Praktischer Datenschutz in der Zahnarztpraxis

Text: Carsten Knoop

Wenn Sie nach Abschluss des Studiums eine Zahnarztpraxis eröffnen oder übernehmen möchten, werden Sie aus Sicht des Datenschutzes zur „verantwortlichen Stelle". Dabei gilt in Deutschland – wie auch im Rest Europas – auch für alle Freiberufler ab Mai 2018 die EU-Datenschutz-Grundverordnung (EU-DSGVO), welche die grundsätzlichen Regelungen samt Bußgeldern (bis 20 Mio. EUR) festlegt und das bisherige Bundesdatenschutzgesetz (BDSG) ablöst.

Die EU-DSGVO sowie lokale Ergänzungsregelungen zum Datenschutz gelten dabei unabhängig von der ärztlichen Schweigepflicht, welche nur eine zusätzliche Konkretisierung des Datenschutzes darstellt. In diesem Artikel sind die wesentlichen Merkmale und Herausforderungen im Umgang mit personenbezogenen Daten von Mitarbeitern und Patienten erläutert, um Ihnen den datenschutzkonformen Start in die Selbstständigkeit zu erleichtern.

Übernahme einer Praxis samt Patienten(daten)?

Wer die Möglichkeit hat, eine gut laufende Praxis übernehmen zu können, kann erheblich von einem bereits etablierten Patientenkollektiv profitieren. Allerdings gilt es, einige Datenschutzaspekte zu berücksichtigen. So kann zwar vertraglich die komplette Einrichtung der Praxis übernommen werden, die Daten von Patienten dürfen aber ohne Weiteres nicht von einem Zahnarzt zum anderen weitergegeben werden.
Die Aufzeichnungspflicht im Rahmen von § 630 f BGB erstreckt sich stets auf den behandelnden Arzt und greift somit direkt in das vertragliche Verhältnis zwischen Patient und Arzt ein. Eine Weitergabe an Dritte, und somit auch an einen Nachfolger, kann nur mit Zustimmung des Patienten erfolgen. Entsprechend müssen alle Daten, sowohl in Papierform als auch elektronisch, die nicht per Einwilligung auf den neuen Praxisinhaber übergehen dürfen, aber dennoch mindestens zehn Jahre nach Behandlungsende aufbewahrt werden müssen, im Eigentum des „alten Behandlers" verbleiben. Patientendaten, die per schriftlicher Einwilligung auf den „neuen Behandler" übertragen werden sollen, dürfen dann vom neuen Praxisinhaber gemäß den gesetzlichen Anforderungen genutzt werden.

Praxisorganisation und Datenschutz

Neben der Frage der Datenübernahme sollte auch geklärt werden, ob ein Datenschutzbeauftragter gemäß EU-DSGVO (bzw. den strengeren Regeln aus dem bald neu erlassenen Bundesdatenschutzgesetz BDSG [neu]) bestellt werden muss. Das ist immer dann der Fall, wenn mehr als neun Personen mit der automatisierten Verarbeitung oder mehr als 20 Personen generell mit der Verarbeitung personenbezogener Daten beschäftigt sind. Haben also mehr als neun Personen (egal, ob Azubi, Mitarbeiter oder Zahnarzt) Zugang zu elektronischen Patientendaten, z. B. zur Praxissoftware, wird ein Datenschutzbeauftragter benötigt. Ansonsten erst, wenn mehr als 20 Personen z. B. mit Papierakten der Patienten arbeiten.
§ 203 StGB regelt die Verschwiegenheit der Ärzte gegenüber Dritten und stellt eine Verletzung unter Strafe. Dies ist aus Sicht des Datenschutzes stets der Fall, wenn der Zugriff durch Dritte auf Patientendaten möglich ist, oder faktisch durchgeführt wird. Der Gesetzgeber sieht vor, dass personenbezogene Daten (hierzu zählen natürlich auch alle Patienten- und Mitarbeiterdaten) nur dann von Dritten verarbeitet werden dürfen, wenn dafür entsprechende Rechtsgrundlagen eingehalten werden. Hierzu zählt z. B. neben einer Einwilligung (Entbindung von der Schweigepflicht) in begrenztem Umfang auch die Verarbeitung im Auftrag gemäß Art. 28 EU-DSGVO auch als Auftragsdatenverarbeitung bezeichnet.
Folgende Sachverhalte fallen in den Bereich der Auftragsdatenverarbeitung, da es sich im Regelfall nicht um Erfüllungsgehilfen (z. B. ZFA oder ZMV) handelt:

