pt_Erfolg

Das Unternehmer-Magazin für erfolgreiche PTs

Februar 2021

BGM Herausforderungen durch Corona und Homeoffice
DVPMG Digitale Anwendungen auf dem Prüfstand
KÜNDIGUNG Der letzte Eindruck zählt

DATEN FALLEN VERMEIDEN

Datenschutz in der Physiotherapie

Die sieben größten Datenfallen – und praktische Tipps, wie Sie sie vermeiden

Ein Beitrag von Achim Barth

Am 25. Mai wird die Datenschutz-Grundverordnung (DSGVO) drei Jahre alt. Seit die Verordnung 2018 in Kraft getreten ist, hat sich einiges getan. Inhaber und Betreiber von physiotherapeutischen Einrichtungen wurden mit zahlreichen Informationen überfrachtet und hörten Horrorgeschichten über Bußgelder und Abmahngefahren. Bisher haben fast alle Physiotherapeuten ihre Hausaufgaben mehr oder weniger erfüllt. Sie konnten sich ja auch kaum dagegen wehren, da rund um die Einführung das Thema überall präsent war.

Grafik: sdecoret/shutterstock.com

Für Eilige

Wussten Sie, dass auch Notizzettel schon ein Dateisystem sind? Und dafür gilt dann die Datenschutz-Grundverordnung. Die Herausforderungen in den Therapiepraxen sind eigentlich immer die gleichen. Es gibt typischerweise sieben Datenfallen, die häufig der Grund für Probleme sind. Dazu gehören unter anderem ungeschulte Mitarbeiter, ungesicherte Partner und veraltete Unterlagen.

Der Berufsverband veröffentlichte Handlungsempfehlungen, eventuell wussten auch Steuerberater oder Anwalt etwas zum Thema beizusteuern, die Tages- und Fachpresse berichtete ebenso umfänglich über die strengen Vorgaben. Nicht selten widersprachen sich die Empfehlungen der Experten oder die Aussagen zur Umsetzung blieben schwammig. „Es kommt darauf an." – Der Lieblingssatz der Rechtsanwälte hilft Physiotherapeuten wenig, wenn sie einfach nur die gesetzlichen Anforderungen erfüllen möchten, ohne sich dabei „zu Tode" zu verwalten.

Mehr juristische Klarheit. Als die DSGVO eingeführt wurde, gab es weder Urteile zu strittigen Auslegungen noch praktische Beispiele, wie Aufsichtsbehörden die Verordnung auslegen. All das entwickelte sich erst. Jetzt, drei Jahren später, nach einigen wegweisenden Urteilen und klaren Ansagen der Aufsichtsbehörden, gibt es deutlich mehr Klarheit. So dachte man zum Beispiel 2018 noch, dass Notizzettel kein Dateisystem seien. Mit dem sogenannten „Zeugen-Jehovas-Urteil" des EuGH vom Juli 2018 ist nun klar, dass auch Notizzettel ein Dateisystem sind und somit hierfür auch die DSGVO gilt.

Ein Urteil, das Relevanz für Physiotherapeuten haben kann. Auch strittige Themen bei der Auftragsverarbeitung und gemeinsamen Verantwortlichkeit in der Datenverarbeitung sind inzwischen

höchstrichterlich geklärt. So ist heute klar, dass ein Betreiber einer Facebook-Unternehmensseite gemeinsam mit Facebook im Sinne der DSGVO verantwortlich ist. Betreiben Praxen eine Facebook-Seite, müssen sie den entsprechenden Vertrag mit Facebook eingehen. Dabei kämpfen Inhaber von physiotherapeutischen Einrichtungen beim Thema Datenschutz mit den immer gleichen Problemen. Im Folgenden bekommen Sie einen Überblick über die sieben häufigsten Datenfallen für Praxisbetreiber – inklusive praktischer Tipps zur Schließung dieser Datenlücken.

