Digital in der Praxis

Cybersicherheit und Datenschutz in der Arztpraxis

Der Medizinsektor wird immer digitaler – Arztpraxen eingeschlossen. Damit verbunden sind steigende Anforderungen in den Bereichen Cybersicherheit und Datenschutz. Dieser Artikel gibt Ihnen erste Anhaltspunkte und Empfehlungen, die Sie teils direkt in Ihren Praxisalltag integrieren können: Wir teilen Wissenswertes zum Thema Datenschutz und DSGVO und erläutern die wichtigsten Richtlinien.

Wann immer sensible Daten im Spiel sind, sollten Cybersicherheit und Datenschutz feste Mitspieler sein. Sensible Patientendaten sind in der Datenschutzgrundverordnung (DSGVO) als „Gesundheitsdaten" zu finden. Sie werden dort gewohnt sperrig, sachlich und umfassend als „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen" beschrieben und zu den besonders schützenswerten personenbezogenen Datenkategorien gezählt.

Hohe Anforderungen an den Datenschutz gelten gleichwohl nicht erst seit der Einführung der DSGVO. Schon im Eid des Hippokrates (460 bis 370 v. Chr.) heißt es „Was immer ich sehe und höre bei der Behandlung oder außerhalb der Behandlung im Leben der Menschen, so werde ich von dem, was niemals nach außen ausgeplaudert werden soll, schweigen, indem ich alles Derartige als solches betrachte, dass nicht ausgesprochen werden darf."

Zurück ins Hier und Jetzt: Strenge Datenschutzrichtlinien, die DSGVO und die Schweigepflicht stellen hohe Anforderungen an den Verschluss personenbezogener Gesundheitsdaten – diese Anforderungen übertragen sich natürlich auf die sogenannte elektronische Datenverarbeitung, deren Nutzung besondere Anforderungen mit sich bringt.

DSGVO & Co. – ein kurzer Überblick

Seit ihrem Inkrafttreten im Mai 2018 hat die EU-Datenschutzgrundverordnung (DSGVO) so manche geläufige Datenschutzregel über Bord geworfen. Vor allem personenbezogene Daten unterliegen seither strikteren Vorgaben.

Oberstes vorgesehenes Ziel der DSGVO ist es, personenbezogene Daten (vor allem gesundheitsbezogene, genetische, biometrische und soziale) vor Missbrauch zu schützen. Bei der Verarbeitung dieser Daten sollten einige wichtige Grundsätze berücksichtigt werden, welche in Art. 5 Abs. 1 der DSGVO detailliert aufgeführt sind: Dazu gehören Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung und auch Richtigkeit.

Wesentliches und Tipps aus Sicht eines IT-Dienstleisters

Wie diese sehr allgemeinen Datenschutzgrundsätze in der immer digitaleren (Arzt-)Praxis konkret umzusetzen sind und auf welche Details und Richtlinien bei der Nutzung von gesundheitsbezogenen Personendaten zu achten ist, haben wir mit Thomas Holst besprochen. Thomas Holst ist Geschäftsführer bei der BT Nord Systemhaus GmbH, Teil der BT Nord Gruppe, einem führenden IT-Dienstleister mit Sitz in Husum, Flensburg und Hamburg, der kleine und mittelständische Unternehmen bei der Positionierung und Zukunftsausrichtung ihrer IT unterstützt.

Maßgeblich ist hier, neben der DSGVO, die IT-Sicherheitsrichtlinie nach § 75b SGB V. Die Umsetzung sollte laufend beachtet werden, damit es später bei einer möglichen Prüfung nicht zu bösen Überraschungen kommt. Thomas Holst sensibilisiert auf den Faktor Mensch: „Beim Umgang mit Patientendaten ist der Mensch das Einfallstor für Angreifer."

Datenschutzrisiko Mensch

Ein gutes Beispiel hierfür seien unbeabsichtigte Offenlegungen von Patientendaten im für Patienten zugänglichen Bereichen, wie z.B. dem Empfangsbereich. Im Speziellen nennt der Datenschutzexperte das Risiko von Datenschutzverstößen bei offen einsehbaren Dokumenten – beispielsweise bei Rezepten, die zur Unterschrift des Arztes am Tresen für den Patienten einsehbar liegen, oder noch geöffnete Röntgenbilder eines vorherigen Patienten im Behandlungsraum.

