

# Datenschutz in der Arztpraxis

*Der Datenschutz in Arztpraxen bildet seit einigen Jahren einen Schwerpunkt der Prüftätigkeit des Bayerischen Landesamtes für Datenschutzaufsicht. Im Rahmen ihrer Vor-Ort-Prüfungen in Praxen (Anmerkung der Redaktion: wir berichteten im „Bayerischen Ärzteblatt“ 7-8/2012, Seite 364 f.) weist die Behörde regelmäßig insbesondere auf die folgenden zehn Punkte hin:*

## Auf Sicht- und Hörschutz achten

Praxisräume und Arbeitsabläufe sind so zu organisieren, dass ein unbefugtes Mithören oder Mitlesen von Patientendaten durch Dritte, insbesondere durch wartende Patienten, möglichst ausgeschlossen ist. Dies ist für Ärzte grundsätzlich eine Selbstverständlichkeit. Häufig können aber vergleichsweise einfache Maßnahmen, wie ein anderes Positionieren von Bildschirmen oder das Aufkleben von Sichtschutzfolien, noch Verbesserungen bringen. Zudem sind beispielsweise Sitzgelegenheiten in Hörweite des Empfangs oder das Bereitlegen von Patientenakten auf dem Empfangstresen zu vermeiden.

## Mitarbeiter für Datenschutz sensibilisieren

Von zentraler Bedeutung für einen verlässlichen Datenschutz ist die regelmäßige Schulung und Sensibilisierung der Mitarbeiter für die Erfordernisse eines datenschutzgerechten Umgangs mit Patientendaten. In diesem Zusammenhang ist auch darauf zu achten, dass Mitarbeiter nach § 5 des Bundesdatenschutzgesetzes (BDSG) bei der Aufnahme ihrer Tätigkeit gesondert auf das Datengeheimnis verpflichtet werden. Ein bloßer Passus im Arbeitsvertrag genügt hierfür nicht.

## Datenschutzbeauftragten bestellen

Sind in der Praxis – einschließlich des Arztes – mehr als neun Personen beschäftigt, die personenbezogene Daten verarbeiten, ist nach § 4f Abs. 1 BDSG ein Datenschutzbeauftragter zu bestellen. Diese Aufgabe kann wahlweise einem internen oder einem externen Datenschutzbeauftragten übertragen werden.

## Einwilligung für Verrechnungsstelle einholen

Erfolgt die Abrechnung privatärztlicher Leistungen über eine externe Verrechnungsstelle, bedarf die hierfür erforderliche Datenübermittlung der schriftlichen Einwilligung des Patienten. Dies setzt eine transparente

Information des Patienten voraus. So ist in der Einwilligungserklärung unter anderem ausdrücklich darauf hinzuweisen, dass sich die Einwilligung auch auf Gesundheitsdaten bzw. auf Diagnose- und Behandlungsdaten erstreckt. Erklärt sich ein Patient nicht mit der Abrechnung durch die Verrechnungsstelle einverstanden, ist sicherzustellen, dass die Rechnungsstellung durch die Praxis selbst erfolgen kann oder die medizinische Versorgung auf andere Weise gewährleistet ist.

## Sichere Passwörter wählen

Um den Zugriff unbefugter Dritter auf Patientendaten zu verhindern, kommt der Verwendung von sicheren Passwörtern große Bedeutung zu. Hierfür spielt neben der Länge des Passworts – ein Passwort sollte in der Arztpraxis mindestens zwölf Stellen haben – die Komplexität des Passworts eine entscheidende Rolle. Passwörter sollten daher Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten.

## Sicherheit beim E-Mail-Verkehr gewährleisten

Immer mehr Arztpraxen bieten ihren Patienten eine Kontaktaufnahme per E-Mail oder Web-Formular an, um Termine zu vereinbaren, Rezepte zu bestellen oder medizinische Informationen zu erhalten. Als Mindestschutz bedarf es hierfür einer Transportverschlüsselung mit SSL/TLS (einschließlich Perfect Forward Secrecy). Bei E-Mails ist zudem grundsätzlich eine Ende-zu-Ende-Verschlüsselung oder eine gleichwertige Sicherung vorzusehen. Bei Web-Formularen oder Internet-Portalen sind wegen des dort in verstärktem Maße bestehenden Hacking-Risikos weitergehende Anforderungen zu erfüllen, um dem hohen Schutzbedarf von Patientendaten Rechnung zu tragen.

## Wartungsvertrag für Praxis-IT abschließen

Wird mit der (Fern-)Wartung der Praxis-IT ein externer Dienstleister beauftragt und kann dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden, bedarf es neben dem zivilrechtlichen Wartungsvertrag eines datenschutzrechtlichen Vertrags mit Festlegungen zur Gewährleistung der Datensicherheit (vgl. § 11 Abs. 5 BDSG). Nicht abschließend geklärt ist allerdings, wie bei der Einschaltung externer IT-Dienstleister eine Verletzung der ärztlichen Schweigepflicht nach § 203 des Strafgesetzbuchs zuverlässig ausgeschlossen werden kann. Hier besteht dringender Handlungsbedarf für den Gesetzgeber.

## Backup-Medien verschlüsseln

Auch Backup-Medien müssen ausreichend vor unbefugtem Zugriff geschützt werden. Zu diesem Zweck sollten Datenträger nicht nur physikalisch (zum Beispiel durch einen abschließbaren Schrank), sondern auch durch eine kryptografische Verschlüsselung (zum Beispiel AES 256-Bit) gesichert werden. Ohne eine solche Verschlüsselung stellt der Diebstahl eines Datenträgers mit Patientendaten grundsätzlich eine Datenpanne dar, über die der Arzt gemäß § 42a BDSG nicht nur die Aufsichtsbehörde, sondern auch die Patienten informieren muss.

## Akten zuverlässig vernichten

Nach Ablauf der Aufbewahrungsfristen sind Papierakten zu vernichten bzw. Daten zu löschen. Informationen zur erforderlichen Sicherheitsstufe des Aktenvernichters finden sich auf den Internetseiten des Bundesamts für Sicherheit in der Informationstechnik. Erfolgt die Aktenvernichtung durch einen externen Dienstleister, ist ein Vertrag zur Auftragsdatenverarbeitung gemäß § 11 Abs. 2 BDSG zu schließen.

## Bei Fragen Rat suchen

Für weiterführende Informationen sind die von der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung erarbeiteten „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ sowie das Handbuch „Datenschutz in der Arzt-/Psychotherapeutenpraxis“ der Kassenärztlichen Vereinigung Bayerns zu empfehlen; beide Publikationen finden sich im Internet. Bei Fragen steht das Bayerische Landesamt für Datenschutzaufsicht gerne beratend zur Verfügung.

## Autorin



*Karin Vedder,  
Bayerisches Landesamt für Datenschutzaufsicht,  
Promenade 27  
(Schloss), 91522  
Ansbach, Internet:  
[www.lida.bayern.de](http://www.lida.bayern.de)*