- IT-Dienstleister, welche die Einrichtung und Wartung Ihrer Praxissysteme durchführen,
- Softwarehersteller und andere Dienstleister, welche mit Fernwartungszugang und Zugriffsmöglichkeit auf Patientendaten ausgestattet sind,
- Cloud-Anbieter, bei denen personenbezogene Daten gespeichert werden,
- Entsorgungsdienstleister, welche Patientenakten vernichten.

In der Praxis hat sich folgendes Vorgehen zur Einhaltung der gesetzlichen Verpflichtungen bewährt:

1. Bei Einbindung externer IT-Dienstleister muss eine vertragliche Verpflichtung zum Datenschutz gemäß den Vorgaben von Art. 28 EU-DSGVO eingefordert werden. Hierzu sind vom Auftragnehmer diverse technische und organisatorische Maßnahmen zum Schutz der Daten nachzuweisen. Im besten Fall hat der Dienstleister gar keinen Zugriff auf Patientendaten, da dies problematisch mit den Verschwiegenheitspflichten gem. § 203 StGB gesehen werden kann.
2. Soweit möglich sollten alle Datenträger (z. B. Festplatten und USB-Sticks) in der Praxis verschlüsselt sein. Damit kann

sichergestellt werden, dass die Patientendaten auch beim Austausch eines Gerätes, bei Diebstahl oder Einbruch, Dritten nicht offenbart werden.

3. Werden für die Praxissoftware regelmäßig Sicherheits- und Funktionsupdates eingespielt, so muss darauf geachtet werden, dass dies ohne Kenntnis der personenbezogenen Patientendaten erfolgt. Hierzu ist im Regelfall eine Fernwartung nur unter Aufsicht zulässig.
4. Alle Mitarbeiter sollten eigene Benutzernamen und individuelle, sichere Passwörter erhalten. Damit kann sichergestellt werden, dass diese nur die für ihren Arbeitsbereich notwendigen Datenzugriffe erhalten. IT-Systeme sind zu sperren, wenn der Arbeitsplatz verlassen wird.
5. Der Zugriff auf das Internet birgt besondere Risiken und sollte soweit es geht minimiert werden. Hierzu kann eine Trennung von Praxis-PC und Internet-PC erfolgen oder ein Schutz über Proxyserver, Firewalls und VPN-Zugänge eingerichtet werden. Der Schutz mittels Firewall und Antivirenschutzsoftware gehört heute zum Standard und sollte regelmäßig aktualisiert werden.
6. Per E-Mail weitergegebene Patientendaten (z. B. digitale Röntgenaufnahmen) sollten verschlüsselt versendet werden (im einfachsten Fall reicht eine ZIP-Datei aus).
7. Bei der Entsorgung von Papier und Datenträgern ist auf eine datenschutzkonforme Vernichtung zu achten. Wer einen Dienstleister damit beauftragen möchte, sollte auf die Zertifizierung nach DIN 66399 und die Einhaltung von Schutzklasse 3 und Sicherheitsstufe 4 achten.

Patientendatenschutz

Im datenschutzrechtlichen Sinne gelten für den Umgang mit Patientendaten in vielen Fällen die Vorgaben der SGB. Weiterhin gelten folgende Grundsätze:

Bei der Identifikation von (Privat-)Patienten sollten die Versichertenkarten genutzt werden. Eine Kopie von Personalausweisen ist unzulässig. Bei Bedarf können die Daten vom Personalausweis nach dem Gebot der Datensparsamkeit und Erforderlichkeit (nur das, was auch benötigt wird) abgeschrieben werden.