Wie kann das vom Personal ausgehende Risiko minimiert werden? „Entscheidend ist die regelmäßige Aufklärung und Schulung von Mitarbeitern in Form von IT-Sicherheits- und Datenschutzschulungen – bestenfalls jährlich", so Holst. Hier geht es darum aufzuzeigen, wie Mitarbeiter Ihre Passwörter gestalten und schützen (beispielsweise durch möglichst lange Passwörter, die jährlich angepasst werden sollten), wie sie echte von Malware-E-Mails unterscheiden können. Oder auch, wie sie ihre Cyberhygiene verbessern, zum Beispiel durch Passwort-geschützte Bildschirmschoner oder spezielle hygienische Dongles, bei denen der Bildschirm automatisch ge- und entsperrt wird, sobald der Nutzer seinen Platz einnimmt oder verlässt.

Weiterhin macht Holst auf die offiziellen Vorgaben zu Datenschutz und Cybersicherheit für Arztpraxen aufmerksam: Neben den gesetzlichen Regelungen (§ 75b SBG V) gibt es spezielle technische und organisatorische Anforderungen durch die KBV, die Arztpraxen befolgen sollten, um eine einwandfreie Praxis-IT zu gewährleisten. Diese können sich allerdings, je nach Größe der Praxis, unterscheiden. Prinzipiell gilt: je größer die Einrichtung, desto strikter die Vorgaben. Wichtig sei hierbei ebenso zu erwähnen, dass nur bestimmte durch die KBV anerkannte IT-Dienstleister Zertifizierungen ausstellen dürfen, die wiederum 12 Monate gültig sind.

Außerdem sollten IT-Hard- und Software ausschließlich neu im (medizinischen) Fachhandel und nur von seriösen Markenherstellern gekauft werden. Über (Online-)Flohmärkte erworbene Geräte seien No-Gos, da hier theoretisch beispielsweise bei USB-Mäusen Schadsoftware vorinstalliert sein kann, die die verbundene IT kompromittieren.

Holst beschreibt in diesem Zusammenhang wichtige Punkte zur IT-Sicherheit:
Dazu gehören unter anderem

- das Bestimmen von Verantwortlichkeiten (wer ist für den Datenschutz und die IT-Sicherheit zuständig?),
- das Identifizieren kritischer Ressourcen oder Daten (welche Daten sind besonders schützenswert?),
- das Durchspielen von Ernstfällen (was ist im Ernstfall zu tun?),
- die Nutzung von Security- und Analyse-Tools zur Angriffs-Prävention, -Detektion und -Reaktion (sind Virenschutz und Firewalls installiert sowie aktuell?),
- die Durchführung regelmäßiger Awareness-Trainings (Einhaltung des Datenschutzes, Sensibilisierung beim Umgang mit sensiblen Daten),
- und die Zusammenarbeit mit IT-Dienstleistern (um Anforderungen einzuhalten und Risiken zu minimieren).

Abschließend gehe es für Arztpraxen nicht einfach nur darum, gesetzliche Vorgaben zu erfüllen, sondern um den Schutz der eigenen Daten, die das Kapital einer jeden medizinischen Einrichtung ausmachen. Denn: „Keine Daten bedeutet kein Geld für die Praxis“, warnt Holst. Schließlich benötigen die Arztpraxen ihre erhobenen EDV-Daten, um Behandlungskosten gegenüber Leistungsträgern geltend zu machen.

Datenweitergabe bei Abrechnung über die PVS

Doch wie sieht es mit der Datenweitergabe für die Erstellung von Abrechnungen der PVS aus? Obwohl es unter dem neuen Recht eigentlich nicht mehr nötig wäre, raten wir zur Zeit noch, wo möglich, eine schriftliche Einwilligung von Patienten einzuholen – sicher ist sicher. Denn etliche Aufsichtsbehörden wollen die vom EU-Gesetzgeber gelockerten Vorschriften – zum Teil vielleicht auch nur aus Gewohnheit – in Deutschland leider weiterhin so restriktiv auslegen. Hierzu stellen wir als PVS/ Schleswig-Holstein • Hamburg Ihnen Formulare zur eigenen Verwendung zur Verfügung. In Deutsch und Englisch erhalten Sie diese unter www.pvs-se.de/einwilligung oder über unsere Materialbestellung für Mitglieder. Über die Mehrwerft® erhalten Sie die Einwilligungserklärungen in 6 weiteren Sprachen (Dänisch, Französisch, Polnisch, Spanisch, Türkisch und Russisch) zum Download oder als Print-Variante.

