MANDANTEN-INFO
DATENSCHUTZ IM GESUNDHEITS-WESEN

Datenschutz im Gesundheitswesen

Richtiger Umgang mit besonders sensiblen Daten

In enger Zusammenarbeit mit

DATEV

Mandanten-Info

Datenschutz im Gesundheitswesen

Inhalt

1. Einführung

Datenschutz im Gesundheitswesen fängt dort an, wo die sensiblen Daten zuerst anfallen.

Hausarzt, Facharzt, Apotheke, Krankenkasse, Klinik ... : Hier sollte größte Sorgfalt herrschen.

Patienteninformationen werden im vernetzten Gesundheitssystem von vielen Stellen erfasst, eingesehen und verarbeitet. Das macht vieles schneller und effizienter. Aber sind sensible Daten dadurch auch unsicherer und leichter ausspähbar?

Diese Frage hat Auswirkungen auf die Organisation des Gesundheitswesens. Denn die betroffenen Stellen haben alle notwendigen Maßnahmen zu ergreifen, um die Kenntnisnahme personenbezogener Daten durch unbefugte Dritte zu verhindern.

Eine gute Praxisorganisation ist nur ein Baustein zur Einhaltung der ärztlichen Schweigepflicht, denn mit der zunehmenden Digitalisierung in Arztpraxen und Krankenhäusern sowie der Internetnutzung geht ein erhöhtes Risiko für die Geheimhaltung der Patienteninformationen einher. So ist die elektronische Aktenführung, der Einsatz von Chipkarten und die Konsultation online nicht ungewöhnlich.

Daher müssen auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden. Denn personenbezogene Daten im Gesundheitswesen werden vom Gesetzgeber in § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG) besonders geschützt. Datenschutzaufsichtsbehörden der jeweiligen Bundesländer richten darauf zunehmend ihre Aufmerksamkeit.

Steuerberater können ihre Mandanten im Gesundheitswesen unterstützen und entsprechend beraten.

2. Allgemeine Grundsätze beim Umgang mit Patientendaten

Unabhängig von der Art der Datenerfassung und -verarbeitung muss z. B. der Arzt beim Umgang mit Patientendaten folgende Grundsätze beachten:

- das Persönlichkeitsrecht des Patienten in der Ausprägung des informationellen Selbstbestimmungsrechts ist zu wahren
- das Patientengeheimnis ist zu wahren
- die Behandlungsabläufe und -ergebnisse müssen dokumentiert werden
- das jederzeitige Recht des Patienten auf Einsicht in die über seine Person gespeicherten Daten bzw. Aufzeichnungen
- subjektive Einschätzungen des behandelnden Arztes können, müssen aber nicht offenbart werden.

3. Freiwilligkeit der Einwilligung – Die Selbstbestimmung des Patienten hat Vorrang

Die Selbstbestimmung des Patienten darf nicht durch eine Digitalisierung im Gesundheitswesen untergraben werden.

Ärzte und medizinische Einrichtungen dürfen eine Behandlung nicht alleine deshalb verweigern, weil der Patient die geforderte Schweigepflichtentbindung oder die datenschutzrechtliche Einwilligung verweigert. Eine vorgegebene ausnahmslose Versagung der Behandlung – z. B. bei medizinischen Notfällen – ist nicht zulässig.

Hierbei müssen immer die jeweiligen Interessen aller Beteiligten abgewogen werden. Dabei sind individuelle Ausnahmesituationen, in denen sich die Patienten befinden, ebenso zu berücksichtigen wie die medizinische Beurteilung. Im Einzelfall muss entschieden werden, ob eine Behandlung nicht auch ohne die Einwilligung vertretbar oder sogar erforderlich ist.

4. Das sollten Praxen beachten

1. Die Benennung eines Datenschutzbeauftragten

   Die überwiegende Mehrheit der Arztpraxen benötigt zwar keinen Datenschutzbeauftragten, da er erst dann zu bestellen ist, sobald mehr als neun Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind (§ 4f Abs. 1 Satz 4 BDSG), aber auch ohne die Bestellpflicht gilt auch für kleinere Arztpraxen oder Unternehmen, dass der Datenschutz eingehalten werden muss. Die Strafen können bei nachlässigem Umgang mit Patientendaten empfindlich sein.

   Der Beauftragte kann ein interner Mitarbeiter oder ein externer Datenschutzbeauftragter sein, der über die geforderten Kenntnisse verfügt oder sich durch Aus- und Weiterbildung entsprechend weiterbildet. Die adäquate Besetzung dieser Stelle ist ein zentraler Punkt, der sicherstellt, dass der Datenschutz in Praxen, Apotheken und Krankenhäusern den Anforderungen der relevanten Gesetze genügt.

2. Verstöße gegen den Datenschutz

   Verstöße gegen den Datenschutz werden nicht nur gemäß den Strafvorschriften des BDSG (§§ 43 Abs. 3, 44 Abs. 1 BDSG) mit einem Bußgeld von bis zu 300.000 Euro oder einer Freiheitsstrafe von bis zu zwei Jahren geahndet, sondern werden zusätzlich auch nach § 203 Abs. 1 Strafgesetzbuch (StGB) – auch für Angehörige der Heilberufe – mit einer Freiheitsstrafe von bis zu einem Jahr bestraft.

