MANAGEMENT& KRANKENHAUS 11.95

MONATLICHER INFORMATIONSDIENST FÜR ALLE FÜHRUNGSKRÄFTE IM GESUNDHEITSWESEN

# Datenschutz muß Schritt halten

Der Einsatz der elektronischen Datenverarbeitung (EDV) im Krankenhaus zur Unterstützung von Informations-, Kommunikations- und Dokumentationsprozessen schreitet seit Anfang der siebziger Jahre voran. War in der Anfangsphase der Verwaltungsbereich von der EDV-Einführung betroffen, werden in jüngster Zeit in den Leistungsbereichen und auch im Pflegebereich Computer eingesetzt. Die Bestrebungen gehen dahin, bestehende „Insellösungen" miteinander zu einem sogenannten Krankenhaus-

Bruno Schierbaum

kommunikations- und Informationssystem (KIS) zu verbinden. Ein KIS zeichnet sich u.a. durch folgende Merkmale aus:

- modularer Aufbau
- Dialogverarbeitung
- zentrale patientenbezogene Datenbank
- einmalige Erfassung der Daten am Entstehungsort
- differenzierte Vergabe der Zugriffsberechtigungen

Diese Entwicklung bringt es mit sich, daß zunehmend personenbezogene Daten der Patieten aber auch der Beschäftigten per EDV gespeichert und verarbeitet werden. So ist folglich dem Datenschutz im Krankenhaus ein hoher Stellenwert beizumessen.

Fortsetzung auf Seite 12

Fortsetzung von Seite 1

# Datenschutz muß Schritt halten

### Datenschutz heißt Schutz der Persönlichkeitsrechte

Läßt man sich von dem Begriff „Datenschutz" leiten, wird man leicht in die Irre geführt. Bei der rechtlichen Regelung des Datenschutzes geht es nicht um den Schutz der Daten als solche, sondern es geht vielmehr um den Schutz der Persönlichkeitsrechte des Betroffenen. Grundlegend in diesem Zusammenhang ist das Urteil des Bundesverfassungsgerichtes (BVerfG, Urteil v. 15.12.1983 NJW 1984, S. 419 ff.). Das Gericht hat aus Art. 1 Abs. 1 und Art. 2 Abs. 1 GG ein Recht jedes einzelnen auf informationelle Selbstbestimmung abgeleitet. Dieses Grundrecht gewährleistet die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Soll dieses Recht auf informationelle Selbstbestimmung eingeschränkt werden, bedarf es einer gesetzlichen Regelung. Entsprechende Regelungen sind u. a. die einschlägigen Datenschutzgesetze.

### Welches Datenschutzrecht ist im Krankenhaus anwendbar?

Neben den Datenschutzgesetzen ist für die Krankenhäuser der § 203 Abs. 1 StGB (Verletzung von Privatgeheimnissen) in Verbindung mit dem § 3 der Berufsordnung für die deutschen Ärzte (vgl. Deutsches Ärzteblatt 1-2/94, S. B-39) von Bedeutung. Welches Datenschutzrecht für das einzelne Krankenhaus anzuwenden ist, hängt von der geographischen Lage und von der Trägerschaft des Krankenhauses ab. So ist der Datenschutz in speziellen Krankenhausdatenschutzgesetzen (z. B. in Bremen) und in Landeskrankenhausgesetzen (z. B. Bayern, Berlin, Saarland) verankert.

In bezug auf die Trägerschaft gilt für Krankenhäuser, deren Träger der Bund oder eine bundesunmittelbare Körperschaft ist, der 2. Abschnitt des Bundesdatenschutzgesetzes (BDSG). Für Krankenhäuser, die von öffentlich-rechtlichen Religionsgemeinschaften oder diesen gleichgestellen oder ihnen zugeordneten Trägern betrieben werden, gelten die entsprechenden Datenschutzgesetze der Amtskirchen.

Ist der Krankenhausträger eine Einrichtung der Sozialversicherung im Sinne des § 35 SGB I, so unterliegt der Schutz der Patientendaten als Sozialdaten gemäß § 79 Abs. 2 SGB X dem 1. und 2. Abschnitt des BDSG, wobei zudem ein betrieblicher Datenschutzbeauftragter gemäß § 36 BDSG zu bestellen ist.

Im übrigen kommt für Krankenhäuser in öffentlich-rechtlicher Trägerschaft außerhalb des Bundes (Stadt, Gemeinde, Gemeindeverband, Kreis, Land) grundsätzlich das jeweilige Landesdatenschutzgesetz zur Anwendung. Da aber alle Landesdatenschutzgesetze für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen - hierzu gehören auch Krankenhäuser - entweder auf die §§ 28, 33 - 36 BDSG oder direkt auf den 3. Abschnitt des BDSG verweisen, sind diese weitgehend aus den Regelungen der Landesdatenschutzgesetze herausgenommen. Somit gelten für diese öffentlich-rechtlichen Wettbewerbsunternehmen im Prinzip die gleichen Datenschutzvorschriften wie für Privatbetriebe.

