DATENSCHUTZ

Löschkonzepte in der Physiopraxis nach DSGVO

von RA Rainer Horbach, Datenschutzbeauftragter, Aachen, www.dataprivat.de

Wenige Fragen haben bei Einführung des neuen Datenschutzrechts für so viel Verunsicherung gesorgt, wie die Frage nach der Zulässigkeit von Speicherung und Löschung von Daten. Dabei sind die meisten Fragestellungen gar nicht neu. Entsprechend genau schauen die Aufsichtsbehörden hin, wenn es um die Einhaltung der Speicher- und Löschfristen geht. Ein Löschkonzept hilft Ihnen, die datenschutzrechtlichen Vorgaben zu erfüllen.

Löschkonzept als Teil der Datenschutz-Compliance

Die wenigsten Praxen haben bisher ein Löschkonzept

Nach dem Grundsatz der Speicherbegrenzung ist jede Praxis verpflichtet, Richtlinien und Verhaltensweisen zur Löschung von Daten als Teil des Datenschutzkonzeptes festzulegen. Das ist zwar keineswegs neu. Die Erfahrung der Datenschutzberatung zeigt jedoch: Nur ein Bruchteil der Praxen hat diese Vorgaben bisher entsprechend umgesetzt.

Quelle: dataprivat.de | Grafik: IWW Institut

Speicherfristen festlegen

Dauer der Datenspeicherung richtet sich nach deren Zweck

Dem Recht, Daten zu speichern, steht die Pflicht zur Löschung gegenüber, wenn die Daten nicht mehr benötigt werden. Die zulässige Höchstdauer der Speicherung folgt aus dem Zweck und der Rechtsgrundlage der Speicherung. Für alle in der Praxis verarbeiteten Kategorien von Daten müssen Löschfristen definiert werden (vgl. Art. 30 Abs. 1 f DSGVO). Kann wegen der Natur der Daten eine feste Frist nicht von vornherein definiert werden, so sind die Umstände zu definieren, bei deren Vorliegen die Daten zu löschen sind.

Zehnjährige Speicherfrist

Behandlungsdokumentation

Alle Daten, die mit der Behandlungsdokumentation zusammenhängen, dürfen auf Grundlage des Behandlungsvertrags gespeichert und müssen zehn Jahre, gerechnet ab Abschluss der Behandlung, aufbewahrt werden (§ 630f Abs. 2 Bürgerliches Gesetzbuch [BGB]; zum Umgang mit Patientendaten bei einer Praxisübergabe siehe PP 01/2019, Seite 18). Nach Ablauf der zehnjährigen Aufbewahrungsfrist müssen die Daten aus der Behandlungsdokumentation grundsätzlich gelöscht werden.

Rechnungen und alle Daten und Unterlagen, die mit der Leistungsabrechnung im Zusammenhang stehen, müssen ebenfalls zehn Jahre gespeichert werden.

Lohn- und Gehaltsunterlagen

Alle Unterlagen, die mit den Löhnen der Arbeitnehmer in Verbindung stehen, müssen ebenfalls zehn Jahre aufbewahrt werden, also: Lohnabrechnungen, Reisekostenabrechnungen, Überstundenlisten, Kontoauszüge, Gehaltslisten, Jahreslohnnachweise für die Berufsgenossenschaft, Unterlagen zur Fahrtkostenerstattung, AU-Bescheinigungen, soweit lohnwirksam.

Sechsjährige Speicherfrist

Unterlagen und Dokumente zu Gerichtsverfahren müssen z. B. sechs Jahre aufbewahrt werden. Ebenso: Die sonstigen Personalunterlagen, soweit keine kürzeren Fristen gelten.

Sonderfälle

Terminkalender

Der Terminkalender der Praxis sollte ebenfalls sechs Jahre aufbewahrt werden, um auch nachträglich noch nachvollziehen zu können, welcher Therapeut wann welche Leistungen abgegeben hat.

Weitere Unterlagen mit besonderer Löschfrist

- Arbeitszeitnachweise sind zwei Jahre aufzubewahren (§ 16 Abs. 2 Arbeitszeitgesetz).
- Bewerbungsunterlagen abgelehnter Bewerber sollten sechs Monate nach Bekanntgabe der Entscheidung gelöscht werden.
- Gesundheitszeugnisse der Mitarbeiter und Belehrungen nach IfSG sind nach dem Ausscheiden des Mitarbeiters aus der Praxis zu löschen/vernichten.
- Mutterschutzunterlagen müssen zwei Jahre aufbewahrt und dann gelöscht werden (§ 19 Abs. 2 Mutterschutzgesetz).

