Checkliste: Datenschutz im Gesundheitsbereich

GUARDIUM®
DATENSCHUTZ

Gerade in Arztpraxen herrscht ein hoher Publikumsverkehr und der Schutz personenbezogener Daten braucht hier erhöhte Aufmerksamkeit, zumal Patientendaten (die auch Gesundheitsdaten (Art. 9 DSGVO) enthalten) einer besonders schützenswerten Art personenbezogener Daten angehören. Die folgende Checkliste für korrekten Datenschutz in der Arztpraxis soll das Augenmerk auf potenzielle Sicherheitslücken lenken.

Rezeption & Eingangsbereich

- » Gibt es eine Zugangskontrolle? ☐
- » Kann jeder ungesehen die Praxis betreten? ☐
- » Ist der Empfang durchgehend besetzt (Stichwort: Raucher- oder Toilettenpausen)? ☐
- » Gibt es einen Diskretionsbereich oder stehen Wartende dicht beieinander? ☐
- » Sind die Bildschirme an der Rezeption blickgeschützt? ☐
- » Ist der Terminplan vor unbefugten Einblicken geschützt? ☐
- » Sind die (Akten- und Dokumenten-) Schränke vor unbefugten Zugriffen geschützt (abschließbar)? ☐

Bei Patientenkontakt:

- » Bekommen (neue) Patienten eine Vorlage für die Verarbeitung personenbezogener Daten zum Gegenzeichnen? ☐
- » Gehen die Betroffeneninformation (ausreichend) auf die speziellen Patientenbezogenen Datenverarbeitungen ein (Rechtsgrundlagen, etc.)? ☐

STICHWORT: VIDEOÜBERWACHUNG

Vermehrt wird in Praxen der Eingangs-, Empfangs- oder Wartebereich videoüberwacht. Dies ist jedoch problematisch, da es sich hier nicht um öffentlich zugängliche Räume (im Sinne des Gesetzes) handelt und eine Videoüberwachung daher nicht gerechtfertigt werden kann. Vor allem aus folgenden Gründen ist eine Videoüberwachung hier nicht zulässig:
Die Videoüberwachung ist regelmäßig nicht erforderlich und nicht verhältnismäßig.
Für die Videoüberwachung ist kein ausreichender Zweck gegeben.
Gleiches gilt für die Videoüberwachung von Mitarbeitern.

Patienten- und Betroffenenrechte (Art. 13 DSGVO)

- » Können Betroffene ihr Betroffenenrecht geltend machen? ☐
- » Werden die Aufbewahrungs- und Löschfristen der erhobenen Gesundheitsdaten eingehalten? ☐
- » Werden Patienten über ggf. mit- und nachbehandelnde Ärzte informiert und wird deren Einverständnis eingeholt? ☐
- » Werden Angehörige von Patienten / Betroffenen nur informiert, wenn sich diese im Vorfeld schriftlich dazu einverstanden erklärt haben? ☐
- » Hängt / liegt eine gut sicht- und lesbare Betroffeneninformation (nach Art.13 DSGVO) aus (auch für Rollstuhlfahrer) ☐
- » Werden (Gesundheits-)Daten der Betroffenen / Patienten nur mit datenschutzkonformer Rechtsgrundlage (v.a. Einwilligung) an Andere (Dienstleister, Abrechnungsstellen etc.) weitergegeben? ☐

STICHWORT: BYOD – BRING YOUR OWN DEVICE

In einigen Arztpraxen / Pflegebetrieben u. a. ist es mittlerweile üblich, dass Mitarbeiter Ihre privaten Geräte (wie Tablets oder Smartphones) für alltägliche Betriebsaufgaben benutzen. Das ist jedoch gerade im Gesundheitsbereich äußerst kritisch und datenschutzrechtlich nicht ohne Weiteres zulässig. Kommen Sie in diesem Fall zur Erörterung der Datenschutzkonformität gerne auf uns zu.

