Robert A. W. Fuhrmann

Datenschutz und Datenverarbeitung nach Einführung des Patientenrechtegesetzes

Robert A. W. Fuhrmann
Univ.-Prof. Dr. Dr.
Universitätspoliklinik für Kieferorthopädie
Martin-Luther-Universität Halle-Wittenberg
Große Steinstraße 19
06108 Halle/Saale
E-Mail:
info@kiss-orthodontics.de

Die elektronische Datenverarbeitung für die Abrechnung, Karteikartenführung, Speicherung von Dokumenten, für Fotos und Röntgenbilder, Arztbriefe und E-Mail-Kommunikation mit Ärzten und Patienten ist mittlerweile der Normalfall in nahezu allen Arztpraxen.

Die schnell wachsende elektronische Kommunikation und Vernetzung von Praxis-PC, DVT- und EDV-Zentren erfordert kontinuierliche Schutzvorkehrungen und Sicherheitsprüfungen aus straf- und haftungsrechtlichen Gründen, um die Sicherheit der Patientendaten zu gewährleisten und betriebswirtschaftliche Kennziffern vor Dritten zu schützen.

Der Gesetzgeber hat mit dem neuen Patientenrechtegesetz (BGB § 630) erstmals die elektronische Dokumentation der ärztlichen Behandlung gesetzlich geregelt. Nach § 630f Absatz 1 kann der Arzt die Patientenakte elektronisch führen. Der Arzt ist dazu verpflichtet, die Manipulationsfreiheit der Akte sicherzustellen, sodass nachträgliche Änderungen automatisch kenntlich gemacht werden.

Die Bundesärztekammer und die Kassenärztliche Bundesvereinigung haben darauf reagiert und im Mai 2014 eine dritte Fassung der ‚*Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis*' vorgelegt. Diese Empfehlungen wurden im Heft 21. des Deutschen Ärzteblatts vom 23. Mai 2014 auf den Seiten 819–828 publiziert. Die inhaltsgleiche PDF-Datei steht unter dem Menüpunkt *Empfehlungen* auf der Homepage der Bundesärztekammer in Berlin zur Verfügung.

Die vollständige Übertragbarkeit dieser Hinweise auf Zahnarztpraxen ist anzunehmen.

Zeiteichung von Verwaltungssoftware

Bisher sind in der Kieferorthopädie nahezu keine Praxisverwaltungssysteme mit dieser gesetzlich geforderten Zeiteichung ausgestattet. Das Gesetz sieht keinerlei Übergangsregelung bzw. Bestandsschutz oder eine alternative Dokumentationslösung vor. Verwendet eine zahnärztliche Praxis eine nicht gesetzeskonforme Verwaltungssoftware, trägt allein der Zahnarzt das Risiko. Der Software-Hersteller haftet nicht für die mangelhafte Software, falls ein Kläger seine elektronische Dokumentation anzweifelt. Kieferorthopäden sind gut damit beraten ihrer Software-Firma nahezulegen, dass die Auflagen aus dem Patientenrechtegesetz kurzfristig einzuhalten sind. Der technische Aufwand für die geforderte Nachrüstung einer Zeiteichung in der Verwaltungssoftware der ärztlichen Dokumentation ist für die Hersteller erheblich.

Eine zeitnahe Verbesserung der IT-Sicherheit von zahnärztlicher Verwaltungssoftware ist wünschenswert, um den Wert der Dokumentation eines beklagten kieferorthopädischen Leistungsanbieters bei einer gerichtlichen Auseinandersetzung zu verbessern. Das Anzweifeln der ärztlichen Aufklärung und Dokumentation ist heutzutage eine zentrale Fragestellung bei den meisten Arzthaftungsprozessen.

Technische Sicherheit von elektronischer Praxisverwaltung

Ein tägliches Back-up auf externen Festplatten und die zusätzliche Verwendung nicht veränderbarer Speichermedien wie DVD- und CD-ROM erfordern

eine Integration in die abendliche Praxisroutine.

Ein weiteres Alltagsproblem ist die Aufnahme externer Dokumente und Befunde in die PC-gestützte Praxisverwaltung. Dabei ist umstritten, ob diese Originaldokumente nach dem Scannen vernichtet werden können oder im Original (also in Papierform) aufbewahrt werden müssen. Sicher ist, dass ein handschriftlich unterzeichneter Originalbrief vor Gericht einen deutlich höheren Beweiswert besitzt, als ein ausgedruckter Scan bzw. eine E-Mail des Arztes.

Praxen, die trotz dieser forensischen Unsicherheit ausschließlich digital archivieren und keine Originalbeiakte für jeden Patienten führen, sollten zumindest die Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik erfüllen.

