die Verschwiegenheit zu verpflichten. Die durchgeführten Maßnahmen sowie der Name der Wartungsperson sind zu protokollieren.

Die Fernwartung von EDV-Systemen in Arztpraxen ist unzulässig, wenn nicht auszuschließen ist, daß dabei auf patientenbezogene Daten zugegriffen werden kann.

Bei Datenträgern für befugte Dritte ist ein sicherer Transport zu gewährleisten.

Die Datenfernübertragung personenbezogener Daten per Leitung muß chiffriert erfolgen.

Auszumusternde Datenträger müssen unter Aufsicht des Arztes (z. B. durch mehrfaches Überschreiben mittels geeigneter Software) unbrauchbar gemacht werden.

Der Arzt sollte beim Abschluß von EDV-Verträgen und in jedem einzelnen Wartungs- oder Reparaturfall darauf achten, daß die genannten Vorschriften eingehalten werden.

Technische und organisatorische Maßnahmen nach § 9 BDSG

Das Vertrauen in eine auf elektronischen Datenträgern erstellte medizinische Dokumentation wird auch dadurch erhöht, daß der Arzt die in § 9 BDSG und in der Anlage zu § 9 Satz 1 BDSG entwickelten Grundsätze beachtet. Unter Beachtung dieser technischen und organisatorischen Vorgaben kann sichergestellt werden, daß der Arzt nicht Gefahr läuft, die ärztliche Schweigepflicht zu verletzen.

3.1 Zugangskontrolle

Durch die Zugangskontrolle soll Unbefugten der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt werden. Der Praxisbetrieb ist daher so zu gestalten, daß der Zugang wirksam verhindert wird. Dies kann bereits durch einfache Mittel erreicht werden. Es sollte z. B. sichergestellt werden, daß Patienten, z. B. im Empfangsbereich, aber auch in den einzelnen Behandlungsräumen, nicht ungewollt Zugang zu fremden Patientendaten haben. Dieses kann dadurch erreicht werden, daß die Bildschirme so angeordnet werden, daß sie nicht im Blickfeld des Patienten sind oder aber daß der Praxiscomputer mit einem "Sleeper" versehen ist, der seinerseits paßwortgeschützt sein sollte.

3.2 Datenträgerkontrolle

Datenträgerkontrolle soll verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dazu sollten bewegliche Datenträger, wie Disketten, Magnetbänder, Wechselplatten oder CDs sicher aufbewahrt werden, aus Gründen der Datensicherheit möglichst nicht in der Praxis

selbst. Um Workstations unterbinden, sollten alle Workstations oder PCs außer dem Hauptserver kein Diskettenlaufwerk besitzen, zumindest aber sollte dieses von außen verkleidet, abgeschlossen oder durch Software (z. B. BIOS-Setup) deaktiviert sein. Auszumusternde Datenträger müssen unter Aufsicht des Arztes unbrauchbar gemacht werden. Darüber hinaus kann die Datenträgerkontrolle dadurch erhöht werden, daß eine Inventarisierung vorgenommen wird.

3.3 Speicherkontrolle

Die Speicherkontrolle soll sicherstellen, daß die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten verhindert wird. Dies ist üblicherweise Aufgabe einer entsprechend zuverlässigen Zugriffskontrolle, wie sie in vielen Betriebssystemen angeboten wird. Die im Speicher befindlichen Daten sollten nur von der Anwendung aus zugreifbar, d. h. lesbar, veränderbar oder löscherbar, sein. Außerhalb der Anwendung sollen die Daten gar nicht oder nur in chiffrierter Form einsehbar sein. Innerhalb der Anwendung sollten bestimmte Daten durch Paßwörter geschützt sein, ebenso wie der Zugriff auf die Anwendung selbst. Ebenfalls ist es sinnvoll, wenn bei der Inbetriebnahme des Rechners sofort die Anwendung (PraxisSoftware) gestartet wird, es also für den "normalen" Nutzer gar keine Möglichkeit gibt, ins Betriebssystem zu gelangen und dort zu arbeiten. Wird der Arbeitsplatz verlassen bzw. wird keine Taste betätigt, sollte nach kurzer Zeit ein paßwortgeschützter Bildschirmschoner aktiviert werden. So kann sichergestellt werden, daß Daten, die gerade auf einer Bildschirmmaske angezeigt werden, nicht von anderen Patienten eingesehen werden können.

