Cybersicherheit ist eines der wichtigen Compliance-Themen. © *www.shutterstock.com*

Compliance in der Zahnarztpraxis

unter besonderer Beachtung der Digitalisierung

Compliance bedeutet die Einhaltung aller gesetzlichen Bestimmungen, was angesichts des streng regulierten Gesundheitsmarktes eine nicht ganz leicht zu nehmende Hürde eines jeden Praxisinhabers darstellt. Gemeint ist nämlich, dass sich jeder Praxisinhaber regelgetreu verhalten soll.

Neben den bereits bestehenden Vorschriften aus den unterschiedlichen Bereichen kommen stetig neue gesetzliche Anforderungen hinzu. Prominent zu erwähnen sei hier die Medical Device Regulation, die final im kommenden Mai 2021 in Kraft tritt und die Vorgaben unter anderem an das Qualitätsmanagement präzisiert.
Auf Grund der dynamischen Anforderungen sollte jede Zahnarztpraxis über ein Compliance-System verfügen. In unserem nachfolgenden Beitrag möchten wir diesem schwammigen Begriff mehr Kontur und Anhaltspunkte für die praktische Umsetzung geben!

Bestandsaufnahme der Ist-Situation und Entwicklung eines Zukunftskonzepts

Regelmäßig wird in einem ersten Schritt eine Bestandsaufnahme und eine Bestandsprüfung der rechtlichen Verhältnisse der Praxis nach außen durchzuführen sein. Darunter ist zu empfehlen, die bestehenden Praxisverträge einer entsprechenden Risikoprüfung zu unterziehen, insbesondere wenn seit deren Aufstellung schon einige Jahre vergangen sind und sich die gesetzlichen Regelungen verändert haben. Daneben sind Arbeitsverträge, gerade bei Neuanstellungen, von Zeit zu Zeit an die aktuellen Vorschriften auf Aktualität und Richtigkeit anzupassen. Ebenso lohnt sich häufig, die eigene Website auf den geltenden Rechts- und Technikstand zu bringen, um Abmahnungen zu vermeiden. Besonderes Augenmerk liegt hier beim Impressum, werblichen Inhalten sowie der Datenschutzerklärung.
Nützlicher Nebeneffekt ist, dass der sorgfältige Außenauftritt auch bei Patienten den Eindruck hinterlässt, dass der Praxisinhaber die gesetzlichen Vorschriften kennt und die Praxis insgesamt modern und aufgeräumt erscheint. Dieser Eindruck spiegelt sich ebenso in etwaigen Praxisverkäufen oder bei der Aufnahme eines weiteren Praxispartners wider, denn es können regelmäßige höhere Summen für Ein- bzw. Austritt verlangt werden, da die Praxis insgesamt modern ist und der Käufer Rechtsberatungskosten für die Aktualisierung der Unterlagen spart.
In einem weiteren Schritt ist für die Praxis ein tragfähiges Compliance-Konzept zu entwickeln, mit dem sichergestellt wird, wie zukünftig die Einhaltung aller gesetzlichen Bestimmungen konkret gewährleistet werden soll, beispielsweise durch interne Audits, das Zwei-Augen-Prinzip oder festgelegte Betriebsabläufe.

Cybersicherheit als Compliance-Thema

Neben der Anpassung der Betriebsabläufe und dem internen Prozessmanagement ist ein weiteres Augenmerk auf die Sicherheit der technischen Praxisabläufe zu werfen, da die Cybersicherheit nicht erst im Jahr 2020 mehr und mehr in den Fokus rückt.

Doch muss das sein? Ja! Auch wenn im privaten Bereich immer noch allzu häufig auf WhatsApp zugegriffen wird, obwohl vermehrt Kritik an der Datensicherheit der App laut wird. Insbesondere bei der gemischten Nutzung des Handys zu beruflichen und persönlichen Zwecken sollte auf die App verzichtet werden, da WhatsApp auf die im Smartphone gespeicherten Telefonkontakte Zugriff erhält. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit sowie die Rechtsprechung (darunter beispielsweise das Amtsgericht Bad Hersfeld mit Beschluss vom 20.03.2017, Az.: F 111/17 EASO) haben den Gebrauch von WhatsApp im beruflichen Kontext als Datenschutzverstoß gewertet.

