Merkblatt
Versand von Patientendaten

Hinweis: Die nachfolgenden Fragen und Antworten sind sorgfältig erstellt, jedoch nicht durch die Aufsichtsbehörden geprüft worden. Die Landeszahnärztekammer Baden-Württemberg kann daher keine Haftung für die Fragen und Antworten übernehmen. Der Fragenkatalog ersetzt keinesfalls eine Beratung durch einen Rechtsanwalt.

1. Welche Grundsätze sind beim Versand von Patientendaten (z. B. Befundberichte und Röntgenbilder) zu beachten

Neben den Vorgaben der EU-Datenschutz-Grundverordnung (Art. 32 EU-DSGVO) hat der Zahnarzt bei der Übermittlung von Patientendaten an Dritte auch die Schweigepflicht nach § 203 Strafgesetzbuch zu berücksichtigen.

Eine Übermittlung von Patientendaten an Dritte ist deshalb nur möglich, wenn:

1. der Patient eingewilligt hat,
   z. B.:
   - Befundbericht nach Überweisung an Kieferorthopäden oder MKG/Oralchirurg
   - Übersendung von Patientenunterlagen an weiterbehandelnden Arzt (Sonderfall Röntgenbilder, siehe hierzu Kapitel 10)

   oder

2. der Zahnarzt zur Übermittlung gesetzlich verpflichtet ist,
   z. B.:
   - KZV zum Zweck der Abrechnung (§ 295 SGB V)
   - KZV zum Zweck der Qualitäts- und Wirtschaftlichkeitsprüfung (§ 298 SGB V)
   - den Medizinischen Dienst der Krankenversicherung (§ 284 mit § 295 SGB V)
   - die gesetzlichen Unfallversicherung (§ 201 SGB VII)
   - die zahnärztliche Stelle (§ 17a RöV)

   oder

3. zur Wahrung berechtigter Interessen des Zahnarztes
   z. B.:
   - zivilrechtliche Geltendmachung von Honorarforderungen
   - Inanspruchnahme rechtlicher Beratung bei Schadenersatzforderungen

2. Wie kann der Versand von Patientendaten erfolgen?

Die nachfolgend aufgezeigten Wege gelten nicht nur für den Versand von Patientendaten an Dritte, sondern auch für den Versand an den betroffenen Patienten selbst. In diesem Zusammenhang weisen wir auch auf die vielfach in den Praxen praktizierte und völlig DSGVO konforme Möglichkeit hin, dem Patienten seine Überweisung samt Röntgenfoto (z.B. auf CD oder USB-Stick) persönlich in der Praxis mitzugeben.

Post
Dem Zahnarzt steht für den Versand von Patientendaten zunächst der Postweg zur Verfügung. Dabei sind die Unterlagen in einem geschlossenen Umschlag möglichst mit dem Vermerk „persönlich“ oder „vertraulich“ zu transportieren. In diesem Fall unterliegt der Inhalt dem Briefgeheimnis, dessen Verletzung nach § 202 Strafgesetzbuch strafbar ist.

Fax
Der Versand von Patientendaten mittels Fax wird von den Landesdatenschutzbehörden als kritisch gesehen. Insbesondere da es sich um sensible personenbezogene Daten handelt, wird davon generell abgeraten. Bemängelt werden u.a. mögliche fehlerhafte Anwahl an die falsche Adresse, unverschlüsselte Übertragung, abhörbar wie ein Telefongespräch, Zugriffsmöglichkeiten auf die Faxgeräte per Fernwartung, Rufumleitungen beim Empfänger, mögliche Einsichtnahme von Unbefugte beim Empfang des Faxes.

Wenn in Ausnahmefällen doch eine Faxübertragung geboten ist, so sollten Versender und Empfänger am Telefon den Sendezeitpunkt und das Empfangsgerät so abzustimmen, das das Fax direkt entgegengenommen werden kann und damit vor der Einsichtnahme Dritter geschützt ist. Diese Absprachen schützen auch vor Fehlleitungen beispielsweise aufgrund veralteter Anschlussnummern oder aktivierter Anrufum- bzw. Weiterleitungen (LDI NRW).