3.4 Benutzerkontrolle

Die Benutzerkontrolle soll verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können. Eine Verbindung des Praxiscomputersystems zur "Außenwelt" ist nur dann zu halten, wenn wirklich Daten übertragen werden, es sollte also keine ständige Leitung vorhanden sein. Der Zugang von außen darf nur dann ermöglicht werden, wenn patientenbezogene Daten geschützt sind. Alle Aktivitäten, die im Zusammenhang mit Datenfernübertragung stehen, sollten protokolliert werden.

3.5 Zugriffskontrolle

Mit der Funktion der Zugriffskontrolle soll gewährleistet werden, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Zu diesem Zweck sollten die berechtigten Personen über Zugriffskontrollmechanismen (z. B. Paßwörter) legitimiert werden. Erzwungene häufige Änderungen des Paßwortes sind nicht ratsam, da dies dazu führt, daß Paßwörter notiert werden.

3.6 Übermittlungskontrolle

Die Übermittlungskontrolle soll gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können. Zu diesem Zweck sollte ein Sendeprotokoll erstellt werden, das die Art der übermittelten Daten und den Status der Sendung (z. B. erfolgreich oder gestört) beinhalten soll. Werden zur Datenübertragung öffentliche Leitungen genutzt, sollten personenbezogene Daten grundsätzlich chiffriert werden.

3.7 Eingabekontrolle

Durch eine Eingabekontrolle soll sichergestellt werden, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem im Datenverarbeitungssystem eingegeben worden sind. Um dieses zu erfüllen, müßte jede Aktivität eines Benutzers in ein von keinem Benutzer oder Supervisor veränderbares Protokoll geschrieben werden. Dieses bedeutet einen erheblichen technischen Aufwand. Ein umfassender Schutz ist zur Zeit gar nicht oder schwer technisch realisierbar und in der Regel nicht in der Praxis-Hardware und PraxisSoftware enthalten. Allerdings kann eine solche aufwendige Eingabekontrolle dazu beitragen, daß der Beweiswert und die Beweissicherheit von elektronischer Dokumentation erhöht werden. Dem gleichen Zwecke kann auch die sogenannte elektronische Signatur dienen, die allerdings ebenfalls heute noch nicht mit angeboten wird.

3.8 Auftragskontrolle

Auftragskontrolle soll gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Der Auftraggeber muß sich versichern, daß der Auftragnehmer alle Anforderungen hinsichtlich der technischen und organisatorischen Maßnahmen nach § 9 BDSG erfüllt.

3.9 Transportkontrolle

Durch Transportkontrollen soll verhindert werden, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Auf dem Datenträger gespeicherte personenbezogene Daten sollten verschlüsselt sein. Bei der Versendung solcher Daten soll also eine geeignete Verpackung für die Datenträger verwendet werden. Sichere Versandformen sind ratsam.

3.10 Organisationskontrolle

Organisationskontrolle bedeutet, daß die innerbetriebliche Organisation so gestaltet wird, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dieses kann dadurch realisiert werden, daß, soweit es erforderlich ist, gemäß § 36 BDSG auch in Arztpraxen ein Beauftragter für den Datenschutz bestellt wird. Darüber hinaus sind alle Mitarbeiter zur Wahrung der ärztlichen Schweigepflicht schriftlich zu verpflichten. Diese doch in Arztpraxen bereits übliche Verpflichtung zur Einhaltung der Schweigepflicht sollte auf die Einhaltung des Datengeheimnisses erstreckt werden.