Datenschutz in der Arztpraxis: Was müssen wir beachten?

Kurze Einleitung

Der Umgang mit Patientendaten (besonders personenbezogene Daten i.S.v. Art. 9 Abs. 1 DSGVO) lässt dem Datenschutz in Arztpraxen im gesamten europäischen Raum einen Hohen Stellenwert zukommen. Die Gesundheitsinformation, welche im Rahmen der Tätigkeiten in Arztpraxen ermittelt werden, gehören nämlich zu den besonderen Arten personenbezogener Daten und sind daher besonders schützenswert. Außerdem kommt ein weiterer besonderer Aspekt hinzu. Dieser umfasst die Schweigepflicht der Ärzte und deren Mitarbeiter.

Inhalt:

Datenschutz in der Arztpraxis

Ob in der Klinik oder in der Arztpraxis, der Datenschutz ist in folgenden Bereichen von enormer Bedeutung. Zum einen spielt der Bereich der Datenerhebung eine wichtige Rolle. Dabei geht es um die Frage welche Daten eines Patienten gesammelt werden dürfen. In der Regel ist es nur erlaubt, die Daten zu erheben, die für die Durchführung der Behandlung und Diagnose von Belang sind.

Ein weiterer wichtiger Faktor betrifft die Datenweitergabe. Sämtliche Informationen, welche sich in der Patientenakte befinden, dürfen nicht automatisch an Versicherungen oder Dritte weitergegeben werden. Hierbei sind je nach Adressat bestimmte Vorgaben zu beachten. Um die Herausgabe der personenbezogenen Daten rechtskonform zu gestalten, muss in der Regel eine Einwilligungserklärung des Betroffenen vorliegen.

Außerdem muss die Datensicherung in den Arztpraxen in der Weise gewährleistet werden, dass personenbezogene Patientendaten vor dem Zugriff von Dritten in ausreichender Art geschützt werden. Dies betrifft neben den analogen Datensätzen wie z.B. Formularen, Ausdrucken oder Notizen, auch die digital gespeicherten Patientendaten.

Bei Gemeinschaftspraxen oder Krankenhäusern ist die Datenweitergabe unter Ärzten in der Regel nur dann zulässig, wenn diese die Patienten auch betreuen. Allerdings darf sich der Datenaustausch nur auf die für die Betreuung des einzelnen notwendigen Informationen beschränken. Jeder Informationsaustausch, der sich außerhalb dieses Rahmens befindet, ist unzulässig.

Datenschutz am Empfang in der Arztpraxis

Jede Arztpraxis hat in der Regel einen Empfangstresen an dem die Patienten in Empfang genommen werden und ihr Anliegen mitteilen. Ab diesem Zeitpunkt muss darauf geachtet werden, dass datenschutzrechtliche Vorgaben eingehalten werden. In diesem Zusammenhang ergeben sich eine Reihe von datenschutzrechtlichen Problemen, die am Empfangstresen entstehen können.

Manchmal kommt es vor, dass am Empfangstresen ein “Patienten-Stau” entsteht. Dabei spricht das Prasxispersonal in ungeschützter Atmosphäre über Gesundheitsdaten, sodass Dritte mithören können und gegebenenfalls über Patienten und deren Diagnosen informiert werden. Ein weiteres Problem besteht darin, wenn das Praxispersonal den Empfangsbereich verlässt. Dabei bleiben Schränke, Akten und Computer oftmals unbeaufsichtigt. Hierbei besteht die Gefahr, dass Unberechtigte Zugriff zu diesen Daten verschaffen können.

Häufig unterhalten sich Ärzte und Arzthelfer über Testergebnisse und Diagnosen von Patienten. Die im Warteraum befindlichen Patienten können bei zu lauter Kommunikation zwischen Arzt und angestelltem Personal über besonders personenbezogenen Daten der einzelnen Patienten mithören.

Das Praxispersonal ist oftmals im Gespräch mit den Patienten. Dies geschieht sowohl über das Telefon als auch digital per E-Mail. Hierbei werden unter anderem Informationen über Testergebnisse, Diagnosen und Therapien angegeben. Allerdings besteht bei derartigen Kontakten das Problem der Verifizierung. Die Praxen können nicht sicherstellen, ob sie auch mit der betroffenen Person sprechen. Die Gefahr, Patientendaten an Nichtberechtigte weiterzugeben, ist daher sehr groß.