Bei der Nutzung von Gesundheitsdaten muss eine noch stärkere Sensibilisierung, auch gegenüber Mitarbeitern, erfolgen, da diese Daten noch mehr geschützt werden müssten. Gleichwohl kommt es vermehrt zum Datenmissbrauch und Datendiebstahl, allein weil eine unzureichende Datensicherung stattfindet. So hat eine Untersuchung des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) hervorgebracht, dass neun von zehn Ärzten leicht zu erratende Passwörter für ihr Praxisnetzwerk verwenden, beispielsweise „Praxis", „Behandlung" oder gar ihren Namen. Zudem haben in 22 von 25 getesteten Arztpraxen mehrere Benutzer dieselbe Zugangskennung mit einfacher oder sogar gar keinem Passwort benutzt. Dies ist erschreckend und zeigt den unsachgemäßen Umgang mit personenbezogenen Daten.

Wie können also Risikofaktoren verringert werden?

Neben den dargelegten Risikofaktoren, die für fast jede Praxis allgemeingültig sind, helfen die nachfolgenden Aspekte als sog. Risiko-Minimierer, die mit einigem organisatorischen sowie finanziellem Aufwand beseitigt werden können:

- Erstellung eines Notfallplans
- Regelmäßige und professionelle Updates der Praxis-IT
- Regelmäßige und professionelle Datensicherungen des Praxisnetzwerks
- Schulung von Mitarbeitern zu Datensicherheit und Datenverarbeitung; doch Vorsicht: Sie bleiben als Arbeitgeber stets Letztverantwortlicher und können das Risiko nicht auf Ihre Mitarbeiter abwälzen
- Komplexe Passwörter, ohne Fantasienamen oder 1234-Kombinationen.

Nicht erst seit der Einführung der DSGVO ist Datenschutz und Cybersicherheit ein aktuelles Thema. Viele Praxisinhaber scheuen sich das Thema IT-Sicherheit aktiv anzugehen, da es nicht in ihrem Fachbereich liegt und vermeintlich mühsam ist anzugehen und umzusetzen. Doch allein auf Grund der empfindlichen Bußgeldkataloge sollte jeder Praxisinhaber ein ausreichendes technisches Sicherheitskonzept haben, um Vergehen oder Abmahnungen ausreichend vorzubeugen. Neben den Bußgeldern selbst treten daneben häufig erforderliche Anwaltskosten sowie bei einem Hackerangriff Kosten für eine Datenrettung. Dies kostet Geld, Zeit und Nerven und je nach Umfang des Datenverlustes droht ein Imageschaden, weil man Patienten darüber informieren muss, dass ihre Daten aus Ihrem Netzwerk gestohlen worden sind. Patienten verlieren das Vertrauen in den sorgfältigen Umgang ihrer Daten und damit in die Praxis insgesamt.

Was kann daher für die Praxis empfohlen werden?

Sich dem Thema mit professioneller Unterstützung annehmen! Nach Angabe der GDV müssten acht von zehn Arztpraxen in Deutschland – und damit 78 % – nach eigener Ansicht ihre Arbeit bei einem erfolgreichen Cyber-Angriff einstellen oder stark einschränken.
Praxisinhaber sollten ihre Augen daher nicht verschließen und ihr Compliance-System um digitale Punkte erweitern oder ein solches System einführen. Daneben empfiehlt es sich neue Arbeitsverträge regelmäßig überprüfen zu lassen, da die arbeitsrechtliche Rechtsprechung besonders häufig Änderungen unterliegt und somit Risiken präventiv verringert werden können.

Auch wenn der Angang an neue Themen stets unangenehm ist: er wird belohnt mit einem langfristigen Erfolg Ihrer Praxis! ■

Leonie Unkelbach

Rechtsanwältin Leonie Therese Unkelbach war vor Eintritt in die Kanzlei in einer deutschen Großbank tätig und hat den Bereich M&A und Finanzierung beraten. Sie ist seit Anfang des Jahres im Team der Kanzlei Lyck+Pätzold healthcare.recht und dort spezialisiert auf das Gesellschaftsrecht für Zahnarztpraxen und Krankenhäuser sowie das Medizinprodukterecht. Sie berät Leistungserbringer und Unternehmen aus dem Gesundheitsmarkt umfassend in medizinrechtlichen Fragestellungen.

Leonie Unkelbach
Lyck+Pätzold. healthcare.recht
Nehringstr. 2
61352 Bad Homburg
Tel. 06172 1399-60
unkelbach@medizinanwaelte.de