Ggf. Wartezimmer

- » Ist das Wartezimmer so abgetrennt, dass Gespräche im Rezeptionsbereich / Behandlungszimmern nicht mitgehört werden können? ☐
- » Hängt eine gut sicht- und lesbare Betroffeneninformation (nach Art. 13 DSGVO) aus? ☐
- » Befinden sich Wartestühle vor Behandlungszimmern, von denen aus Gespräche in Behandlungszimmern zu hören sind? ☐

Ggf. Behandlungsbereich

- » Können Fenster und Türen der Behandlungsräume so verschlossen werden, dass vertrauliche Gespräche unbefugten Dritten vorenthalten bleiben? ☐
- » Sind sensible Unterlagen (Patientenakten, Röntgenbilder usw.) vor unbefugten Zugriffen in Behandlungsräumen geschützt, sollte der Patient allein im Behandlungszimmer warten? ☐
- » Sind Patientenunterlagen in Behandlungsräumen generell geschützt, auch vor z.B. raschen Blicken vorbeigehender Patienten? ☐
- » Haben Patienten im Behandlungsbereich Zugang zu ungesicherten Rechnern? ☐

STICHWORT: ANGEHÖRIGENAUSKUNFT

Dieser Prozess kann sich teilweise sehr schwierig gestalten. Sollten Angehörige Auskunft verlangen, aber dies über Fernkommunikationsmittel, kann deren Identität meist nichts zweifelfrei bestätigt werden. In solchen Fällen ist es z.B. sinnvoll, vorher mit dem Patienten ein Codewort auszumachen, das von den Angehörigen genannt werden muss, um Auskunft zu bekommen. Sollte ungerechtfertigter Weise Auskunft erteilt werden, ist dies eine Datenschutzverletzung!

Verwaltung

- » Sind alle Mitarbeiter über ihre Wahrung der Schweigepflicht informiert? ☐
- » Werden alte Patientenakten sicher aufbewahrt? ☐
- » Hat das Reinigungspersonal Zugang zu sensiblen, personenbezogenen Daten? ☐
- » Entspricht der Aktenvernichter (Schredder) der DIN 66399-1/2 der Partikelgröße P-5 (ehem. Sicherheitsstufe 4)? ☐
- » Sind Drucker und Faxgeräte sowie Postablagen vor unberechtigten Zugriffen sicher? ☐
- » Werden Mitarbeiter regelmäßig im Datenschutz geschult? ☐
- » Liegt ein Konzept für den Notfall einer Datenschutzverletzung vor? ☐

STICHWORT: DATENSCHUTZVERLETZUNG

Schon eine mit eingefügten Gesundheitsdaten verschickte E-Mail, die ausversehen an den falschen Empfänger geschickt wird, stellt eine Datenschutzverletzung dar. Mitarbeiter müssen daraufhin sensibilisiert werden, solche Vorfälle nicht auf die leichte Schulter zu nehmen, denn gerade bei Datenschutzverstößen, die Patienten- und Gesundheitsdaten betreffen, können schnell hohe Bußgelder fällig werden.

Informationstechnik

- Wird für die Verarbeitung von Patientendaten, Lohnabrechnungen usw. ausschließlich autorisierte (nicht private) Hardware verwendet? ☐
- Ist die verwendete Hardware ausreichend durch Virenscanner, Firewalls und KV-Safenets geschützt? ☐
- Gibt es zur Hardware personalisierte Passwörter und Zugänge? ☐
- Werden Änderungen in den Patientenakten nachvollziehbar protokolliert? ☐
- Werden regelmäßig Sicherheitskopien gemacht? ☐
- Werden die Sicherheitskopien sicher vor Diebstahl, Wasser- und Feuerschäden etc. gelagert? ☐
- Werden für die Verarbeitung von Patientendaten ausschließlich autorisierte Programme verwendet, die in einem Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) erfasst sind? ☐
- Werden elektronische Patientendaten, soweit möglich, verschlüsselt gespeichert? ☐
- Ist eine ausreichende Löschpolitik in der Praxis etabliert, sollte ein Betroffener auf sein Recht auf Löschung Gebrauch machen (Art. 17 DSGVO)? ☐
- Ist das verwendete WLAN ausreichend verschlüsselt? ☐
- Werden alte Datenträger nach Datenschutzstandards entsorgt? ☐

STICHWORT: EINGABEKONTROLLE

In vielen Praxen ist es üblich, bei Gesundheitssystemen einen gemeinschaftlichen Zugang zu den Programmen zu benutzen. Im Zuge der technischen und organisatorischen Maßnahmen (TOM), die laut DSGVO eingehalten werden müssen, ist dies aber nicht zulässig, da die Änderungs- oder Löschhistorie in Akten nicht nachvollziehbar ist.

STICHWORT: SERVERTEILUNG

In Ärztehäusern oder Praxisgemeinschaften ist es nicht selten, dass sich verschiedene Praxen einen Server teilen. Doch Vorsicht: Das ist nicht nur ein ernstes Sicherheitsrisiko, sondern stellt auch eine ernstzunehmende Datenschutzverletzung dar, die bei einer eventuellen Kontrolle durch Behörden mit einem hohen Bußgeld belegt würde.