

lässt sich dies über den Anamnesebogen regeln. Allerdings gilt: Wird die Einwilligung wie hier in Zusammenhang mit anderen Erklärungen/Sachverhalten eingeholt, muss sie deutlich von diesen abgegrenzt werden, damit der Patient erkennt, worin er einwilligt. Außerdem muss sie in klarer, einfacher Sprache verfasst werden. Wer Patienten auch an Termine erinnern will – etwa per Brief, Mail oder SMS – der sollte dies noch einmal getrennt von der Einwilligung zur normalen Verarbeitung der Daten in der Praxis-EDV aufführen.

Zweckbindung der Daten: Die Praxis darf die beim Patienten erhobenen Daten, dazu zählen auch die Diagnosen, immer nur zum Zweck der Leistungserbringung und Abrechnung erheben. Wer bei privatversicherten Patienten die Abrechnung über einen externen Dienstleister laufen lässt, sollte sich hierfür beim Patienten eine getrennte Einwilligungserklärung einholen. Vorsicht ist bei der Weitergabe von Daten zu Studienzwecken geboten. Auf der sicheren Seite sind Ärzte nur dann, wenn sie den Patienten ebenfalls vorher um sein Einverständnis bitten. Allerdings bietet das deutsche Datenschutzrecht (§ 27 DSAnpUG-EU) hier dank Öffnungsklausel in der EU-Verordnung für wissenschaftliche Zwecke etwas mehr Spielraum: In diesem Fall kann auf eine gesonderte be-

ziehungsweise erneute Einwilligung verzichtet werden, sofern die Interessen des Verantwortlichen für die Datenverarbeitung die Interessen der jeweils betroffenen Person an seinem Ausschluss „erheblich überwiegen“. Damit scheint der Gesetzgeber vor allem die künftigen Möglichkeiten von Big-Data-Anwendungen im Hinterkopf gehabt zu haben. Diese würden mit einer allzu scharfen Einwilligungspflicht nämlich bereits im Keim erstickt. Vorsicht ist für Ärzte überdies beim Datenaustausch in Ärztenetzen oder Kooperationen geboten: Auch hier sollte vor jeglicher Datenweitergabe der Patient explizit zustimmen.

Das Recht auf Löschen: Hauptsächlich getrieben durch die Entwicklungen im Internet und in den Sozialen Medien mit schnellen Unwahrheitsbehauptungen per Knopfdruck wurde in der EU-Verordnung das Recht von Privatpersonen auf ein Löschen ihrer Daten gestärkt. Für Ärzte ist dies insofern relevant, dass sie vor allem bei einer Datenverknüpfung mit anderen Stellen – etwa in Kooperationen, oder wenn sie Praxisdaten in gesicherten Clouds ablegen, schauen müssen, wann und welche Daten eventuell zu löschen sind, wenn ein Patient dies wünscht. Nicht davon betroffen sind allerdings Daten, die Ärzte zum Nachweis der Leistungserbringung oder aus Haftpflichtgründen aufbewahren

müssen. Diese Datensicherung darf dann allerdings nur begrenzt und in bestimmten Fällen zugänglich sein.

Portabilität der Daten: Hier werden die Praxis-EDV-Anbieter gefragt sein, geeignete Formate zur Verfügung zu stellen, auch eine Telematikinfrastruktur könnte hier künftig ihren Beitrag leisten. Denn die Patienten haben nach § 20 der EU-DS-GVO das Recht, die sie betreffenden Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“ und diese Daten ohne Medienbrüche an Dritte zu übermitteln. Damit machen sich EU-Parlament und -Rat – sicherlich unwissend – auch für die elektronische Patientenakte stark.

Schwachstelle Datensicherung?

Unbedingt prüfen sollten Praxen ihre Datensicherung, denn künftig sind sie verpflichtet, Verletzungen des Schutzes personenbezogener Daten – wie sie etwa bei Phishing-Attacken vorkommen können – innerhalb von 72 Stunden nach Bekanntwerden an den Bundesdatenschutzbeauftragten zu melden. Dies gilt nur dann nicht, wenn voraussichtlich keine Gefahr von Rechtsgütern der betroffenen Personen besteht. Die vom Schutzleck betroffenen Patienten müssen übrigens, wenn sich aus einem Datenklau Nachteile für sie ergeben könnten, ebenfalls informiert werden. Also sollten die technisch gängigen Vorkehrungen zum Schutz von Praxisdaten erfüllt werden: Firewall, aktuelle Version des Betriebssystems, Virens Scanner.

Wo möglich, sieht die EU-Verordnung auch eine Anonymisierung oder zumindest Pseudonymisierung von Daten vor – dies sollten Praxen vor allem beim elektronischen Austausch von Patientendaten mit anderen Leistungserbringern bevorzugen. Der elektronische Arztbrief über einen Kommunikationsdienst wie KV-Connect etwa ist wesentlich sicherer als eine ungeschützte E-Mail oder gar ein Fax.

Als Sanktionen bei Datenschutzverstößen drohen nach der EU-Verordnung Unternehmen, zu denen Arztpraxen zu zählen sind, Geldbußen in Höhe von bis zu 4 % des gesamten Jahresumsatzes des vorangegangenen Geschäftsjahres.

Rebekka Höhl

KV-Connect zum Nulltarif – Telematik macht's möglich

Niedergelassene Ärzte sollten die Telematikinfrastruktur (TI) als Einstieg für die Arbeit mit dem elektronischen Arztbrief und andere sinnvolle Anwendungen nutzen, die über den sicheren Kommunikationskanal der Kassenärztlichen Vereinigungen KV-Connect laufen. Das empfiehlt der Telematik-Experte der KV Nordrhein und Berater der KV Telematik Gilbert Mohr. „Mit der TI-Technologie lässt sich KV-Connect quasi beiläufig und ohne Mehrkosten installieren“, so Mohr auf dem Kongress „Medizinische Versorgung im digitalen Zeitalter“ der KV Westfalen-Lippe im Oktober 2017. Die KBV hat vereinbart, dass

die Praxen, die einen gematik-Konnektor erhalten, über die Verbindung zur TI auch Systeme wie KV-Connect erreichen können, berichtete er.

Die zwischen KBV und Krankenkassen abgeschlossene Finanzierungsvereinbarung für die TI sieht nicht nur Pauschalen für den Kauf und die Installation der Konnektoren und der Lesegeräte vor. Hinzu kommt über fünf Jahre eine Pauschale für die Betriebskosten: 298 € pro Quartal bis zum zweiten Quartal 2018 und danach 248 € pro Quartal. „Damit kann man KV-Connect finanzieren“,

Ilse Schlingensiepen