3. Die Gestaltung der Praxisräume – der erste Schritt zur Sicherstellung der Vertraulichkeit!

   Die Prüfungsschwerpunkte der Aufsichtsbehörden liegen vor allem in der Gestaltung der Praxisräumlichkeiten. Dazu zählen datenschutzkonforme Trennungen der Eingangs-, Warte- und Behandlungsbereiche.

   - Patientenunterlagen dürfen grundsätzlich nicht einsehbar sein und müssen vor unbefugtem Zugriff geschützt sein.
   - Die Computer-Bildschirme sind so zu stellen, dass diese nicht von Dritten/Unbefugten eingesehen werden können. Auch von Bildschirmsperren sollte regelmäßig Gebrauch gemacht werden.
   - Auch bei Telefonaten ist im medizinischen Bereich die Geheimhaltung sicherzustellen. So ist z. B. bei der Durchgabe von Befunden am Telefon vom Arzt oder seinem Personal darauf zu achten, dass das Gespräch nicht mitgehört werden kann. Ggf. muss dazu ein gesonderter Raum aufgesucht werden.
   - Sinnvoll kann es sein, Patientendaten zunächst mit Hilfe eines Fragebogens vom Patienten selbst erfassen zu lassen.
   - Durch eine räumliche Aufteilung der Arztpraxis in einen Empfangsbereich und einen Behandlungsbereich kann bereits für eine gewisse Diskretion gesorgt werden. Der Patient muss nicht seine Belange und Fragen am Empfangstresen im Beisein Dritter (z. B. weiterer Patienten) erörtern. Auf einen ausreichenden Diskretionsabstand an der Anmeldung ist daher zu achten.

4. Die Entsorgung von Patientendaten

   Die Entsorgung von Behandlungsunterlagen, wie z. B. Patientenkarteien (Papier), digitalen Aufnahmen (Röntgenbilder) oder digitalen Datenträgern (CD, DVD) wird oft von der Praxis an externe Dienstleister übergeben.

   Entscheidend ist hier, dass erst nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfristen die Unterlagen vernichtet werden können und auch hier die Art und Weise der Entsorgung den Datenschutzbestimmungen gerecht werden muss.

   Im Allgemeinen liegt eine datenschutzkonforme Entsorgung der Patientenunterlagen dann vor, wenn die Patienteninformationen nach dem Entsorgungsvorgang

   - nicht mehr lesbar vorhanden sind
   - und eine Rekonstruktion der Unterlagen grundsätzlich nicht mehr möglich ist.

   Hierzu gibt es DIN-Vorgaben, wie z. B. die Größe der Papierschnipsel.

> ⓘ **Hinweis**
>
> Besondere Sorgfalt ist geboten bei der Auswahl eines externen Entsorgungsunternehmens. Durch eine entsprechende Vertragsgestaltung kann sichergestellt werden, dass das Unternehmen die hochsensiblen Daten ordnungsgemäß entsorgt und hierfür auch haftet.

5. Weitere Konstellationen und Folgen bei der Weitergabe von Patientendaten

   Für Ärzte, medizinische Einrichtungen und deren Mitarbeiter gibt es eine Vielzahl weiterer Sachverhalte, die den Umgang mit besonders sensiblen Patientendaten betreffen – wie z. B.:

   - Gemeinsamer Zugriff auf Patientendaten bei einer Organisationsgemeinschaft (Praxisgemeinschaft) und einer Berufsausübungsgemeinschaft (Gemeinschaftspraxis)
   - Sanktionsmöglichkeiten und Folgen bei Datenschutzverstößen
   - Informationsansprüche der Krankenkassen, des Medizinischen Dienstes der Krankenversicherung (MDK) und der Sozialversicherungsträger
   - Entbindung von der Schweigepflicht
   - Verarbeitung von Patientendaten für Forschungszwecke
   - Datenschutz bei meldepflichtigen Erkrankungen und Infektionen
   - Übermittlung an nachbehandelnde Einrichtungen/Inkasso
   - Weitergabe von Patientenakten bei Praxisübergaben (Nachfolge)
   - Mitarbeiter als Patienten: Besondere Schutzwürdigkeit (VIP-Konzepte)
   - Archivierung von Krankenhausunterlagen, welche als besonders sensibel einzustufende Gesundheitsdaten gelten; Besonderheiten der Krankenhausinformationssysteme

5. Reduzierung der Datenschutz- und IT-Risiken für Ihre Arztpraxis

Mit dem nachfolgenden Maßnahmen- und Fragenkatalog zum Thema Datenschutz haben Sie die Möglichkeit ganz bestimmte Arbeitsbereiche in Ihrer Arztpraxis zu hinterfragen und zu optimieren:

Datenschutz-Dokumentation/Datenschutzhandbuch

- Vorlage für das externe sowie das interne Verfahrensverzeichnis
- Vorlage für ein Datenschutz- und IT-Sicherheitskonzept
- Vorlage für ein Datenschutzhandbuch mit Hinweisen und Regelungen
- Vertragsvorlagen (z. B. Verschwiegenheitserklärung)
- Checklisten (z. B. Beauftragung neuer Dienstleister)

Mitarbeitersensibilisierung

- Durchführung von Schulungen und Informationsveranstaltungen für Ihre Mitarbeiter zum datenkonformen Umgang mit personenbezogenen Daten und Patientendaten
- Information der Mitarbeiter zu datenschutzgerechtem Verhalten in der Arztpraxis

Sichere E-Mail-Kommunikation und Internetnutzung

- Wie sichere ich meine E-Mails und mein Praxisnetz gegen unberechtigte Zugriffe ab?
- Wie vereinbare ich mit meinem Patienten und weiterbehandelnden Ärzten die abgesicherte Kommunikation?
- Was müssen meine Mitarbeiter und Patienten tun?

- Wie regele ich die E-Mail- und Internetnutzung in der Arztpraxis?

Organisation und Praxisgestaltung

- Wie gestalte ich meine Praxisräume (z. B. Anmeldung, Behandlungsräume) gemäß den Anforderungen des BDSG?
- Was müssen meine Mitarbeiter im täglichen Praxisalltag beachten?

Externe Dienstleister und Auftragsdatenverarbeitung (ADV)

- Mit welchen Dienstleistern muss ich einen Vertrag zur Auftragsdatenverarbeitung schließen?
- Welche Dienstleister muss ich zur Verschwiegenheit verpflichten?
- Wie gestalte ich einen Vertrag zur Auftragsdatenverarbeitung?

Rechnungsstellung und Verbuchung von Geldeingängen

- Wie ist die Übergabe der (privat-)ärztlichen Leistung in das rechnungserstellende Programm geregelt?
- Sieht ein Betriebsprüfer über die Zahlungseingänge – z. B. von Patienten oder Privatärztlichen Verrechnungsstellen (PVS) – auf den Bankkonten evtl. auch in die Diagnosen?
- Was ist bei den Schnittstellen zwischen rechnungserstellendem Programm zur Software der Privatärztlichen Verrechnungsstellen (PVS) zur beachten?

Berechtigungskonzept

- Wie gestalte ich das Berechtigungskonzept datenschutzkonform?
- Wie muss ich die Nutzungskontrolle und die Windows-Freigabe gemäß den Anforderungen des BDSG einrichten?

IT-Konzept, einschl. Virenschutz und Datensicherung

- Standort des Servers und Notfallvorsorgekonzept
- Welche Daten muss ich wie sichern?
- Wie schütze ich meine Arztpraxis vor Viren?

Mobiles Arbeiten

- Wie schütze ich meine mobilen Geräte?
- Was muss ich bei der Absicherung von Notebooks, Tablet-PCs und Smartphones beachten?
- Wie sichere ich Heimarbeitsplätze ab?

Berichterstellung (abhängig vom Umfang)

- Schriftlicher Bericht mit Stand der Arztpraxis
- Empfehlungen für technische und organisatorische Maßnahmen zur Reduzierung der Datenschutz- und IT-Risiken

> ⓘ **Hinweis**
>
> Wie sicher sind Ihre Daten? Verstöße gegen den Datenschutz, Verlust von Patientendaten und der Missbrauch sensibler Daten können für betroffene Arztpraxen existenzgefährdend sein.
>
> Lassen Sie sich hierzu individuell von Ihrem Steuerberater unterstützen! Sie/Er berät Sie gerne beim Aufbau und Betrieb eines Datenschutzmanagements.

6. Fazit

Mitarbeiter im Gesundheitswesen müssen immer sensibel sein im Umgang mit Patientendaten – etwa in welcher Form diese weitergeleitet werden, gerade wenn externe Dienstleister oder IT-Unternehmen beauftragt sind. Ebenso stellen Entsorgungsunternehmen für Patientendaten ein Sicherheitsrisiko dar. Die Verträge zur Auftragsdatenverarbeitung und den Überwachungs- und Kontrollpflichten sollten genau unter die Lupe genommen werden.

Auch die Umsetzung der technischen und organisatorischen Maßnahmen, zum Beispiel die Benutzerverwaltung und das Rechtekonzept, eingesetzte Antivirenprogramme sowie die Firewall, ein Datensicherungskonzept, Regelungen zur Internet- und E-Mail-Nutzung, verschlüsselte Datenübertragung oder Passwortregeln sollten regelmäßig überprüft werden.

Ihr Steuerberater kann Sie hierzu umfassend beraten und beim Aufbau einer sicheren Praxisorganisation unterstützen.

DATEV eG, 90329 Nürnberg (Verlag)

Stand: Oktober 2014
DATEV-Artikelnummer: 19455
E-Mail: literatur@service.datev.de