BEITRAGSREIHE ZUM THEMA DATENSCHUTZ IN DER ZAHNARZTPRAXIS

IT-Sicherheit für den Zahnarztpraxisalltag – Wie schütze ich meine Daten?

Seit einigen Wochen gilt die Datenschutzgrundverordnung (DSGVO) verbindlich in Deutschland. Der Schutz der personenbezogenen Daten (Ihrer Patienten und Mitarbeiter) steht dabei im Fokus der neuen gesetzlichen Regelungen. Die voranschreitende Digitalisierung des Praxisalltages beschleunigt viele Arbeitsprozesse im Rahmen der Erfüllung des Behandlungsvertrages bzw. der Praxisorganisation. Diese Effizienzsteigerung verlangt jedoch zugleich einen erhöhten Aufwand im Bereich der IT-Organisation. Die stetig wachsenden Risiken, die durch unzureichende IT-Sicherheit entstehen, dürfen keinesfalls unterschätzt werden. Praxisinhaber sollten deswegen bei den aktuell anstehenden Umstellungen auf die neuen Vorgaben der DSGVO neben dem Einsatz professioneller Hard- und Softwarelösungen auch Überlegungen zur Etablierung sinnvoller technischer/organisatorischer Maßnahmen (TOMs) anstellen, um ein datenschutzkonformes Sicherheitsniveau in der eigenen Zahnarztpraxis zu gewährleisten.

Foto: Privat

Dr. jur. Matthias Müller, Nürnberg

Maßnahmen zur Gewährleistung der IT-Sicherheit sind nicht erst seit dem Start der DSGVO am 25.05.2018 umzusetzen. Dennoch wird der Sicherung vorhandener EDV-Systeme und damit dem technischen Schutz der Patienten-Daten in vielen Zahnarztpraxen noch immer zu wenig Beachtung geschenkt. Dies nutzen Cyberkriminelle aus – wie in jüngster Vergangenheit auch in einigen Zahnarztpraxen in Niedersachsen – und verschaffen sich Zugang zu Praxissystemen, vertraulichen Patienten- und Abrechnungsdaten und verursachen erhebliche wirtschaftliche Schäden.

Wir beantworten deswegen im fünften Teil unserer Fachartikel-Serie zum Thema Datenschutz in der Zahnarztpraxis die Fragen zur IT-Sicherheit: Welche gesetzlichen Vorgaben sind bei der IT-Sicherheit zu beachten? Welche Schutzmaßnahmen sollten unbedingt umgesetzt werden? Welche sonstigen Risiken bestehen?

Gesetzliche Vorgaben zur IT-Sicherheit in der Zahnarztpraxis

In Punkto IT-Sicherheit verlangt der Europäische Gesetzgeber von jedem Praxisinhaber, gem. Art. 5 Abs. 1 f) DSGVO, dass eine „angemessene Sicherheit der personenbezogenen Daten gewährleistet wird". Die schließt neben dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung – durch ein rechtskonformes Datenschutzkonzept (vgl. Fachartikel zum Datenschutzkonzept in der April-Ausgabe des NZB) – auch die Verhinderung eines unbeabsichtigten Verlustes, Zerstörung oder Schädigung der Daten durch geeignete technische und organisatorische Maßnahmen ein. Verantwortliche haben ein, dem jeweiligen Risiko angepasstes Schutzniveau durch Umsetzung entsprechender TOMs zu gewährleisten, die sich an dem „Stand der Technik" zu orientieren haben, Art. 32 DSGVO. Dies bedeutet nicht, dass jede technische Neuerung, die der Markt hervorbringt, eingesetzt werden muss. Vielmehr sind IT-Systeme einzusetzen, die sich in der Praxis bewährt haben (Geeignetheit und Effektivität).

Absolute technische Sicherheit gibt es in der Praxis (leider) nicht. Neben einer regelmäßigen Aktualisierung der Software (Updates von Antivirus und Firewall Systemen) kann jedoch mit vergleichsweise unkomplizierten organisatorischen Maßnahmen bereits eine erhebliche Verbesserung des IT-Sicherheitsniveaus erreicht werden. Nach dem Grundsatz: „Risikovermeidung durch Zugriffsbeschränkung" sollten hierzu u.a. ausschließlich gesicherte WLAN-Netze verwendet, den Mitarbeitern die private Internetnutzung (Facebook & Co.) und der Einsatz ungeprüfter Speichermedien (USB-Sticks) am Arbeitsrechner untersagt werden. Zugriffe auf das IT-System sind – auch für beauftragte IT-Sachverständige (bspw. mit TeamViewer) – erst nach jeweils vorheriger Freigabe und Kontrolle am eingeloggten Computer zuzulassen.