Auskünfte über Patientendaten dürfen grundsätzlich nur an den Patienten selbst erfolgen. Dieser hat ein Auskunftsrecht über alle zu seiner Person vorliegenden Daten. Dritten, auch Angehörigen, steht dieses Auskunftsrecht nicht zu. Möchte der Patient Sie als Zahnarzt in die Lage versetzen Dritten gegenüber Auskünfte zu erteilen, so muss er Sie – am besten schriftlich – von der Verschwiegenheitspflicht entbinden. Dies muss z. B. auch bei Anfragen von Versicherungen stets nachgewiesen werden. Gleiches gilt auch für die Weitergabe von Kostenvoranschlägen, Heil- und Kostenplänen oder dem Paradontalstatus an Versicherungen bzw. an die Träger der örtlichen Sozialkassen.

Bei der Abrechnung von Leistungen über die Kassenzahnärztliche Vereinigungen sind im Regelfall keine besonderen Vorgaben einzuhalten, da diese regelmäßig über eine gesetzliche Abrechnungsgrundlage verfügen. Anders sieht dies jedoch bei Einbezug von privaten Abrechnungsstellen aus. Hier muss eine Einwilligung des Privatpatienten vorliegen, da mit den Rechnungsdaten oft auch Informationen zur Diagnose und Behandlung verarbeitet werden, welche nicht über einen Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 EU-DSGVO abgedeckt sind.

Bedingungen für Einwilligungen

Gemäß Art. 7 EU-DSGVO müssen zukünftig folgende Bedingungen bei der Einholung einer Einwilligung gewährleistet sein, damit diese gültig und damit rechtswirksam ist:

- Die Einwilligung muss in verständlicher Form und einfacher Sprache gehalten sein.
- Eine freie Entscheidung des Betroffenen (Patient oder Mitarbeiter) muss vorliegen.
- Die Information über den jederzeitigen Widerruf muss enthalten sein.
- Ausführliche, erkennbare und festgelegte Information des Betroffenen gemäß Art. 13 bzw. 14 EU-DSGVO über Zweck und Verarbeitung der Daten müssen gemacht werden.
- Der Nachweis einer Einwilligung muss gewährleistet sein (Dokumentation).

Umgang mit Mitarbeiterdaten

Für die Daten eines jeden Beschäftigten gilt § 32 BDSG für den Beschäftigtendatenschutz. Aus Sicht des Datenschutzes ist es dabei unerheblich, ob es sich um Vollzeitkräfte, Teilzeitkräfte oder Auszubildende handelt. Grundsätzlich sollten die gleichen Sicherheitsvorkehrungen wie bei den Patientendaten eingehalten werden, allerdings sind einige Abweichungen zu berücksichtigen.

Einsicht und Bearbeitung von Mitarbeiterdaten (z. B. Personal- und Bewerbungsdaten, Gehaltsabrechnungen) sind nur für den Praxisinhaber oder die damit betraute ZMV bzw. den Steuerberater oder das Lohnabrechnungsbüro zulässig. Bedenken Sie also die unterschiedlichen Berechtigungen, wenn diese Daten elektronisch vorliegen oder lassen sie diese getrennt von den Patientenakten unter Verschluss. Weiterhin gilt, dass Sie lediglich die Daten über Ihre Mitarbeiter erfragen und verwenden dürfen, die auch wirklich für das Arbeitsverhältnis notwendig sind. Dazu zählen generell keine Fotos, private Daten oder Gesundheitsdaten (Ausnahmen gelten z. B. bei Schwangerschaft). Möchten Sie die Fotos Ihrer Mitarbeiter z. B. im Internet veröffentlichen, ist dies stets nur mit deren Einwilligung möglich.

Neben der Unterweisung in die Verschwiegenheitspflichten nach § 7 Abs. 3 der Musterberufsordnung für Zahnärzte bzw. der Berufsordnungen der jeweiligen Landeszahnärztekammer und deren Dokumentation, müssen die Mitarbeiter auch auf das Datengeheimnis gemäß § 5 BDSG verpflichtet werden. Dies sollte gleich mit Ausfertigung des Arbeitsvertrages erfolgen und anschließend um Sicherheitseinweisungen im Umgang mit der Praxis-IT ergänzt werden.

KONTAKT

Dipl. Wirt.-Inf. Carsten Knoop, M.Sc.
audatis Consulting GmbH
Leopoldstraße 2–8
32051 Herford
Tel.: 05221 85496-91
info@audatis.de
www.audatis.de