### Zulässigkeit der Verarbeitung und Nutzung von Daten

Da in vielen Krankenhäusern das BDSG zur Anwendung kommt, soll insbesondere auf den dritten Abschnitt des BDSG näher eingegangen werden. Voraussetzung für die Anwendung des BDSG ist die Verarbeitung personenbezogener Daten in oder aus Dateien. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (vgl. § 3 Abs. 1 BDSG). Unter personenbezogenen Daten sind alle Informationen zu fassen, die etwas über eine Person aussagen. Eine Datei ist eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren ausgewertet werden kann (vgl. § 3 Abs. 2 BDSG).

Ist die Voraussetzung der dateimäßigen Verarbeitung personenbezogener Daten gegeben, muß das BDSG angewandt werden und somit für jedes personenbezogene Datum eine Zulässigkeitsprüfung vorgenommen werden. Das BDSG geht nach § 4 Abs. 1 von einem grundsätzlichen Verbot mit Erlaubnisvorbehalt in bezug auf die Verarbeitung und Nutzung personenbezogener Daten aus. Das bedeutet, daß die Verarbeitung personenbezogener Daten in den einzelnen Verarbeitungsphasen nur dann zulässig ist, wenn

- eine andere Rechtsvorschrift dieses anordnet oder erlaubt,
- das BDSG selbst dieses erlaubt oder
- der Betroffene eingewilligt hat.

Wenn eine Rechtsvorschrift die Verarbeitung und Nutzung personenbezogener Daten ausdrücklich erlaubt oder sogar anordnet, kommt es auf die Einwilligung des Betroffenen oder auf die Regelungen des BDSG nicht an. Es muß sich dabei aber um Rechtsnormen wie Gesetze, Rechtsverordnungen, autonome Satzungen, den normativen Teil von Betriebs- oder Dienstvereinbarungen oder Sprüchen von Einigungsstellen handeln.

Soll die Einwilligung des Betroffenen die Rechtsgrundlage für die Datenverarbeitung bilden, so ist folgendes zu beachten. Die Einwilligung

- muß der Speicherung vorausgehen,
- bedarf der Schriftform,
- muß hinreichend bestimmt sein und
- vom Betroffenen persönlich abgegeben werden.

Bildet das BDSG die Rechtsgrundlage, sind die Vorschriften des § 28 BDSG zu beachten. Danach darf eine Verarbeitung und Nutzung personenbezogener Daten im Rahmen der Zweckbindung eines Vertragverhältnisses oder vertragsähnlichen Vertrauensverhältnisses erfolgen. Es dürfen nur die Daten verarbeitet werden, die unbedingt zur Durchführung und Abwicklung des Vertragsverhältnisses erforderlich sind. Zudem ist eine Interessensabwägung in bezug auf die berechtigten Interessen der speichernden Stelle und den schutzwürdigen Interessen des Betroffenen vorzunehmen, wobei die Interessen gleichberechtigt nebeneinander stehen.

### Technisch-organisatorische Maßnahmen

Nach § 9 BDSG müssen Betriebe, die personenbezogene Daten verarbeiten, technisch-organisatorische Maßnahmen zum Datenschutz treffen. In § 9 BDSG und der Anlage zu § 9 werden die Anforderungen an die Datenschutzmaßnahmen umschrieben: „Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind die Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

Das Prinzip der Verhältnismäßigkeit bezieht sich nicht auf die Frage, ob die vom Gesetz ausgesprochenen Vorgaben zu beachten sind. Es geht dabei einzig und allein um Art und Umfang der Maßnahmen und nicht darum, ob diese überhaupt umgesetzt werden müssen. Die speichernde Stelle hat in bezug auf die konkreten technischen oder organisatorischen Maßnahmen einen Gestaltungsspielraum.

### Rechte der Betroffenen

Sowohl die Patienten als auch die Beschäftigten haben ein Recht auf

- Benachrichtigung (§ 33 BDSG),
- Auskunft (§ 34 BDSG)
- Berichtigung (§ 35 Abs. 1 BDSG),
- Löschung (§ 35 Abs. 2 BDSG),
- Sperrung (§ 35 Abs. 4 BDSG).

Speichernde Stellen müssen den Betroffenen von der erstmaligen Speicherung in Kenntnis setzen. Die Benachrichtigung, die nicht der Schriftform bedarf, muß die Speicherung selbst und die Art der Daten umfassen. Kommt eine der in § 33 Abs. 2 BDSG genannten Ausnahmen zum Tragen, braucht die Benachrichtigung nicht zu erfolgen. Das zentrale Kontrollrecht bildet das Auskunftsrecht nach § 34 Abs. 1 BDSG. Die Auskunft muß sich grundsätzlich auf alle über den Betroffenen gespeicherten Daten, dem Zweck der Speicherung und die Datenempfänger beziehen, an die regelmäßig Daten übermittelt werden. Die Auskunft muß schriftlich erteilt werden und kostenlos erfolgen. Konsequenterweise steht dem Betroffenen ein Recht auf Berichtigung zu, wenn die gespeicherten Daten unrichtig sind (§ 35 Abs. 1 BDSG). Gelöscht werden müssen Daten u. a. dann, wennn ihre Speicherung unzulässig ist (§ 35 Abs. 2 Nr. 1 BDSG) oder die Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist (§ 35 Abs. 2 Nr. 3 BDSG). Zu Sperren sind die Daten z. B. dann, wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt (§ 35 Abs. 4 BDSG).