Datenfalle 1: Unwissenheit – schützt vor Strafe nicht. Physiotherapeuten verarbeiten täglich Gesundheitsdaten ihrer Patienten. Daher ist es wichtig, beim Thema Datenschutz am Ball zu bleiben. Schließlich behandeln Sie Menschen, die Ihnen vertrauen. Verschwiegenheit und Verlässlichkeit gehört zum Kerngeschäft. Genauso wie es selbstverständlich ist, vertrauliche Gespräche mit Patienten nicht weiterzugeben, muss es auch selbstverständlich sein, die Anforderungen und den Status quo aus dem Datenschutz zu kennen. Die meisten Praxen haben keinen Datenschutzbeauftragten, weil sie dazu nicht verpflichtet sind (Ende 2019 wurde die Benennpflicht von zehn auf 20 Beschäftigte erhöht). Somit fehlt der fachkundige Berater, den Sie um Rat fragen können und der wichtige Neuerungen im Blick behält. Abonnieren Sie daher geeignete Newsletter und schauen Sie regelmäßig, ob der Berufsverband, die Industrie- und Handelskammer (IHK) oder andere Verbände aktuelle Beiträge veröffentlichen. Haben Sie als Praxisinhaber doch einen Datenschutzbeauftragen benannt, erinnern Sie ihn an seine Pflichten. Schließlich ist das Thema einer enormen Dynamik unterworfen.

Datenfalle 2: Mitleser, Lauschangriffe und Fahrlässigkeit. Am Empfang gewinnen Patienten den ersten Eindruck über die Praxis. Oft wird dieser Bereich offen gestaltet, um eine entspannte Atmosphäre zu schaffen. Diese Offenheit müssen wir in Einklang mit dem Datenschutz bringen. Zudem erwarten Patienten Diskretion, was ihre eigenen Daten betrifft. Im Empfangsbereich laufen viele Informationen von vielen Menschen auf engem Raum zusammen. Hinzu kommen eingehende Anrufe, Faxe und E-Mails. Damit alles datenschutzkonform abläuft, müssen Sie technische und organisatorische Maßnahmen treffen.

Der Empfangsbereich sollte ausreichend groß sein. Nur so können Sie auch bei mehreren wartenden Patienten sicherstellen, dass die erforderlichen Diskretionsabstände (mindestens ein Meter) eingehalten werden. Fordern Sie Patienten zum Beispiel durch ein Schild dazu auf, den Abstand zu respektieren. Unterlagen für Behandlungen, Patientenakten, Anamnesebögen, Einwilligungen, Fragebögen oder zu unterscheibende Behandlungstermine haben auf dem Tresen der Anmeldung nichts zu suchen. Werden diese aus organisatorischen Gründen an der Anmeldung bearbeitet, muss eine Einsichtnahme durch Unbefugte ausgeschlossen sein. In diesem Fall sind ebenfalls die Diskretionsabstände wichtig. Auch bei Gesprächen im Anmeldebereich ist der Datenschutz zu wahren. Wenn andere Patienten mithören können, sollten zum Beispiel keine Fragen zum Grund des Besuchs in der Praxis gestellt werden. EDV-Geräte wie Bildschirm, Tastatur, Maus, Kartenlesegerät, Drucker und Rechner sowie Speichermedien sind so zu platzieren, dass unerwünschter Zugriff Dritter auf Daten der Praxis nicht möglich ist. Verlassen Mitarbeiter ihren Arbeitsplatz, ist der Computer zu sperren.

Auch bei Gesprächen im Anmeldebereich ist der Datenschutz zu wahren.

In der Regel befindet sich bei der Anmeldung auch die Telefonanlage der Praxis. Die telefonische Informationsweitergabe kann leicht und ungewollt zu einer unzulässigen Offenbarung von Patientendaten führen. Nicht immer können Therapeuten sicher sein, dass sie tatsächlich zum Beispiel mit dem Patienten oder einem Bevollmächtigten sprechen. Um den Datenschutz bei Telefonaten zu wahren, sind folgende Regeln zu befolgen:

1. Vermeiden Sie die namentliche Anrede am Telefon, wenn Dritte mithören können.

2. Sie benötigen ein Verfahren, um Patienten eindeutig zu identifizieren.

3. Verzichten Sie darauf, an der Rezeption Diagnosen und Befunde weiterzugeben. Solche Telefongespräche sollten in einem separaten Raum geführt werden. In diesem Fall kommt hinzu, dass der Gesprächsteilnehmer sich hinreichend identifizieren muss, bevor etwa Gesundheitsdaten weitergegeben werden können.

