Foto: © Coloures-Pic/Fotolia.com

Der Umgang mit Patientendaten im Hinblick auf die DSGVO – „State of the Art 2018“

Patientenbezogene Daten (z. B. Anamneseangaben, Befunde, Behandlungsempfehlungen) sind besonders schützenswert. Die datenschutzrechtlichen Bestimmungen, die es in einer Zahnarztpraxis zu beachten gilt, sind mannigfaltig. Einen Problemkreis stellt beispielsweise die unbefugte Weitergabe der Gesundheitsdaten dar. Darüber hinaus ist auch § 203 StGB („Verletzung von Privatgeheimnissen“) zu beachten. Dieser Verschwiegenheitsverpflichtung wegen müssen Zahnärzte dafür sorgen, dass die Patientendaten nicht von Unbefugten zur Kenntnis genommen werden können (s. dazu auch NZB 2/2018 S. 40). Dieser Artikel soll einen Überblick geben, unter welchen Voraussetzungen sensible Patientendaten weitergegeben werden dürfen und welche Möglichkeiten hierfür zur Verfügung stehen.

1 Allgemeine Voraussetzungen zur Verarbeitung personenbezogener Daten.

Die Verarbeitung und somit auch die Übermittlung von Daten stellt nach der Datenschutz-Grundverordnung (DSGVO) ein Verbot mit Erlaubnisvorbehalt dar.
Die Verarbeitung von personenbezogenen Daten ist danach erst einmal generell verboten. Das Verbot kann nur durch eine Erlaubnis/Einwilligung zur Verarbeitung aufgehoben werden (es muss ein „Erlaubnisstand“ geschaffen werden). Art. 6 DSGVO unterscheidet hierbei die Möglichkeit der Einwilligung von der gesetzlichen Erlaubnis.

1.1 Die Einwilligung des Patienten

Gem. Art. 6 Abs. 1 lit. a) DSGVO ist die Verarbeitung von personenbezogenen Daten zulässig, wenn der Patient eine entsprechende Einwilligung erteilt.

Für alle diejenigen Verarbeitungen, für die kein gesetzlicher Erlaubnistatbestand besteht, ist immer die Einwilligung des Patienten erforderlich.

Beispiele: Einwilligung in die Nutzung eines Recall-Systems, die Abrechnung über externe Verrechnungsstellen, Konsultation Dritter.

→ Musterformulare für Einwilligungserklärungen finden Sie auf unserer Internetseite www.zkn.de unter der Rubrik Datenschutz → Checkliste zum Datenschutz.

Die Einwilligung ist in Art. 4 Nr. 11 DSGVO legal definiert als jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Voraussetzungen einer rechtswirksamen Einwilligung (Art. 7 DSGVO) in die Verarbeitung sind also:

- Unmissverständlichkeit der Einwilligung (Einwilligung kann schriftlich, mündlich oder durch schlüssiges Handeln erteilt werden),
- Bestimmtheit der Einwilligung (Pauschalierungen oder Blankoeinwilligungen genügen nicht),
- Information des Betroffenen (z.B. Zweck und Rechtsgrundlage der Verarbeitung),
- Freiwilligkeit der Einwilligung (echte Wahlmöglichkeit des Betroffenen, Kopplungsverbot),
- Widerruflichkeit der Einwilligung (für die Zukunft jederzeit möglich; der Widerruf muss genauso einfach möglich sein wie die Erteilung der Einwilligung).

Erfolgt die Einwilligung nicht in schriftlicher Form, ist darauf zu achten, dass zu Beweiszwecken die Abgabe einer Einwilligungserklärung dokumentiert werden sollte, da der Praxisinhaber als Datenschutzverantwortlicher für die Abgabe der Einwilligungserklärung die Beweislast trägt.

Bereits eingeholte Einwilligungen bleiben bestehen, sofern diese der Art nach der Datenschutzgrundverordnung entsprechen.

→ Bitte überprüfen Sie bereits eingeholte Einwilligungserklärungen. Die grundsätzlichen Anforderungen an die Wirksamkeit einer Einwilligung haben sich durch das Inkrafttreten der DSGVO nicht verändert. Sollten Sie sich dennoch nicht sicher sein, ob diese den oben aufgeführten Voraussetzungen genügt, lassen Sie sich eine neue Einwilligung erteilen.