Der Beweiswert eingescannter Originaldokumente steigt, wenn bei allen Einlesevorgängen beispielsweise das Vieraugenprinzip (Zeugen) eingehalten wird oder E-Mails mit einer qualifizierten elektronischen Signatur und Zeitstempeln versehen sind.

Die Nutzung fremder Speichermedien wie USB-Sticks oder fremder Festplatten kann zu einer unbeabsichtigten Einspielung von Schadsoftware auf dem Praxiscomputer führen. Bereits durch das Einstecken entsteht eine Infektionsgefahr.

Eine Integration von WLAN-Netzen ist nur bei besonderen Sicherheitsvorkehrungen sinnvoll. Die größtmögliche Sicherheit bieten klar definierte abgeschlossene Kabelnetzwerke.

Telekommunikation auf Basis von IP-Technologie (Voice over IP) wird mittlerweile als sichere Technik eingestuft. Letztlich muss der Arzt als Technikanwender sich auf die Vertraulichkeit der Kommunikationsanbieter verlassen.

Die Verwendung des populären ‚Skype'-Dienstes für die Übermittlung von Patienteninformation ist für eine sichere Kommunikation bedenklich, da Skype bei der Bundesnetzagentur nicht registriert ist.

Die zunehmende Empfehlung von Cloud-basierten medizinischen Diensten ist kritisch zu bewerten, da eine externe Sicherung von Patientendaten erfolgt. Die externe Datenspeicherung von medizinischen Informationen ist nur dann statthaft, wenn eine Verschlüsselungstechnik angewendet wird, sodass kein Mitarbeiter der IT-Firma oder ein sonstiger Fremdnutzer Zugriff auf diese Daten hat.

Angesichts der Fülle von technischen Risiken ist es empfehlenswert, mit seinen Hard- und Software-Kooperationspartnern bzw. Datendienstleistern schriftlich zu vereinbaren, dass die Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik bei der Praxisverwaltung eingehalten werden und ein unbefugter Zugriff auf die Patientendaten ausgeschlossen ist.

Schweigepflichtrisiken in medizinischen Verwaltungsnetzen

Die Einhaltung der ärztlichen Schweigepflicht und des gebotenen Datenschutzes wird mit zunehmender Anzahl der Mitarbeiter einer überörtlichen Gemeinschaftspraxis oder anderen Formen gemeinschaftlicher Organisation (Labor, DVT, Röntgen, usw.) mit digitalen Zugriffsrechten auf die Praxisverwaltung schwieriger, da die Anzahl der zugriffsberechtigten Personen wächst. Das Herausfinden von Passwörtern und die Aushebelung von installierten Schutzhindernissen ist mittlerweile eher ein Ansporn als ein verlässlicher Schutz für die betroffenen Ärzte.

Unternehmerische Risiken

So mancher Fernanschluss einer externen Abrechnungshilfe oder eines viel beschäftigten IT-Experten ist bedenklich und kann zur Sammlung von Praxisinformationen verwendet werden. Aufgrund der Vollständigkeit des Datenmaterials in einer Praxisverwaltung sind daraus Umsätze, Kosten und vertrauliche Informationen des Unternehmens externen Fachkräften zugänglich. Sicherlich kann ein regionaler Wettbewerber aus einer Weitergabe des Datenmaterials einen beträchtlichen Nutzen ziehen.

Mit zunehmender Mitarbeiterfluktuation ist das Thema Datensicherheit ein grundsätzliches unternehmerisches Risiko für jede Arztpraxis.

Schlussfolgerung

Das neue Patientenrechtegesetz § 630 BGB fordert im Absatz f eine neue Qualität in der Dokumentation sensibler Patientendaten mittels Informationstechnik. Die elektronische Routineausstattung zahnärzt-

licher Praxen bedarf einer beträchtlichen Nachrüstung, um die gesetzlich geforderte Zeiteichung zu ermöglichen.

Nachträgliche Änderungen in der Patientenkartei müssen automatisch zeitlich kenntlich gemacht werden. Diese Forderung ist ad hoc für alle ärztlichen Leistungsanbieter verbindlich.

Eine zeitlich geeichte Dokumentation bzw. digitale Karteikarte wird derzeit von den meisten Herstellerfirmen von zahnärztlicher Praxisverwaltungssoftware und Hardware nicht angeboten. Dadurch entsteht für die Zahnärzte ein forensisches Sicherheitsrisiko bei der Vorlage der digital geführten Karteikarte, der Aufklärungsbelege und Befunddokumente in Arzthaftungsprozessen. Die Beweislast für die regelrechte zeitnahe Dokumentation liegt auf den Schultern der Ärzte.