Der Gesprächsteilnehmer muss sich identifizieren, bevor Gesundheitsdaten weitergegeben werden können.

4. Nach dem Grundsatz der Datensparsamkeit sollen bei der Terminvereinbarung nur die Daten abgefragt werden, die unmittelbar für die Behandlung beziehungsweise für die Planung erforderlich sind.

5. Treffen Sie klare Regelungen und Anweisungen gegenüber Ihren Mitarbeitern, welche Informationen am Telefon abgefragt werden, um den Anrufer zu identifizieren.

6. Achten Sie darauf, dass sich Ihre Schweigepflicht auch auf Familienangehörige erstreckt. Der anrufende Ehemann, der nach seiner Frau fragt, die angeblich in der Praxis ist, birgt so manchen datenschutzrechtlichen Fallstrick. Allein schon Auskünfte über die An- oder Abwesenheit sind schützenswerte Daten.

Wichtig! Vertrauliche Telefonate müssen immer unter „Ausschluss der Öffentlichkeit“ geführt werden. >>

Datenfalle 3: Löchrige EDV, ungewollte Einsichten. Generell gilt, dass technische Lösungen nachhaltiger sind als organisatorische. Sie können Patienten wiederkehrend auffordern, sich nicht über den Tresen zu lehnen und auf den Bildschirm zu schauen. Dennoch wird dieser Appell nur für den Augenblick helfen und ist beim nächsten Patienten erneut fällig. Daher sollten Bildschirme so platziert werden, dass Einsicht durch Patienten nicht möglich ist.

Im praktischen Alltag stellt das die Mitarbeiter häufig vor technische Probleme: Monitore sind nicht beliebig positionierbar. Kann ein Monitor nicht vor ungewollten Blicken geschützt werden, helfen Blickschutzfolien. Diese Folien sorgen dafür, dass Daten nur für die Person erkennbar sind, die sich unmittelbar vor dem Monitor befindet. Schräg von der Seite erscheint der Monitor schwarz. Auch Faxgeräte sollten so positioniert werden, dass sie sich nicht im Sichtbereich für Patienten befinden. Ferner sind Geräte zu bevorzugen, die Papierausdrucke mit dem Schriftbild nach unten ausgeben.

Kann ein Monitor nicht vor ungewollten Blicken geschützt werden, helfen Blickschutzfolien.

Zu einer geschützten IT-Infrastruktur gehören sichere Passwörter. Natürlich sind auch Programme durch Kennwörter zu schützen. Diese dürfen nicht zu kurz sein. Ich empfehle mindestens zwölf Zeichen mit Sonderzeichen (Beispiel: „x4p2$o9?q2Sd“) oder einen kurzen Satz über 20 Zeichen (wie „IchesseitjahrengerneSushi!“). Das Passwort darf nicht leicht zu erraten sein, also nicht im Wörterbuch stehen. Namen und Geburtsdaten sind unsichere Kombinationen. Passwörter müssen nicht mehr in kurzen Abständen geändert werden. Ist das Passwort lang genug und nicht auf einem Notizzettel vermerkt, müssen Sie es auch nicht ändern.

Für Mitarbeiter, die nicht mehr in der Praxis tätig sind, werden die Zugänge gelöscht. Zudem sollten Mitarbeiter nur auf die Daten zugreifen können, die auch für die Durchführung der Tätigkeit notwendig sind. Wird wiederholt ein falsches Passwort eingegeben, sollte der Zugriff automatisch gesperrt werden. Zur Absicherung der IT-Systeme sollten Inhaber auf jeden Fall eine Firewall und Antivirus-Software installieren. Beide schützen aber nur, wenn sie aktuell gehalten werden.

Mitarbeiter sollten nur auf Daten zugreifen können, die für die Durchführung der Tätigkeit notwendig sind.

Die meisten Hackerangriffe gelingen jedoch aufgrund geöffneter E-Mail-Anhänge. Sorgen Sie daher dafür, dass Mitarbeiter mit E-Mails sensibel umgehen. Per Mail übermittelte Text-, Bild- oder Datendateien dürfen nicht ohne Prüfung des Absenders und Echtheit der Daten geöffnet werden. So können gefährliche Schadprogramme Schwachstellen von Software oder des Betriebssystems ausnutzen und Viren oder Trojaner ins System gelangen.