Befinden sich Patienten das erste Mal bei einem neuen Arzt, werden personenbezogene Daten abgefragt. Um sich physischen Aufwand, durch die ganze Papierwirtschaft zu sparen, legen einige Praxen vorgefertigte Informationsschreiben zum Datenschutz nach Art. 13 DSGVO aus und bitten den Patienten diese Information zu lesen und dann mündlich eine Zustimmung zur Erhebung der Daten zu erteilen. Dies ist ein fataler Fehler. Fordert beispielsweise der Patient oder eine Behörde einen Nachweis über die mündlich erteilte Zustimmung, ist die Praxis nicht in der Lage, diesen zu leisten – welches als bußgeldbewährter Datenschutzverstoß gewertet werden kann. Um diesem Problem entgegenzuwirken, sollte stets darauf geachtet werden, immer eine schriftliche Einwilligung einzuholen.

Datenschutz Arztpraxis Checkliste

Mit der folgenden Checkliste können Sie überprüfen, ob ihre Praxis alle datenschutzrechtlichen Anforderungen erfüllt. Alle aufgeführten Fragen sollten mit "Ja" beantwortet werden.

- Liegt eine revisionssichere Einwilligung für die Verarbeitung der Patientendaten vor?
- Wurde die Datenschutzerklärung auf der Homepage rechtskonform aufgestellt?
- Gibt es eine Zutrittskontrolle (z.B. verschlossene Eingangstür)?
- Ist der Empfang ununterbrochen besetzt?
- Werden Anmelde- bzw. Patientendaten diskret erhoben?
- Sind Computerbildschirme und Telefondisplays am Empfang so aufgestellt, dass Dritte den Inhalt nicht sehen können?
- Sind die Postkörbe und die Ablagen für die Patientenakten so aufgestellt, dass Dritte nicht mitlesen können?
- Sind Personalakten gegen unbefugten Zugriff gesichert?
- Sind die Wartezimmer so abgesichert, dass keine Gespräche zwischen Patienten und Praxispersonal mitgehört werden kann?
- Erfolgt der Anruf der Patienten mittels Verifizierungscode oder ähnliches?
- Bestehen Auftragsverarbeitungsverträge mit Dienstleistern (z.B. Cloudanbieter)?
- Ist der Serverraum geschützt?
- Ist die Praxis gegen Einbrüche geschützt
- Ist für die EDV eine externe Stromversorgung angerichtet?
- Werden Passwörter regelmäßig gewechselt?
- Sind unbeaufsichtigte Computer regelmäßig gesperrt?
- Sind Antivirenprogramme installiert ?
- Werden die Antivirenprogramme stets auf den neuesten Stand gebracht?
- Werden nicht mehr benötigte Personalakten datenschutzkonform entsorgt?
- Wird die Entsorgung protokolliert?
- Werden regelmäßig Backups erstellt?
- Sind alle Praxisbeschäftigte auf das Daten-Geheimnis hingewiesen worden und in puncto Datenschutz geschult?

Rechtsgrundlagen für die Verarbeitung von Patientendaten

Wie bereits in der Einleitung beschrieben geht es bei Patientendaten um besonders personenbezogene Daten, da es sich hierbei um Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO handelt. Die Rechtsvorschrift für Verarbeitung besonderer personenbezogener Daten innerhalb Deutschlands ergibt sich aus Art. 9 Abs. 1 DSGVO i.V.m § 22 Abs. 1 Nr. 1 lit. b) BDSG. Für den gesamten europäischen Raum gilt dagegen der Art. 9 Abs. 2 lit. h) und i) DSGVO. Somit müssen oftmals datenschutzrechtliche Einwilligungen eingeholt werden.

Datenschutzerklärung für Arztpraxis

Arztpraxen müssen auf ihren Websites eine Datenschutzerklärung in präziser, transparenter, verständlicher und leicht zugänglicher Form zur Verfügung zu stellen. Um diese Pflichten in Einklang zu bringen, wird ein gewisser Wortschatz in den Formulierungen und den Aufbau erforderlich sein.

Bei der Datenschutzerklärung muss darauf geachtet werden, dass der Besucher der Arztpraxis über alle Vorgänge aufzuklären ist, bei denen dessen personenbezogenen Daten verarbeitet werden. Ferner muss jede Datenschutzerklärung den Namen und Kontaktdaten

(Anschrift, E-Mail) des Betreibers und somit "Verantwortlichen" enthalten. Darüber hinaus müssen die Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden) aufgeführt werden. Dazu gehören sowohl die Anschrift als auch die E-Mail Adresse. Für jedes Tool, dass personenbezogene Daten verarbeitet, müssen folgende Angaben gemacht werden – im Folgenden werden beispielhafte Verarbeitung aufgeführt:

- Facebook "Like-Buttons" oder ähnliche Social- Plugins anderer Anbieter
- Webformulare (Kontaktformulare, etc.)
- Cookies (Information zum Zweck, Empfänger der Daten, etc.)