Längere Speicherung in Einzelfällen möglich

Unterlagen als gerichtliches Beweismittel

In Einzelfällen ist auch eine längere Speicherung möglich, sofern dies zur Verteidigung von Rechten nötig ist, z. B. weil ein Klageverfahren läuft oder angedroht worden ist (PP 03/2018, Seite 16).

PRAXISTIPP | Praxen können zudem die Behandlungsdokumentation auch länger als zehn Jahre speichern, wenn sie die Patienten ausdrücklich, z. B. in der Datenschutzinformation, darauf hinweisen (§ 35 Abs. 2 BDSG). Nach zehn Jahren muss die Verarbeitung jedoch eingeschränkt werden (vgl. Art. 18 DSGVO).

Festlegen von Prüfintervallen

Prüfintervalle ggf. anlassbezogen festlegen

Insbesondere der Bestand an Patientenunterlagen sollte jährlich auf Löschungsreife hin überprüft werden, sofern die Praxis nicht, wie oben beschrieben, die Behandlungsdokumentation länger als zehn Jahre speichert. Auch alle Unterlagen im Zusammenhang mit der Abrechnung und der Besteuerung sowie die Personalunterlagen sollten turnusmäßig auf Löschungsreife geprüft werden. Ansonsten sollten anlassbezogene Prüfintervalle festgelegt werden, z. B. bei Bewerbungsverfahren.

Verantwortlichkeiten mit festlegen

PRAXISTIPP | Bei Festlegung der Prüfintervalle sollte stets auch gleich bestimmt werden, wer die Daten zu prüfen und sie ggf. anschließend zu löschen hat. Wegen der besonderen Verantwortung und der therapeutischen Schweigepflicht, sollte die Prüfung und Löschung von Patientenakten dem Therapeuten vorbehalten sein.

Verfahren für Löschanfragen definieren

Ggf. Datenschutzbeauftragten hinzuziehen

Nach der DSGVO können die von Datenverarbeitung Betroffenen die Löschung ihrer Daten verlangen, sofern kein Grund mehr für die Speicherung besteht. In der Betriebsorganisation der Praxis sollte festgelegt sein, wie mit solchen Anfragen umgegangen wird und insbesondere, welche Mitarbeiter sie bearbeiten. Es muss nämlich vonseiten der Praxis sichergestellt sein, dass nur Daten gelöscht werden, zu deren Aufbewahrung keine Pflicht mehr besteht. Ist ein Datenschutzbeauftragter in der Praxis benannt, sollte dieser bei Löschanfragen immer hinzugezogen werden.

Löschverfahren bestimmen

Datenträger nach DIN 66399 vernichten

Zur Wahrung der Vertraulichkeit und der Datensicherheit sollten Verfahren für die Datenlöschung definiert werden. Datenträger sollten immer nach der DIN 66399 vernichtet werden. D. h., dass Papierakten immer mindestens mit einem Aktenvernichter der Sicherheitsstufe P-4 oder höher vernichtet werden müssen (PP 01/2019, Seite 17). Auch die Inanspruchnahme eines Dienstleisters, der eine entsprechende Sicherheit gewährleistet, ist möglich. In dem Fall ist ein Vertrag über die Auftragsverarbeitung zu schließen.

Elektronische Datenträger, wie externe Festplatten, USB-Sticks, ganze PCs, o. Ä., dürfen niemals einfach entsorgt werden. Ein einfaches Löschen – Ablegen von Dateien in den Papierkorb – ist durch entsprechende Software leicht rückgängig zu machen. Die Datenträger sind daher entweder physisch zu zerstören oder aus Sicherheitsgründen vorzugswürdig mit einem Löschprogramm wie etwa DBAN oder Secure Erase zu löschen.

FAZIT | Jede Praxis ist verpflichtet, ein Löschkonzept zum Teil des Datenschutzkonzepts zu machen und dieses zu dokumentieren. Auch die einzelnen Löschvorgänge sollten dokumentiert werden. Unter Beachtung der vorgenannten Hinweise, lässt sich ein DSGVO-konformes Datenlöschkonzept in jeder Praxis mit vertretbarem Aufwand implementieren.