Zu digitalen IT-Sicherheit gehört auch, die Daten der Praxis regelmäßig zu sichern. Dabei müssen Inhaber die Aufbewahrungsfristen berücksichtigen und Maßnahmen ergreifen, die Datenverlust unmöglich machen. Idealerweise werden die Daten täglich auf mindestens zwei verschiedenen transportablen oder externen Speichermedien (Cloud, USB-Stick, externe Festplatte) in automatisierter Form gesichert und an einem sicheren Ort aufbewahrt. Das Einspielen vorhandener Backups muss in unregelmäßigen Abständen simuliert werden. Auch Geschehnisse wie Einbruch oder Diebstahl der IT-Hardware, aber auch andere Risiken wie Hochwasser oder ein Brand können zu Datenverlust führen.

Wird das Praxisverwaltungssystem mittels Fernwartung gepflegt, sind folgende Punkte zu beachten:

1. Die Fernwartung muss vom Praxisrechner gestartet werden.
2. Der Rechner darf während der Dauer der Fernwartung nicht ohne Aufsicht sein.
3. Es ist eine Auftragsvereinbarung inklusive der Verpflichtung auf das Berufsgeheimnis nach §203 StGB mit dem Dienstleister abzuschließen (wenn Patientendaten eingesehen werden könnten).
4. Der Umfang und der Zeitpunkt der Wartung ist unter Angabe des Namens des Technikers zu dokumentieren.

Datenträger, die nicht mehr benötigt werden, sollten entweder eigenhändig zerstört oder durch eine Firma so entsorgt werden, dass eine Löschung der Daten garantiert ist. Diesen Vorgang sollten Sie schriftlich dokumentieren. Wenn die Fachfirma die Datenträger nicht in oder vor der Praxis vernichtet, sichern Sie sich mit einem Auftragsverarbeitungsvertrag ab. Werden Datenträger an Dritte weitergegeben, sind diese zu verschlüsseln. Der Datenempfänger erhält den Schlüssel auf andere Weise und muss sich schriftlich zur Geheimhaltung verpflichten.

Datenfalle 4: Ungeschulte Mitarbeiter. Damit die technischen und organisatorischen Maßnahmen (kurz TOMs) in der Praxis funktionieren, müssen Mitarbeiter und Therapeuten-Team die Anforderungen und Pflichten kennen, die sich durch den Datenschutz ergeben. Datenschutz funktioniert nur, wenn alle an einem Strang ziehen. Alle im Team müssen sich bewusst sein, welche Rechte die betroffenen Patienten geltend machen können. Zudem kann kein Inhaber oder Chef die Maßnahmen alleine umsetzen. Unabdingbar ist daher eine allgemeine Datenschutzschulung für die Mannschaft, dazu mindestens einmal im Jahr eine Auffrischung mit aktuellen Themen.

Alle mit der Datenverarbeitung beschäftigten Mitarbeiter sind bei der Aufnahme ihrer Tätigkeit auf Vertraulichkeit zu verpflichten. Die Mitarbeiter, die

die Praxis-IT betreuen, sind umfangreich in der eingesetzten Software zu schulen. Darunter fallen auch Einweisungen in:

- Aktualisierung und Überprüfung von Antiviren-Programmen und Firewall
- Sicherung der Daten
- Durchführung von Sicherheitsupdates

Datenfalle 5: Ungesicherte Partner. Die meisten Unternehmer wissen, dass sie mit Dienstleistern, die personenbezogene Daten verarbeiten, Auftragsverarbeitungsverträge abschließen müssen. Auch Facebook ist ein Thema, mit denen Praxisinhaber gemeinsam verantwortlich sind. Zudem arbeiten Inhaber mit weiteren Dienstleistern wie Steuerberatern, Abrechnungszentren oder Anwälten zusammen – Letztere sind im Regelfall eigenständig verantwortlich, aber auch hier gibt es Ausnahmen. Daher ist ein guter Rat: Erfassen Sie alle externen Dritten, die personenbezogene Daten (Mitarbeiterdaten, Patientendaten) erhalten, in einer Liste. Prüfen Sie systematisch, mit welcher Rechtsgrundlage Sie die Daten weitergeben. Vermerken Sie, ob die notwendigen Verträge abgeschlossen und wo diese abgelegt sind.