Datensicherheit mit der PVS

Unser Anspruch: Konsistenz, Vereinbarkeit und Plausibilität

Die PVS kümmert sich darüber hinaus für Sie um die Abrechnung und den Einzug von Honoraransprüchen für privatärztliche Leistungen. Wir beraten individuell bei allen anfallenden gebühren- und vertragsrechtlichen Fragestellungen – und legen großen Wert auf ordnungsgemäße Abrechnungen. Das bedeutet konkret: Konsistenz, Vereinbarkeit mit der Gebührenordnung und Plausibilität.

Unser Abrechnungs- und Datenschutz-Kodex - für Ihre Sicherheit

Gegenseitiges Vertrauen zwischen Ihnen als Arzt und uns als PVS ist das Fundament für eine erfolgreiche Partnerschaft. Denn wir verstehen uns als Mittler zwischen Ihnen, Ihren Patienten und Kostenträgern und besitzen eine besondere Pflicht zum verantwortungsvollen Datenhandling. Wir haben uns gefragt: Wie können wir diese bestmöglich erfüllen? Im Folgenden finden Sie wesentliche Inhalte unseres Kodex mit verbindlichen Grundsätzen zu Abrechnung und Datenschutz:

Schulungen für Mitarbeiter
Die PVS stellt sicher, dass ihre Mitarbeiter fachlich und datenschutzrechtlich immer up to date sind. Das erreichen wir durch regelmäßige Schulungen und Weiterbildungsmaßnahmen zum ärztlichen Gebühren- und Berufsrecht, Datenschutz und Berufsgeheimnis.

Datenschutz und Schweigepflicht
Unabhängig von der Frage, ob es einer ausdrücklichen Einwilligungserklärung der Patienten heute überhaupt noch bedarf: Voraussetzung für die Weitergabe von rechnungsrelevanten Informationen vom Arzt an die PVS ist in jedem Fall die **unabdingbar transparente Aufklärung des Patienten**. Hierzu stellt die PVS, wie oben erwähnt, **Muster** zur Verfügung, die Sie für ihre dokumentierte Aufklärung verwenden können.

Wir setzen zudem auf strikte Vertraulichkeit, sowohl in allen für die Abrechnung erforderlichen Informationen über Gesundheitszustand und ärztlichen Diagnosen des Patienten, als auch in allen Behandlungsfragen. Die personenbezogenen (digitalen) Daten von Patienten und Ärzten dürfen dabei **ausschließlich** dem Verwendungszweck der **konkreten Abrechnung und dem Forderungsmanagement** dienen. Diese werden dem Arzt frühestmöglich übergeben oder von der PVS zu gegebener Zeit nach gesetzlichen Vorschriften vernichtet.

Die PVS und der Datenschutz: Vertrauen ist alles

Die Bereiche Datenschutz und Cybersicherheit sind nicht nur für die allgemeine Digitalisierung von großer Bedeutung, sondern auch auf Mikroebene – also in jeder noch so kleinen Arztpraxis – wichtige Voraussetzungen für gegenseitiges Vertrauen zwischen Arzt und Patient.

Wir machen dieses komplexe Thema für Sie greifbar, zum Beispiel in Form von Musterformularen oder über die für unsere Mitglieder kostenlose Broschüre „DSGVO in der Praxis“, die Sie ebenfalls über die Mehrwerft® bestellen können.

Schaffen Sie sowohl für die Patientenbetreuung als auch für alle anderen wichtigen Aufgaben Freiräume in Ihrer Praxis, indem Sie die Privatabrechnung über die PVS/ Schleswig-Holstein • Hamburg bearbeiten lassen. Vereinbaren Sie hierzu einfach einen kostenlosen und unverbindlichen Beratungstermin mit unseren Mitarbeitern.