Unter dem Begriff Compliance ist die Einhaltung gesetzlicher Bestimmungen zu verstehen. Es geht also um die sogenannte Regeltreue eines jeden Praxisinhabers, was angesichts des hochregulierten Gesundheitsmarktes eine große Bürde darstellt. Der vorliegende Beitrag umreißt die Kernpunkte zum Thema Compliance.

Christian Erbacher
[Infos zum Autor]

Compliance im Zeitalter der Digitalisierung

Christian Erbacher, LL.M.

In Zeiten sich ständig wandelnder und vor allem wachsender gesetzlicher Anforderungen sollte jede Zahnarztpraxis über ein Compliance-System verfügen. Doch was ist das eigentlich genau?

Beurteilung/Prüfung der Istsituation und Zukunftskonzept

In einem ersten Schritt sind zunächst einmal eine Bestandsaufnahme und eine Bestandsprüfung durchzuführen. So sind zum Beispiel die aktuellen Praxisverträge – insbesondere dann, wenn der Vertragsabschluss schon einige Zeit (oder Jahre) zurückliegt, als noch andere gesetzliche Regelungen galten – einer Risikoprüfung zu unterziehen oder die Webseite und der Außenauftritt an sich auf Aktualität und Richtigkeit zu prüfen.

Wichtig dabei ist, diese Beurteilung nicht stetig aufzuschieben. Denn oftmals werden diese Themen unter Zeitdruck und nicht mit der notwendigen Sorgfalt aufgearbeitet; dies zum Beispiel bei einem anstehenden Praxisverkauf, einer Aufnahme eines Praxispartners, einem Umzug etc., was dazu führt, dass unter Umständen ungünstige Kompromisse einzugehen sind.

In einem zweiten Schritt ist ein tragfähiges Konzept auszuarbeiten, mit dem sichergestellt wird, wie und auf welche Art und Weise die Einhaltung gesetzlicher Bestimmungen für die Zukunft konkret gewährleistet wird.

Cybersicherheit ein Compliance-Thema

Diese Sorgfältigkeitsprüfung ist im digitalen Zeitalter durch einige Punkte – wie zum Beispiel die Cybersicherheit – zu ergänzen.
Muss das sein? Schließlich legt der massenhafte Gebrauch von WhatsApp im beruflichen Bereich nahe, dass sich viele Menschen eigentlich gar nicht so richtig dafür interessieren, was mit ihren Daten geschieht. Die Tatsache, dass WhatsApp Zugriff auf die auf dem Smartphone gespeicherten Telefonkontakte erhält, wird augenscheinlich hingenommen. Gleiches gilt für die Ansichten des Hessischen Beauftragten für Datenschutz und Informationsfreiheit oder der Rechtsprechung (z.B. Amtsgericht Bad Hersfeld, Beschluss vom 20.3.2017, Az.: F 111/17 EASO), nach denen der Gebrauch von WhatsApp im beruflichen Bereich einen Datenschutzverstoß darstellt. So weit so gut (oder auch nicht).
Bei Gesundheitsdaten sollte eine hohe Sensibilisierung vorliegen. Denn diese stellen längst ein teures Wirtschaftsgut dar, für deren Sammeln viele Unternehmen Ausgaben in Millionenhöhe zu verzeichnen haben. Diese Daten müssten deshalb eigentlich besonders geschützt sein. Müssten. Eigentlich.
Wie kommt es dann, dass in 22 von 25 getesteten Arztpraxen mehrere Benutzer dieselbe Zugangskennung mit einfacher oder sogar gar keinem Passwort benutzen? Dies zeigt eine aktuelle Untersuchung des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV). Die Analyse kommt zu dem Ergebnis, dass neun von zehn Ärzten leicht zu erratende Passwörter wie „Behandlung", „Praxis" oder den Namen des Arztes verwenden. Zudem finden sich von jeder zehnten Arztpraxis und sogar von 60 Prozent der Kliniken E-Mail- und Passwortkombinationen im sogenannten Darknet.

Risikofaktoren verringern

Fünf große Risikofaktoren in Praxen – die mit einem geringen organisatorischen und finanziellen Aufwand beseitigt bzw. minimiert werden können – sind:

- fehlende oder einfache Passwörter und Zugänge
- arglose Mitarbeiter
- fehlende oder unregelmäßige Datensicherungen
- fehlende oder unregelmäßige Sicherheits-Updates
- kein Notfallplan

Es kommt neben rechtlichen Gesichtspunkten also auch auf technische Details an. Die Vorhaltung von zum Beispiel regelmäßigen Datensicherungen oder Sicherheits-Updates ist per se nicht kompliziert; doch es muss eben daran gedacht werden.
Insofern ist Cybersicherheit definitiv ein Thema, mit dem sich jeder Unternehmer bzw. Praxisinhaber bereits aus Eigeninteresse beschäftigen sollte. Einerseits sehen rechtliche Normen, wie zum Beispiel die DSGVO, empfindliche Bußgelder vor (daneben drohen Anwaltskosten). Andererseits ist der Imageschaden bei einem erfolgreichen Angriff enorm, denn die Patienten verlieren das Vertrauen.

Bei Gesundheitsdaten sollte eine hohe Sensibilisierung vorliegen. Denn diese stellen längst ein teures Wirtschaftsgut dar, für deren Sammeln viele Unternehmen Ausgaben in Millionenhöhe zu verzeichnen haben. Diese Daten müssten deshalb eigentlich besonders geschützt sein.
Müssten. Eigentlich.

Praxisempfehlung

Da nach Angabe der GDV acht von zehn Arztpraxen in Deutschland – und damit 78 Prozent – nach eigener Ansicht ihre Arbeit bei einem erfolgreichen Cyberangriff einstellen oder stark einschränken müssten, sollten erfolgreiche Unternehmer/Praxisinhaber die Augen hiervor nicht verschließen und ihr Compliance-System um digitale Punkte ergänzen, neugestalten oder einführen.
Weiterhin werden im Rahmen eines Compliance-Systems wie dargelegt der Istzustand überprüft und bestehende Praxisverträge (Mietvertrag, Gesellschaftsvertrag, Arbeitsverträge etc.) ebenfalls einer Risikoüberprüfung unterzogen, sodass Risiken präventiv ausgeschaltet oder zumindest verringert werden können. Auch dies sichert den langfristigen Erfolg der Praxis.
Daneben sollte sich jeder Praxisinhaber auch selbst fragen, wie er zu dem Schutz der Gesundheitsdaten beitragen kann. Denn der tatsächliche Wert von Gesundheitsdaten ist für die meisten Menschen kaum greifbar; definitiv ist es bzw. wird es allerdings so sein, dass derjenige, der über die meisten Daten verfügt, auch gleichzeitig die größte Macht besitzt bzw. besitzen wird. Deshalb dürfen Gesundheitsdaten auch nur für denjenigen einsehbar sein, für den sie auch bestimmt sind.

Lyck+Pätzold. healthcare.recht
[Infos zum Unternehmen]

Kontakt

Christian Erbacher, LL.M.
Rechtsanwalt

Lyck+Pätzold. healthcare.recht
Nehringstraße 2
61352 Bad Homburg
Tel.: 06172 139960
www.medizinanwaelte.de