Datenfalle 6: Veraltete Unterlagen. Seit Einführung der DSGVO haben Unternehmer eine Rechenschaftspflicht. Das heißt, Praxisinhaber müssen nachweisen, dass sie die Anforderungen erfüllen. Drei Jahre nach Einführung der DSGVO ist es an der Zeit, zu prüfen, ob die eigenen Angaben noch aktuell sind. Gibt es die Verfahren so noch? Passt die Rechtsgrundlage? Sind die Löschfristen in der Praxis umzusetzen? Folgende Dokumente sollten Sie prüfen:

1. Verzeichnis von Verarbeitungstätigkeiten
2. Dokumentation Ihrer technischen und organisatorischen Maßnahmen
3. Prozess zum Umgang bei Betroffenenanfragen
4. Prozess zum Umgang mit Datenschutzpannen
5. Risikobewertung der einzelnen Verarbeitungen
6. Unterweisung der Mitarbeiter

Die Dokumentation zur Erfüllung der Rechenschaftspflicht ist eine Fleißaufgabe, die zusätzlich zum Tagesgeschäft anfällt. Aber keiner verlangt, dass diese Dokumentation an einem Nachmittag fertig sein muss. Fangen Sie klein an und setzen Sie sich umsetzbare Meilensteine.

Datenfalle 7: Veraltete, intransparente Website. Praxen, Therapiezentren und Angebote für Rehasport suchen, finden und bewerten potenzielle Patienten heutzutage fast ausschließlich im Internet.

Sieben Tipps gegen die wichtigsten Datenfallen

1. Bleiben Sie informiert.
2. Schaffen Sie Vertrauen durch Diskretion.
3. Sorgen Sie für eine sichere digitale Infrastruktur.
4. Unterweisen Sie Ihr Team.
5. Erfassen Sie alle Ihre Dienstleister in einer Liste.
6. Prüfen Sie Ihre Datenschutz-Dokumentation.
7. Machen Sie Ihren Internetauftritt zur datensicheren Visitenkarte.

Somit haben Praxisinhaber ein berechtigtes Interesse, eine moderne Webseite zu betreiben, bei der sie eventuell sogar mit den Patienten interagieren können. Moderne Webseiten bieten enorme Möglichkeiten. Entscheidend im Sinne des Datenschutzes sind vor allem folgende Aspekte:

- dass Inhaber in den Datenschutzhinweisen über alle Verarbeitungen transparent informieren,
- dass Inhaber die notwendigen Einwilligungen einholen, wenn sie bestimmte Dienste wie Google Analytics einsetzen und
- dass sie dafür sorgen, dass die Sicherheit der Webseite dem Stand der Technik entspricht und aktuell sowie gewartet ist.

Oftmals wissen viele Unternehmer gar nicht, welche Dienste auf ihrer Seite aktiviert sind. Dies lässt sich leicht durch einen Webseitenscan prüfen. Auf barth-datenschutz.de können Sie diesen kostenfrei durchführen. Sie erhalten eine E-Mail-Nachricht mit kurzem Bericht darüber, ob Handlungsbedarf auf Ihrer Seite besteht.

Stück für Stück zur datensicheren Einrichtung. Auch wenn das Thema lästig erscheint: Datenschutz ist wichtig, wird in zunehmend digitalen Zeiten immer bedeutender und von den Patienten erwartet. Zudem sind Praxisinhaber vom Gesetzgeber verpflichtet, die Vorgaben zu erfüllen. Wer heute damit beginnt, diese Tipps mit seinem unternehmerischen Status quo abzugleichen, hat den ersten Schritt getan. Daraufhin planen Sie die Umsetzungsmaßnahmen. Wer in den nächsten sechs bis zwölf Monaten alle Tipps umgesetzt hat, ist mit seiner Praxis optimal aufgestellt. Wenn Sie keine eigenen Kapazitäten zur Umsetzung bereitstellen können, suchen Sie sich externe Hilfe. ●

Erfassen Sie alle externen Dritten, die personenbezogene Daten (Mitarbeiterdaten, Patientendaten) erhalten, in einer Liste.

Oftmals wissen viele Unternehmer gar nicht, welche Dienste auf ihrer Seite aktiviert sind.