Für den Fall eines physischen oder technischen Zwischenfalls fordert die DSGVO das Vorhalten eines „Notfallplanes",

Foto: © jd-photodesign/Fotolia.com

um eine „rasche Wiederherstellung" der Daten zu ermöglichen, gem. Art. 32 Abs. 1 c) DSGVO. Somit ist ein Back-up-System – das heute zum Standard einer jeden Praxis gehören sollte – nunmehr obligatorisch einzurichten. Die verschlüsselten Datensicherungen sollten dabei in möglichst kurzen Intervallen (täglich oder wöchentlich) auf externen Speichermedien unbedingt getrennt vom Hauptsystem (außerhalb der Praxis / im feuerfesten Tresor) aufbewahrt werden. Sollte Ihren gespeicherten Praxis-Daten doch einmal etwas passieren (bspw. Zerstörung durch Naturgewalt oder Unbrauchbarkeit durch Hackerviren) können Sie mit Hilfe der Datensicherung Ihr System neu aufsetzen, ohne Ihre Patientenversorgung zu gefährden, längere Ausfallzeit zu haben, Kostenabrechnung nicht mehr vornehmen oder Ihren steuerlichen Aufbewahrungspflichten nicht nachkommen zu können.

Soweit die notwendigen TOMs zur IT-Sicherheit implementiert sind, sind diese regelmäßig zu überprüfen, Art 32 Abs. 1 d) DSGVO. Diese sog. „Penetrationstests" können vom zuständigen IT-Unternehmen vorgenommen und sollten entsprechend dokumentiert/bescheinigt werden. Hierdurch können Schwachstellen aufgedeckt und zukünftig vermieden werden.

Risiken und Nebenwirkungen

Die durch die DSGVO vorgegebenen Anforderungen stellen sicherlich lediglich die Mindestanforderungen der IT-Sicherheit in der Zahnarztpraxis dar. Die möglichen Risiken sind jedoch nicht nur mögliche Eingriffe von außen (bspw. Schadsoftware oder Hackerzugriffe), sondern eben auch der Verlust oder die Beschädigung der gesammelten Daten durch physische Einflussnahmen (bspw. Feuer- oder Wasserschäden). Der zuständigen Aufsichtsbehörde ist die Erfüllung der gesetzlich geforderten (Mindest-)Maßnahmen im Zuge der Rechenschaftspflicht (vgl. Fachartikel der April-Ausgabe des NZB) auf Anfrage nachzuweisen. Bei einer Vernachlässigung gefährden Verantwortliche nicht nur den Verlust Ihrer wertvollen Praxis-Daten, sondern auch ein Bußgeld von (theoretisch) bis zu 20 Mio. Euro, Art. 83 Abs. 5 DSGVO.

i

Vertiefend vgl. Bundeszahnärztekammer und Kassenzahnärztliche Bundesvereinigung: „Rechtsgrundlagen und Hinweise für die Zahnarztpraxis – Datenschutz- und Datensicherheits-Leitfaden für die Zahnarztpraxis-EDV" https://www.bzaek.de/fileadmin/PDFs/za/datenschutzleitfaden.pdf

Fazit

Zahnärzte sollten – soweit nicht bereits erfolgt – die Anforderung an die IT-Systeme in der Praxis im Rahmen der Umstellung und Implementierung eines rechtskonformen Datenschutzkonzeptes auf die neuen Datenschutzvorgaben der DSGVO unbedingt umsetzen. Zudem sollten Sie eine regelmäßige Überprüfung der Aktualität Ihrer technischen und organisatorischen Vorkehrungen nicht alleine wegen datenschutzrechtlicher Sanktionen vornehmen, sondern bereits auf Grund der stetig wachsenden Risiken durch immer neu hinzukommende Gefahrenpotentiale aus der Cyberkriminalität.

Bei der individuellen Umsetzung der notwendigen Maßnahmen hilft Ihnen Ihr Datenschutzbeauftragter in Zusammenarbeit mit Ihrem zuständigen IT-Fachbetrieb. Die Auslegung der exakten gesetzlichen Verpflichtungen und die Umsetzung der technischen Möglichkeiten sind nicht immer ganz trivial und sollten in den meisten Fällen mit professioneller Unterstützung erfolgen.

Für einen effektiven Datenschutz hat nicht nur die Nutzung der Patientendaten ordnungsgemäß zu erfolgen, sondern es muss auch die Sicherheit der eingesetzten IT-Systeme gewährleistet werden. Dabei sollten Sie auch unbedingt darauf achten, Ihre Mitarbeiter zu sensibilisieren, auf bestimmte Sicherheitsregelungen vertraglich zu verpflichten und bezüglich aktueller Gefahrenpotentiale zu schulen. ■

Dr. jur. Matthias Müller, Nürnberg