von **Dr. Sebastian Kraska**

Datenschutz in der Arztpraxis - welche Anforderungen sind an IT-Systeme aus datenschutzrechtlicher Sicht zu stellen?

Personenbezogene Daten über den Gesundheitszustand sind nach dem Bundesdatenschutzgesetz so genannte "besondere Arten personenbezogener Daten". Daher werden an die Verarbeitung dieser Daten besondere datenschutzrechtliche Anforderungen gestellt. Auswirkungen hat dies insbesondere auf die informationstechnische Verarbeitung und Sicherung dieser Daten in Arztpraxen (sowie im übrigen Gesundheitsbereich). Der Beitrag erläutert, warum sich die Einhaltung der datenschutzrechtlichen Vorgaben in der Arztpraxis letztlich auch finanziell auszahlt.

Nach dem Bundesdatenschutzgesetz (BDSG) werden gemäß § 3 Abs. 1 BDSG personenbezogene Daten geschützt, also Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Das BDSG gilt dabei sowohl für Unternehmer (so genannte "nicht-öffentliche Stellen") wie für Behörden (so genannte "öffentliche Stellen"), wobei bei diesen datenschutzrechtlich weiter zu differenzieren ist (Bundes- oder Landesbehörde etc.).

Grundsatz nach dem BDSG: Einwilligung des Betroffenen oder gesetzliche Gestattung nötig

Grundsätzlich ist die Datenerhebung, Verarbeitung und Nutzung soweit zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Für die Verarbeitung personenbezogener Daten in der Arztpraxis ist daher neben den Vorschriften zur Einwilligung besonderes Augenmerk auf die Regelungen des Dritten Abschnitts des BDSG zu legen, da dort das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke geregelt ist.

Gesundheitsdaten: besondere Art personenbezogener Daten nach § 3 Abs. 9 BDSG

Das BDSG lautet in § 3 Abs. 9 BDSG wie folgt:

> *"Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben."*

Damit sind Gesundheitsdaten von Patienten als "besondere Arten personenbezogener Daten" zu verstehen und daher in der Folge einem besonderen datenschutzrechtlichen Schutz zu unterstellen. So bedingt beispielsweise § 4d Abs. 5 Nr. 1 BDSG die Durchführung einer Vorabkontrolle "automatisierte Verarbeitungen", wenn personenbezogene Daten automatisiert verarbeitet werden sollen. § 4a Abs. 3 BDSG stellt für die Einwilligung hinsichtlich besonderer Arten personenbezogener Daten spezielle Voraussetzungen auf.

Für den Bereich der technischen Umsetzung der Datenverarbeitung hebt § 9 BDSG hervor, dass Unternehmen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen haben, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. Erforderlich sind alle Maßnahmen, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Gemäß § 3 Abs. 9 i.V.m. § 4a Abs. 3, § 4d Abs.5 und § 28 Abs. 6 BDSG muss bei Patientendaten immer von einem hohen Schutzbedarf ausgegangen werden.

Gemäß § 1 Abs. 3 S. 2 BDSG bleiben neben dem BDSG die berufsrechtlichen Regelungen unberührt. Die Bewertung der ärztlichen Schweigepflicht per se findet damit auch Einzug in das Datenschutzrecht. Daneben muss bei der Anwendung eines IT-Systems auf die Einhaltung der Grundsätze der Vertraulichkeit, Verfügbarkeit und Integrität der Daten geachtet werden.

An welche Faktoren werden besondere Ansprüche gestellt?

Generell sind vor allem die folgenden datenschutzrechtlichen Belange für eine Arztpraxis relevant:

Zu beachten ist zunächst der datenschutzrechtliche Grundsatz, dass das Speichern, Verändern, Übermitteln und die sonstige Nutzung personenbezogener Daten nur im Rahmen der Zweckbestimmung des Vertragsverhältnisses mit dem Patienten oder zur Wahrung berechtigter Interessen des Arztes bzw. der Behandlungseinrichtung zulässig ist. Auch dies gilt jedoch nur dann, wenn nicht anzunehmen ist, dass das schutzwürdige Interesse des Patienten an dem Ausschluss der Verarbeitung oder der Nutzung überwiegt (siehe insofern § 28 Abs. 6 BDSG).

Einwilligungserklärung: grundsätzlich immer schriftlich

Die datenschutzrechtliche Einwilligungserklärung des Patienten bedarf der Schriftform gemäß § 4a Abs. 1 S. 3 BDSG, wenn nicht wegen besonderer Umstände eine andere Form angemessen ist.

Sicherstellung der technischen und organisatorischen Mittel: was ist nötig?

Der Arzt muss sicherstellen, dass die technischen und organisatorischen Mittel hinsichtlich der zu treffenden Sicherheitsmaßnahmen gemäß § 9 BDSG getroffen werden. Was im Einzelfall als erforderlich zu gelten hat kann erst nach einer Ermittlung der Schutzbedürftigkeit der gespeicherten Daten festgestellt werden. Im Grundsatz sind gemäß der Anlage zu § 9 BDSG insbesondere folgende technischen Vorgaben einzuhalten: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Zweckbindung.