1.2 Die allgemeinen gesetzlichen Erlaubnistatbestände

Art. 6 Abs. 1 lit. b-f) DSGVO enthält die allgemeinen gesetzlichen Erlaubnistatbestände. Beispielhaft lassen sich die Verarbeitung zur Erfüllung des Behandlungsvertrages oder zur Erfüllung rechtlicher Pflichten benennen.
Auch Art 9 Abs. lit. h gibt einen gesetzlichen Erlaubnistatbestand in Form der Gesundheitsvorsorge
Eine rechtliche Verpflichtung zur Verarbeitung besteht beispielsweise bei der gesetzlichen Unfallversicherung (§§201 ff. SGB VII), bei der Übermittlung an die Kassenzahnärztliche Vereinigung (§ 298 SGB V) oder im Rahmen des Infektionsschutzgesetzes (§§ 6 ff. IfSG). Auch zur Wahrung berechtigter Interessen des Betroffenen ist die Verarbeitung rechtmäßig. Dies ist beispielsweise bei der zivilrechtlichen Geltendmachung von Honorarforderungen oder bei Schadensersatzforderungen der Fall.

2 Weitergabe von Patientendaten an Dritte

Nicht selten kann sich im Praxisalltag die Notwendigkeit ergeben, Patientendaten an Dritte weiterzugeben. So kann es z.B. passieren, dass der neue Zahnarzt eines verzogenen Patienten die Behandlungsunterlagen anfordert. Die Möglichkeiten Patientendaten zu übermitteln, sind in der vergangenen Zeit explodiert. Deshalb stellt sich die Frage, ob und wie diese an Dritte weitergegeben werden dürfen und auf welchem Wege dies geschehen kann, um den gesetzlichen Anforderungen zu genügen. In diesem Zusammenhang darf nicht vergessen werden, dass vor einer Übermittlung von Patientendaten grundsätzlich eine Entbindung von der ärztlichen Schweigepflicht durch den Patienten erforderlich ist. Bezogen auf unser Beispiel bedeutet dies, dass der bisherige Zahnarzt die angeforderten Informationen nur übermitteln darf, wenn ihm eine ausdrückliche Schweigepflichtsentbindung vorliegt.

2.1 Persönliche Übergabe an den Patienten

Sie können dem Patienten seine Unterlagen (z.B. Überweisung, Röntgenbild) persönlich übergeben, beispielsweise indem Sie das Röntgenbild auf einen CD-/DVD-Rohling brennen oder auf einem USB-Stick speichern. Bei der Nutzung eines USB-Stick sollte jedoch darauf geachtet werden, dass dieser vor seiner ersten Benutzung original verpackt ist, um mögliche Schadsoftware zu umgehen. Außerdem gilt es zu bedenken, dass in vielen EDV-Systemen ▸▸

Foto: © kras99/Fotolia.com

- die USB-Anschlüsse gesperrt sind, weil insbesondere über USB-Sticks Schadsoftware auf die Rechner bzw. in die Praxisnetzwerke gelangen könnte. Diese Gefahr besteht nicht bei der Dateiübermittlung per CD-/DVD-Rohlingen. Bei der Übergabe an den Patienten entfällt natürlich die Notwendigkeit einer Entbindung von der ärztlichen Schweigepflicht.

2.2 Post

Patientendaten können in einem verschlossenen Umschlag auf dem Postweg verschickt werden. Hier kommt das in § 202 StGB verankerte Briefgeheimnis zum Tragen. Gem. § 202 StGB ist es verboten, verschlossene Schriftstücke zu öffnen und zu lesen, wenn diese nicht zur Kenntnis bestimmt sind. Deshalb gilt dieser Übermittlungsweg immer noch als sehr sicher.
Enthält die Adresse einen Vertraulichkeitsvermerk (z.B. „persönlich", „vertraulich", „privat"), darf die Post ausschließlich von dem Adressaten geöffnet werden. Wird eine Postsendung mit einem Vertraulichkeitsvermerk unautorisiert durch eine dritte Person geöffnet, ist das eine Verletzung des Briefgeheimnisses und kann strafrechtliche Folgen haben.