E-Mail

Beim Versenden eines personenbezogenen Dokumentes wird dieses Dokument verschlüsselt und dann als E-Mail Anhang versendet.

Der Zahnarzt muss über diese Verschlüsselung gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dabei ist auch zu beachten, dass der Betreff der E-Mail und der E-Mailtext selber nicht verschlüsselt werden und deshalb hierin keine Patientennamen auftauchen dürfen.

Die Verschlüsselung kann auf verschiedenen Wegen erfolgen. Hierfür werden beispielsweise Packprogramme im ZIP und RAR-Format angeboten. Bei der Nutzung solcher Packprogramme muss darauf geachtet werden, dass die Schlüssellänge mindestens 256 Bit-AES beträgt. Ein freies Datenkompressionsprogramm mit Verschlüsselung ist zum Beispiel 7zip, welches auf http://www.7-zip.de kostenlos erhältlich ist. Weitere Möglichkeiten bietet die Nutzung serverbasierter Verschlüsselungsanbieter, wie bspw. Cryptshare®, welches von der KZV BW für ihre Mitglieder angeboten wird.

Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) wird eine GNUPG/PGP Verschlüsselung (siehe https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Tools/Gpg4Win/gpg4win_node.html und auch Wikipedia „GNU Privacy Guard“) gerade für kleinere Unternehmen empfohlen. Hierbei handelt es sich um eine asymmetrische Verschlüsselung, bei der mit einem öffentlichen und einem privaten Schlüssel gearbeitet wird. Ein Passwort wird nicht geteilt und nicht übermittelt. Diese Art der Verschlüsselung ist nach derzeitigem Wissensstand als "sicher" anzusehen. Die vom BSI initiierte Software samt Anleitung (Kompendium) ist unter https://www.gpg4win.de für Windows und unter https://gpgtools.org für macOS jeweils in deutscher Sprache kostenlos verfügbar. Für Outlook, Thunderbird und Apple Mail Nutzer wird sogar ein PlugIn mitinstalliert, welches die Ver- und Entschlüsselung von E-Mails und deren Anhängen voll automatisiert und damit ohne Aufwand ermöglicht.

In der ärztlichen Praxis ist diese Art der Verschlüsselung empfehlenswert für den häufigen E-Mailverkehr mit immer denselben Partnern, also z. B. mit dem Zahntechniker oder Überweisern. Nach einmaligem gegenseitigem Austausch der öffentlichen Schlüssel läuft die Kommunikation wie früher auch, nur verschlüsselt und damit gesetzeskonform nach DSGVO.

Für die Kommunikation mit nicht regelmäßigen Teilnehmern, z. B. Patienten, ist diese Art der Verschlüsselung zum jetzigen Zeitpunkt eher unpraktikabel, da die wenigsten Privatpersonen eigene Schlüssel erzeugt haben geschweige denn mit dieser Verschlüsselung umgehen können. Für diesen Teilnehmerkreis ist es momentan sicher am einfachsten, eine per Cryptshare gesendete Nachricht zu öffnen, da hierzu außer einer bestehenden Internetverbindung keine Programm- oder Schlüsselinstallationen notwendig sind.
Bei allen Verschlüsselungsarten ist darauf zu achten, dass jede Verschlüsselung nur so gut ist, wie das Passwort, welches benutzt wird. Bei der Erstellung des Passwortes sollten deshalb folgende Grundsätze des Bundesamtes für Sicherheit in der Informationstechnik beachtet werden:

- das Passwort sollte keine logische Zeichenfolge enthalten (Abfolge direkt benachbarter Zeichen auf der Tastatur),
- 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 (bspw. Lebensmittel, Namen, Musiktitel, etc.).

Neue Passwortempfehlungen aus den USA empfehlen inzwischen längere Sätze mit Wörtern, die nicht im Wörterbuch stehen (z. B. Schwäbisch oder Badisch).

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

Messenger-Dienste

Die meisten Messenger-Dienste, wie z.B. WhatsApp sind zur Übermittlung von Patientendaten aus datenschutzrechtlicher Sicht ungeeignet. Grundsätzlich ist bei der Verwendung eines Messenger-Dienstes dieser bezüglich der Vorgaben der EU-DSGVO hin zu überprüfen.

Ihre
LZK-Geschäftsstelle