Wie sicher sind meine Gesundheitsdaten?

Gesundheitsdaten sind besonders sensible Informationen. Grundsätzlich dürfen nur Daten erhoben werden, die für die Behandlung erforderlich sind. Daneben dürfen personen- oder einrichtungsbezogene Daten der Versicherten oder der Leistungserbringer zur Qualitätssicherung im gesetzlich begrenzten Rahmen genutzt werden.

Mit zunehmender Digitalisierung entstehen für alle Beteiligten, allen voran für die Patientinnen und Patienten neue Herausforderungen. Seit Mai 2018 gilt die Europäische Datenschutz-Grundverordnung (DS-GVO) auch in Deutschland. Ihr Ziel ist es, die Rechte der von der Datenverarbeitung betroffenen Personen zu stärken. Bei Datenschutzverstößen drohen empfindliche Strafen.

Die Europäische Datenschutz-Grundverordnung hat Bewegung in eine längst fällige Debatte gebracht, meint Mark Peters. Mit seinem Unternehmen, Praxismanagement Bublitz/Peters GmbH & Co. KG, berät er Ärzte, Krankenhäuser und Pflegeeinrichtungen in Sachen Datenschutz. Er kennt die praktischen Probleme, die sich in der täglichen Arbeit mit Patientendaten ergeben. Die erste Schwachstelle ist meist schon die Anmeldung in der Arztpraxis. Andere Patienten hören zu. Der Bildschirm mit Patientendaten ist einsehbar.
Mark Peters benutzt am liebsten das Wort von der Informationssicherheit. Da stecken sowohl der Datenschutz, als auch die IT-Sicherheit drin. In seinem Alltag geht es um technische und organisatorische Maßnahmen, wie dies zu gewährleisten ist.

Datenschutz in Europa ist nichts Neues

Die Europäische Datenschutz-Grundverordnung ist übrigens nichts völlig Neues. Bereits 1995 wurde vom Europäischen Parlament und dem Rat die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ beschlossen. Im Recht der Mitgliedsstaaten wurde sie allerdings sehr individuell umgesetzt. Es kam zu sehr unterschiedlichen Regelungen. Das alles ist nach über 20 Jahren nicht mehr auf der Höhe der Zeit. Die DS-GVO war überfällig, um in allen Mitgliedsstaaten den gleichen Schutz und die gleiche Sicherheit zu gewährleisten. Ihr Kern: Personen sollen vor unbefugter Verwendung oder Weitergabe ihrer persönlichen Daten geschützt werden. Einrichtungen im Gesundheitswesen müssen nachweisen, dass sie den Datenschutz einhalten.

Um seine Rechte ausüben zu können, soll der Betroffene wissen, wer über ihn personenbezogene Daten erhebt und verarbeitet und zu welchem Zweck dies geschieht. Dazu gibt es ein Recht auf Auskunft über gespeicherte Daten, den Zweck der Verarbeitung, den Empfänger der Daten, die geplante Speicherdauer und rechtliche Hinweise. Auch kann die Löschung der Daten verlangt werden, wenn die Speicherung unzulässig war, die Daten zu der Zweckerfüllung nicht mehr erforderlich sind oder eine Einwilligung widerrufen wird. Ein solcher Widerspruch ist jederzeit möglich. Dann dürfen die

Daten nicht mehr verarbeitet werden. Mit dem Inkrafttreten der DS-GVO erhält jeder Betroffene auf Anfrage die über ihn gespeicherten Daten in Maschinenlesbarer Form (z.B. auf USB-Stick).

Dass die DS-GVO für das Gesundheitswesen erforderlich ist, unterstrich Mark Peters mit einigen drastischen Beispielen. So fand 2012 ein Fußgänger in Hessen rund 20 Krankenhausakten von Psychiatriepatienten. Getoppt wurde das noch in NRW. Ein Laptop wurde auf einem Flohmarkt angeboten. Auf der Festplatte die Daten Hunderter Psychiatriepatienten. Unverschlüsselte Patientendaten fanden sich auch im Internet. Vertraulicher Unterlagen wurden in einem öffentlich zugänglichen Müllcontainer entsorgt.

IT-Sicherheit oberstes Gebot

IT Sicherheit und Cyber Schutz müssen auch oberstes Gebot bei digitalen Anwendungen, z.B. der Steuerung von Insulinpumpen oder von Defibrillatoren sein. Nicht auszudenken, wenn solche im Körper eingesetzten Geräte gehackt werden.

Auch der persönliche Umgang mit Gesundheits-Apps war Thema. Man sollte sich genau informieren, auf welchen Servern die eigenen Daten landen. Oft stehen die Server außerhalb Europas. Die DS-GVO gilt dort nicht. Es gibt keinerlei Sicherheitsgarantie.

Mark Peters empfiehlt die Anforderungen an die Informationssicherheit sehr ernst zu nehmen. Wer als Gesundheitsdienstleister nicht ausreichend vorsorgt, müsse mit empfindlichen Strafen rechnen. Geldbußen können bis weit in die Tausende oder gar Millionen Euro gehen. Einige Anwaltsbüros hätten sich bereits auf Abmahnungen gegen Ärzte spezialisiert. Auf jeden Fall wollen die Aufsichtsbehörden verstärkt prüfen.

Gerade auch deshalb rate sein Unternehmen zu einem rechtlich korrekten Umgang mit Daten und IT Anwendungen. „Wir stellen für Patienten und Ärzte realitätsnahe, praxistaugliche und zeitgemäße sektorenübergreifende Lösungen zur Verfügung“, sagt Peters. Eine Übersicht bietet die Datenschutzkarte im Gesundheitswesen auf seiner Homepage www.datenschutzzertifizierung.info

Für die ASG ist klar, dass das Thema Informationssicherheit auf der politischen Tagesordnung bleiben muss. Die Kunst muss sein, einen optimalen Schutz für Patienten und Beschäftigte im Gesundheitswesen zu gewährleisten ohne ausufernde Bürokratie und Kosten. Chancen und Probleme der Digitalisierung werden auch einen Schwerpunkt auf der kommenden Bundeskonferenz im März 2019 bilden.

SPD ASG
Arbeitsgemeinschaft der
Sozialdemokratinnen und Sozialdemokraten
im Gesundheitswesen (ASG)
Region Heidelberg / Mannheim/Rhein-Neckar