2.3 Telefax

Gerade im Hinblick darauf, dass es sich bei Patientendaten um personenbezogene, sensible Daten handelt, sollte eine Übermittlung von Patientendaten per (Tele)fax grundsätzlich nicht erfolgen. Es besteht die Gefahr, dass es zu einer Fehlübertragung kommt, z.B. durch einen „Dreher" in der Faxnummer. Überdies erfolgt die Übertragung unverschlüsselt. Sollte diese Versandart in Einzelfällen notwendig sein, müssen Maßnahmen getroffen werden, die einen Zugriff Unbefugter auf diese Daten verhindern. So sollte eine angemessene Sorgfalt bei der Eingabe der Zielnummer erfolgen, indem sich der Absender vor dem Versenden noch einmal über die Richtigkeit der Zifferneingabe vergewissert. Der Absender sollte sich des Weiteren vor dem Absenden des Dokuments mit dem Empfänger absprechen, dass das Fax direkt vom gewünschten Adressaten entgegengenommen und nicht von unautorisierten Dritten eingesehen werden kann.

2.4 E-Mail – digitale Kommunikation

Entscheiden Sie sich für eine digitale Kommunikation, müssen Sie auf Grund des hohen Schutzbedarfes von Gesundheitsdaten zumindest die Datei(en) mit personenbezogenen Informationen, die Sie mit dem E-Mail versenden wollen, sicher verschlüsseln. Erst dann darf der Versand erfolgen.

Wenn nicht das gesamte E-Mail – also auch der eigentliche E-Mail-Text mit seiner Betreffzeile – verschlüsselt wird, dann müssen sowohl die Betreffzeile als auch der E-Mail-Text vor dem Versand soweit pseudonymisiert werden, dass keine Bestimmung der betroffenen Person(en), um die es in dem E-Mail und seinem eventuellen Anhang geht, daraus erfolgen kann.

Der Absender muss durch seine Maßnahmen (Verschlüsselung und ggfl. Pseudonymisierung) gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung bis hin zum gewünschten Adressaten weder unbefugt gelesen, noch kopiert, verändert oder entfernt werden können.

2.4.1 Dateiverschlüsselungen

Verschlüsselung kann auf verschiedenen Wegen erfolgen. Hierfür werden beispielsweise sogenannte Packprogramme im ZIP- und RAR-Format angeboten, die neben der Komprimierung von Dateien auch deren Verschlüsselung ermöglichen. Bei der Nutzung solcher Packprogramme muss darauf geachtet werden, dass die zur Verfügung gestellte Verschlüsselungstechnik dem aktuellen technischen Standard entspricht: Zurzeit beträgt die Schlüssellänge mindestens 256 Bit-AES (= „Advanced Encryption Standard"). Ein im Internet frei erhältliches Datenkomprimierungsprogramm mit Verschlüsselung ist zum Beispiel „7zip", das unter http://www.7-zip.de kostenlos erhältlich ist.
Es soll aber nicht unerwähnt werden, dass es auch Berichte gibt, dass die Verschlüsselungen solcher komprimierter „Dateipakete" von daran interessierten Dritten bereits – unautorisiert! – entschlüsselt worden sein sollen. Hilfen zum Entschlüsseln solcher Dateipakete sollen sich auch im Internet finden lassen.
Weitere Möglichkeiten bietet die Nutzung serverbasierter Verschlüsselungsanbieter, wie zum Beispiel Cryptshare®. Diese Verschlüsselungs- und Versandhilfe wird über den sog. Web-Browser in einer gesicherten Verbindung erreicht. Es wird keine Installation von weiteren Programmen benötigt. Cryptshare® wird mittlerweile von einigen zahnärztlichen Körperschaften und ab sofort auch von der Zahnärztekammer Niedersachsen (ZKN) für ihre Mitglieder angeboten (s. nähere Infos dazu auf Seite 36 in diesem NZB). Mit Cryptshare® kann auch unter der Cryptshare®-Oberfläche ein Begleittext mit dann sogar personenbezogenen Infor-

mationen erfasst/eingetippt werden, der dann gemeinsam mit einer oder mehreren Dateien verschlüsselt übermittelt werden kann.