Zu den eben genannten Verarbeitungen müssen immer mindestens separate Angaben zum Zweck und der Rechtsgrundlage der Datenverarbeitung erfolgen. Es ist erforderlich weitere Angaben zu machen, um eine transparente Verarbeitung zu gewährleisten. Deshalb sollten die Informationen gemäß Art. 13 Abs 2 DSGVO immer zusätzlich aufgeführt werden. Dazu zählen:

- Dauer der Speicherung der personenbezogenen Daten
- Recht des Besuchers auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und das Wiederrufsrecht
- Beschwerderecht bei der Aufsichtsbehörde
- Bestehen einer automatisierten Entscheidungsfindung
- die Umstände der Bereitstellung der Daten, unter anderem ob eine gesetzliche oder vertragliche vorgeschrieben ist

Datenweitergabe an Krankenkassen

Krankenkassen speichern eine Vielzahl von Daten ihrer Versicherten. Dies ist erforderlich, damit sie Ihre Aufgabe der medizinischen Versorgung nachkommen können. Die gesetzlichen Kassen erheben und speichern eine Vielzahl von Sozialdaten ihrer Versicherten. Dazu gehören nicht nur Adressangaben der betroffenen Personen, sondern auch Krankheitsdiagnosen und Abrechnungsbelege aus Heilbehandlungen.

Es ist offensichtlich, dass die Krankenkassen diese Informationen benötigten, um Ihren gesetzlichen Auftrag erfüllen zu können, die die medizinische Versorgung sicherstellen. Die Speicherung und Erhebung der Daten durch die Krankenkasse ist daher nach § 284 SGB V zulässig.

Allerdings unterliegen die Krankenkassen ebenfalls dem Grundsatz des Datenschutzrechts, insoweit, als das die Krankenkassen nur so viele Daten erheben dürfen, wie sie für die Aufgabenerledigung benötigen. Dieser datenschutzrechtliche Grundsatz wird aus dem Rechtsgedanken gemäß der Datenminimierung nach Art. 5 Abs. 1 c) DSGVO geschlossen.

Hinsichtlich der rechtlichen Regelung zur Löschung der Daten sieht der § 84 Abs. 2 S. 2 SGB X vor, dass die Krankenkassen die Daten löschen müssen, sobald sie nicht erforderlich sind und kein Grund zur Annahme besteht, die Daten weiterhin zu speichern.

Datenschutz Folgenabschätzung in der Arztpraxis

Das Verarbeiten von personenbezogenen Daten birgt immer ein Risiko für die Rechte und Freiheiten der betroffenen Personen. Deshalb müssen Maßnahmen zur Datensicherheit gem. Art. 32 DSGVO getroffen werden. Ziel ist, dass sich datenverarbeitende Instanzen, so wie Arztpraxen, mit diesen Risiken auseinandersetzen. Ein Instrument des Gesetzgebers dazu ist die Datenschutzfolgenabschätzung (DSFA), bei der die Risiken beschrieben, bewertet und schützende Maßnahmen erarbeitet werden müssen.

Wann muss eine Arztpraxis eine Datenschutz Folgenabschätzung durchführen?

Im Falle einer Verarbeitung von personenbezogenen Daten, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person birgt, ist eine Datenschutzfolgenabschätzung (DSFA) durchzuführen. In einer Arztpraxis kann von einem erhöhten Risiko ausgegangen werden, doch letztendlich muss der Verantwortliche immer selbst entscheiden, wann voraussichtlich hohes Risiko besteht. Soll eine DSFA durchgeführt werden, muss immer ein Datenschutzbeauftragter hinzugezogen werden.

Da ein erhöhtes Risiko nicht leicht einzuschätzen ist, hat der Gesetzgeber die Aufsichtsbehörden damit beauftragt, Listen mit Verarbeitungen zu erstellen, für die eine Datenschutzfolgenabschätzung durchzuführen ist:

1. Analyse der Persönlichkeit

Analyse der Persönlichkeit: Eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen (Kunden-Scoring, systematische automatisierte Kundenanalyse, Persönlichkeitstest im Recruiting).

2. Besondere personenbezogene Daten

Eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten (gem. Art. 9 Abs. DSGVO) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (gem. Art. 10 DSGVO).

3. Videoüberwachung

Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Beispiel: Videoüberwachung, soweit diese öffentliche Bereiche wie Gehwege oder Plätze mit erfasst).