Erforderlich: ordnungsgemäße Datensicherung

Für die erforderliche Datensicherung sind täglich Sicherungskopien zu erstellen. Dafür sind geeignete externe Medien zu verwenden. Die nähere Dokumentation richtet sich nach § 10 MBO, der Muster-Berufsordnung für die deutsche Ärzteschaft. Die Berufsordnung gestattet ausdrücklich auch die elektronische Dokumentation. Die so angefertigten Dokumente müssen zehn Jahre archiviert werden, so dass eine gute Datensicherung eine Grundvoraussetzung darstellt. Während der Archivierungszeit müssen die Dokumente auf Verlangen lesbar und verfügbar sein.

EDV-System muss laufend gewartet werden

Die Benutzung eines EDV-Systems erfordert immerzu eine stetige Wartung. Zu beachten ist, dass die einzelnen Maßnahmen der Wartung durch den Arzt autorisiert und überwacht werden müssen. Insofern handelt es sich, wenn ein Dritter mit der Wartung beauftragt wird, im Grundsatz um eine Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch Externe gem. § 11 Abs. 5 BDSG. Damit müssen die für die Datenverarbeitung im Auftrag geltenden Grundsätze gem. § 11 Abs. 1 bis Abs. 4 BDSG beachtet werden (bitte beachten Sie die weiteren Differenzierungen hinsichtlich jener Bundesländer ohne landesspezifische Regelungen bzgl. § 203 StGB und IT-Outsourcing - in diesen Fällen können noch weitergehende Maßnahmen erforderlich sein). Letztlich ist immer der Arzt für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Dies macht damit stets eine sorgfältige Auswahl des Auftragsnehmers erforderlich.

Zur Gewährleitung der Integrität der Daten: Datenmanagement nötig

Alle im Rahmen der Behandlungsvorgänge gespeicherten Daten müssen den datenerhebenden Personen stets zugeordnet werden können. Die Administrationspflicht wird vom BDSG insoweit an die verarbeitende bzw. verantwortliche Stelle geknüpft. Wer der so genannte "Herr der Daten" ist muss am Einzelfall bestimmt werden, da die Frage insbesondere in Bezug auf Gemeinschaftspraxen nicht immer leicht zu beantworten ist.

Stets Zugangsautorisierung nötig

Zu Grunde zu legen ist eine ernstzunehmende Autorisierungprozedur, damit jegliche Nutzung des IT-Systems kontrolliert werden kann. Dabei dürfen Benutzer des IT-Systems sich nur auf der Applikationsebene und niemals auf der Administrationsebene bewegen können. Wenn eine Autorisierung stattgefunden hat kann die Speicherung von Daten mit Kennung und Datum versehen werden, so dass ein sicheres Datenbankmanagement möglich ist.

Zugriff auf das IT-System muss vertraulich geschehen

Daneben führt der Autorisierungsprozess gleichzeitig zum sicheren Zugriffsmanagement. Nur wenn alle Zugriffsberechtigen registriert sind und über individuelle Zugriffsprofile verfügen, kann ein sicherer Zugang gewährleistet werden.

Datenübertragung: nur im sicheren Netz

Übertragungswege müssen sowohl gegen Datenverluste wie auch gegen Datenverfälschungen und unbefugte Kenntnisnahmen abgesichert werden. Eine Organisation über ein Wireless-Local-Area-Network kann ein Sicherheitsdefizit darstellen. Zudem stellt der unverschlüsselte Versand medizinischer Daten via E-Mail durch Ärzte oder ihre Mitarbeiter ein unverantwortliches Sicherheitsrisiko dar. Daneben ist die Nutzung je nach Verwendung des gewählten Netzmanagements auch gegen Angriffe aus dem Internet als Übertragungsweg zu schützen. Entsprechend ist ein fortgeschrittenes Firewallsystem erforderlich.

Arztpraxis: Datenschutzbeauftragter erforderlich?

Zur Frage der Bestellung eines Datenschutzbeauftragten in der Arztpraxis finden Sie in unserem Artikel **"Datenschutz in der Arztpraxis: brauchen Ärzte einen Datenschutzbeauftragten?"** weitere Informationen.

Fazit

Zur Vermeidung straf- und ordnungsrechtlicher Konsequenzen müssen Ärzte beim Einsatz von EDV-System zur Verarbeitung von Patientendaten zahlreiche datenschutzrechtliche Vorgaben beachten. Letztlich lohnt die Investition in die Informations- und Risikovorsorge: mit einem rechtssicheren Datenschutzkonzept können Ärzte Schwierigkeiten mit Aufsichtsbehörden und Patienten vermeiden sowie die finanziellen Risiken im Fall eines Datenschutzvorfalls minimieren.

Autor:
Dr. Sebastian Kraska
Rechtsanwalt