2.4.2 Komplette E-Mail-Verschlüsselung
Eine, im Übrigen auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als sicher anerkannte Möglichkeit, komplette E-Mails, also neben eventuellen Anhängen auch die Betreffzeile und den eigentlichen E-Mail-Text, verschlüsselt zu übermitteln, funktioniert über die sogenannte Ende-zu-Ende-Verschlüsselung.
Von offiziellen Stellen wie dem BSI wird dafür, insbesondere für kleinere Unternehmen, oft eine sogenannte GnuPG/PGP Verschlüsselung empfohlen.
Das dahinterstehende Verschlüsselungskonzept Pretty Good Privacy (PGP) erlebt seit den Enthüllungen um die Lauschangriffe US-amerikanischer Geheimdienste eine Wiederbelebung. Vertrauenswürdigkeit von Kommunikation wird hier nicht von übergeordneten Instanzen (z.B. mittels Zertifikaten) beglaubigt, die natürlich auch schon kompromittiert sein könnten, sondern von allen Teilnehmern untereinander.
Den nötigen Unterbau liefert seit Jahren das deutsche Open-Source-Projekt GnuPG mit der gleichnamigen Software. PGP beruht auf einer sogenannten Public-Key-Infrastruktur (PKI). Weil in dieser Infrastruktur sowohl jedermann zugängliche öffentliche (public) als auch geheime (private) Schlüssel eine Rolle spielen, heißt sie auch „asymmetrisches Kryptosystem". Jeder Teilnehmer besitzt in diesem System ein Schlüsselpaar aus einem geheimen und einem öffentlichen Schlüssel, die zusammengehören. Das klingt komplizierter als es ist, wenn denn die dafür notwendige Software einmal installiert ist. Und genau da liegt aber das Problem:
In vielen Zahnarztpraxen ist die Installation/Implementierung dieser Software (z.B. in bestehende E-Mailprogramme wie Microsofts Outlook oder Mozillas Thunderbird in Verbindung mit dem Verschlüsselungs-Add-on Enigmail) nicht problemlos realisierbar. Dies liegt teilweise an häufig anzutreffenden begrenzten eigenen IT-Kenntnissen oder einem individuell zu hohem finanziellen Aufwand bei Fremdbeauftragung.


Foto: Privat

Ass. jur. Sabrina Pfütze, Abteilung Aus- und Fortbildung der ZKN

2.4.3 Generell wichtig bei Verschlüsselungen
Bei allen Verschlüsselungsarten ist darauf zu achten, dass jede Verschlüsselung nur so gut ist, wie das Passwort, welches dafür eingesetzt/benutzt wird. Bei der Erstellung des Passwortes sollten deshalb folgende Grundsätze des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beachtet werden:

- das Passwort sollte keine logische Zeichenfolge enthalten (also beispielsweise keine Abfolge direkt benachbarter Zeichen auf der Tastatur oder Alphabet-Ausschnitte),
- das Passwort sollte zwischen acht und zwölf Zeichen als Mindestlänge haben,
- das Passwort sollte Groß- und Kleinbuchstaben enthalten,
- das Passwort sollte neben Buchstaben auch Ziffern enthalten,
- das Passwort sollte auch Sonderzeichen (&, $, §, #, etc.) enthalten und
- das Passwort sollte kein leicht zu erratender Alltagsbegriff sein (also beispielsweise keine Lebensmittel, Namen, Musiktitel, etc.).

Neue Passwortempfehlungen aus den USA empfehlen inzwischen längere Sätze mit Wörtern, die nicht im Wörterbuch stehen (z.B. aus dem Plattdeutschen, Schwäbischen oder Badischen).

Das derart zum Verschlüsseln genutzte Passwort sollte auf einem anderen Kommunikationsweg dem Empfänger zugänglich gemacht werden, also z.B. per Telefon, Brief oder SMS.

2.4.4 Messenger-Dienste
Nicht unerwähnt bleiben, aber ausdrücklich von einer Nutzung für den Zweck abgeraten werden soll die Möglichkeit, Dateien und Texte auch mit Messenger-Diensten, wie z.B. WhatsApp an Dritte übermitteln zu können.
Solche Messenger-Dienste sind in der Regel zur Übermittlung von Patientendaten aus datenschutzrechtlicher Sicht völlig ungeeignet.
Auf jeden Fall ist bei der Verwendung eines Messenger-Dienstes dieser bezüglich der Vorgaben der Europäischen Datenschutz-Grundverordnung hin zu überprüfen. ■

→ Bitte nicht vergessen:
Das Haftungsrisiko bei Datenverlust liegt beim Absender der E-Mail.

Ass. jur. Sabrina Pfütze, Sachbearbeitung ZKN