### Der betriebliche Datenschutzbeauftragte

Die Umsetzung des Datenschutzes obliegt der Geschäftsleitung, wobei ein zu bestellender betrieblicher Datenschutzbeauftragter hierbei eine zentrale Rolle spielt. Die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht, wenn in der Regel fünf Arbeitnehmer ständig personenbezogene Daten verarbeiten (§ 36 Abs. 1 BDSG). Da Datenverarbeitung lediglich ein Bestandteil der Arbeitsaufgabe der einzelnen Beschäftigten sein muß, ist die Zahl von fünf Personen in den meisten Betrieben erfüllt. Die Person des Datenschutzbeauftragten muß über Zuverlässigkeit und Fachkunde verfügen. Um nicht gegen das Kriterium Zuverlässigkeit zu verstoßen, verbietet es sich z. B. einen Leiter der EDV zum Datenschutzbeauftragten zu bestellen, weil diese Person in Interessenskonflikte gerät. So können Konflikte entstehen, wenn man als EDV-Leiter bestimmte EDV-Projekte möglichst kostengünstig durchführen muß, als Datenschutzbeauftragter möglicherweise Datenschutz- und Datensicherungsmaßnahmen durchsetzen muß, die mit zusätzlichen Kosten verbunden sind.

Der Datenschutzbeauftragte muß neben der Sicherstellung des Datenschutzes Übersichten führen über

- eingesetzte Datenverarbeitungsanlagen,
- Bezeichnung und Art der Dateien,
- Art der gespeicherten Daten
- Geschäftszwecke, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
- deren regelmäßige Empfänger,
- zugriffsberechtigte Personengruppen und Personen, die allein zugriffsberechtigt sind (§ 37 Abs. 2 BDSG).

### Schritte zur Umsetzung des Datenschutzes

Zur Prüfung der aktuellen Situation des Datenschutzes im Krankenhaus kann anhand der folgenden Fragen vorgegangen werden:

- Welches Datenschutzrecht ist anzuwenden?
- Sind aktuelle Kommentare zu den einschlägigen Datenschutzgesetzen vorhanden?
- Verarbeiten mehr als fünf Personen personenbezogene Daten (Patienten- bzw. Mitarbeiterdaten)?
- Ist ein betrieblicher Datenschutzbeauftragter gemäß § 36 Abs. 1 BDSG zu bestellen?
- Wurden alle Mitarbeiter, die personenbezogene Daten verarbeiten, auf das Datengeheimnis verpflichtet?
- Existiert eine Übersicht über die eingesetzte Hardware, Software sowie die Dateien mit personenbezogenen Daten (§ 37 Abs. 2 BDSG)?
- Ist eine Zulässigkeitsprüfung in bezug auf Verarbeitung und Nutzung der personenbezogenen Daten gemäß § 4 BDSG vorgenommen worden?
- Sind die technisch-organisatorischen Maßnahmen gemäß § 9 BDSG umgesetzt worden?

Auf dieser Basis ist für das Krankenhaus ein Datenschutzkonzept zu entwickeln, welches ständig zu überprüfen und auf auf dem aktuellen betrieblichen und gesetzlichen Stand zu halten ist.

### Die zehn Gebote der Personaldatenverarbeitung

Folgende Maßnahmen sind durch das BDSG vorgegeben:

#### Zugangskontrolle

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet werden, zu verwehren.

#### Datenträgerkontrolle

Es ist zu verhindern, daß Datenträger (z. B. Disketten) unbefugt gelesen, kopiert, verändert oder entfernt werden können.

#### Speicherkontrolle

Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten ist zu verhindern.

#### Benutzerkontrolle

Es ist zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können.

#### Zugriffskontrolle

Es ist zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

#### Übermittlungskontrolle

Es ist zu gewährleisten, daß überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.

#### Eingabekontrolle

Es ist zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in Datenverarbeitungssysteme eingegeben worden sind.

#### Auftragskontrolle

Es ist zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

#### Transportkontrolle

Es ist verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

#### Organisationskontrolle

Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird.

*Bruno Schierbaum,*
*BTQ Niedersachsen*
*(Beratungsstelle für Technologiefolgen und Qualifizierung),*
*Donnerschweer Str. 84,*
*26123 Oldenburg,*
*Tel.: (04 41) 8 20 68,*
*Fax: (04 41) 8 38 24*