Fragen und Antworten rund um das Thema Datenschutz im Gesundheitswesen

Die Einhaltung der datenschutzrechtlichen Regelungen stellen viele Teilnehmer des Gesundheitswesens, wie z.B. Arztpraxen und Krankenhäuser vor große Herausforderungen.

Erst in diesem Monat berichtete der Bayerischen Rundfunk, dass mehr als 13.000 Datensätze von Patienten in Deutschland ungeschützt im Internet zu finden gewesen sein sollen. Rund die Hälfte dieser Daten enthalten demnach hochauflösende Bilder, die mit zahlreichen personenbezogenen Informationen versehen sind. Wenn das stimmt, werden offenbar grundsätzliche Datenschutzvorgaben zu oft ignoriert.

Dabei sollte der Datenschutz gerade von Krankenhäusern und Arztpraxen sehr ernst genommen werden. Denn der Datenschutz ist nicht nur im Bundesdatenschutzgesetz geregelt, sondern auch in anderen Gesetzen, wie z.B. dem Strafgesetzbuch. Damit die für den Datenschutz verantwortlichen Personen überhaupt wissen, welche Regelungen zu beachten sind, ist es zu empfehlen, sich zunächst einen groben Überblick über die rechtlichen Rahmenbedingungen zu verschaffen.

Gesetzliche Grundlagen

Zu nennen sind neben der auf europäischer Ebene geltenden DS-GVO, das die DS-GVO ergänzenden und konkretisierende nationale Bundesdatenschutzgesetz (BDSG), das Sozialgesetzbuch 10 (SGB X), das IT-Sicherheitsgesetz oder auch das Strafgesetzbuch (StGB). Auf Landesebene sind daneben noch die jeweiligen Landesdatenschutzgesetze zu beachten; gleiches gilt für die Landeskrankenhausgesetze, in denen ebenfalls datenschutzrechtliche Vorgaben zu finden sind. Als weitere speziellere Gesetze können schließlich das Telemediengesetz (TMG) oder das Telekommunikationsgesetz (TKG) genannt werden. Der Datenschutz findet sich, so viel kann festgehalten werden. in einer Vielzahl von Normen wieder, die hier nicht abschließend beschrieben werden können.

Zu beachten ist weiter, dass die datenschutzrechtlichen Regelungen einem steten Wandel unterzogen sind. Als Beispiele können das 2. DSAnpUG-EU (Datenschutz-Anpassungs-und Umsetzungsgesetz EU) oder das DSUmsAnpG-EU (Datenschutz-Umsetzungs- und Anpassungsgesetz EU) dienen, die am 27. Juni 2019 vom Bundestag in der Fassung der Ausschussempfehlungen verabschiedet worden sind.

Eine wesentliche Änderung ist hier in der Neufassung von § 38 BDSG zu sehen, nach der die maßgebliche Personenzahl, ab der ein betrieblicher Datenschutzbeauftragter zu benennen ist, von 10 auf 20 angehoben wird. Die Begründung der Ausschussempfehlung des Bundestagsausschusses für Inneres und Heimat lautete dahingehend, dass mit dieser Herabsetzung „vor allem eine Entlastung kleiner und mittlerer Unternehmen sowie ehrenamtlich tätiger Vereine“ angestrebt werde.

Und was gilt in Krankenhäusern?

Die datenschutzrechtlichen Regelungen werden von der Aufnahme bis zur Entlassung relevant. Welche Daten dürfen bei der Aufnahme erhoben werden? Dürfen bei der Aufnahme Daten der Vorbehandlung abgefragt werden? Welche Mitarbeiter dürfen wie und wann Zugang zu den besonders schützenswerten Gesundheitsdaten haben? Es stellen sich unzählige Einzelfragen.

Im Grundsatz gilt, dass bei der Aufnahme alle Daten abgefragt werden dürfen, die zur Erfüllung der Behandlungspflicht erforderlich sind; klassischerweise geht es hier um den Namen, die Adresse und das Geburtsdatum. Im Gegensatz hierzu sind Daten über Voraufenthalte erst einmal nicht relevant, soweit diese nicht zur Behandlung benötigt werden. Es gilt mithin all-

Rechtsanwalt Christian Erbacher

gemein der Grundsatz der Datensparsamkeit Bei der Verwahrung der Krankenakte wird das Thema der Cybersicherheit relevant. Bereits das Anlegen von sicheren, passwortgeschützten Benutzerprofilen im KIS kann viele Datenschutzverstöße verhindern. Im Grundsatz gilt hier, dass Unbefugte keine Einsicht in die Krankenakte haben dürfen. Die mit der Behandlung betrauten Personen dürfen also, soweit es zur Behandlung notwendig ist, Einsicht in die Dokumentation nehmen. Verwaltungsmitarbeiter nur insoweit, wie es zur ordnungsgemäßen Organisation erforderlich ist.

Problematisch und beunruhigend hieran ist, dass sich nach einer aktuellen Untersuchung des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) eine von jeder zehnten Arztpraxis und sogar von 60 Prozent der Kliniken E-Mail- und Passwort-Kombinationen im sog. Darknet wiederfinden.

Schließlich ist eine Weitergabe der Daten an Dritte, wie z.B. die Mitteilung der Zimmernummer durch den Pförtner an Besucher oder die Weitergabe der Daten zu externen Forschungszwecken nur mit vorheriger ausdrücklicher, schriftlicher Einwilligung zu lässig. Auch bei der Weitergabe zu internen Forschungszwecken innerhalb des Krankenhauses ist es zu empfehlen, eine ausdrückliche, schriftliche Einwilligung einzuholen, wenngleich eine solche interne Weitergabe datenschutzrechtlich wohl noch legitimierbar wäre.

Resumée

Der tatsächliche Wert von Gesundheitsdaten ist kaum greifbar, geschweige denn zu beziffern. Erst kürzlich investierte die PKV 100 Millionen Euro in Gesundheitsstartups und technischen Anwendungen. Um die Gesundheitsdaten hinreichend zu schützen, spricht alles dafür, dass Gesundheitsdaten nur für diejenigen einsehbar sein dürfen, für die sie auch bestimmt sind. Dafür ist die Einhaltung der datenschutzrechtlichen Regelungen unerlässlich. Daher sollte der Datenschutz einen festen Platz im Compliance-Konzept eines Krankenhauses haben. Wer ohne diesbezügliche Comliance handelt, handelt grob fahrlässig in Bezug auf Patientendaten aber auch in Bezug auf die ganz persönliche Haftung. www.medizinanwaelte.de

Rechtsanwalt Jens Pätzold