Gesundheitsdaten von Patienten sind besonders sensibel. Deswegen sollte Datenschutz im Gesundheitssystem einen sehr hohen Stellenwert haben. Seit 2018 gibt es mit der Datenschutz-Grundverordnung („DS-GVO") eine europaweit geltende gesetzliche Regelung. Der Bundesverband Klinischer Diabetes Einrichtungen – BVKD- Die Diabetes-Kliniken – hat dieses Thema aufgegriffen und möchte nicht nur seine Mitgliedseinrichtung diesbezüglich sensibilisieren. Hierbei geht es nicht um abstrakte theoretische juristische Überlegungen, sondern um praxisrelevante Probleme, die alle im Gesundheitssystem tätigen Einrichtungen betreffen.

Für den folgenden Artikel konnten wir die Rechtsanwältin Johanna Clausen als Autorin gewinnen. Johanna Clausen ist bei der Kanzlei Taylor Wessing am Standort Berlin tätig. Sie berät überwiegend im Datenschutz sowie in urheber-, wettbewerbs-, IT- und fernabsatzrechtlichen Themen sowie sonstigen technologierechtlich relevanten Fragestellungen. Dies beinhaltet natürlich die Umsetzung und Einhaltung der DS-GVO. Ein Schwerpunkt von Johanna Clausen liegt in der Beratung gesundheitsbezogener Datenschutzfragen, wie etwa im Rahmen klinischer Studien und e-Health.

Dr. med. Thomas Werner

Rechtliche Folgen bei **Datenschutz**-Verstößen

Verantwortung *Personenbezogene Daten müssen von Gesetzes wegen geschützt werden. Das gilt besonders im Gesundheitswesen. Rechtsanwältin Johanna Clausen zeigt, worauf Sie besonders achten sollten.*

Text: Johanna Clausen.

Der Schutz personenbezogener Daten hat in Deutschland Tradition, dabei ist auch die Verarbeitung von Gesundheitsdaten keine Ausnahme. Personenbezogene Daten werden verstanden als sämtliche Informationen, die die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dennoch ging mit Inkrafttreten der Datenschutz-Grundverordnung („DS-GVO") im Mai 2018 ein Ruck durch das Land. Dies lag zum einen an den hohen Schutzvorgaben, die die europaweit gleichermaßen geltende Verordnung festsetzt. Vor allem sorgten aber die Vorschriften zu Bußgeldern, die für einen Verstoß gegen die Vorschriften der DS-GVO drohen, für Aufsehen. Nach den Regelungen der DS-GVO können die zuständigen Aufsichtsbehörden Summen von bis zu 20 Mio. Euro oder 4 % des weltweiten Bruttojahresumsatzes für Fälle der Zuwiderhandlung verhängen – je nachdem, welcher Betrag höher ist.

© Pixelot - Fotolia

Bei Verstößen gegen die Datenschutz-Grundversorgung drohen empfindliche Strafen.

Verstöße gegen das erforderliche Schutzniveau von Gesundheitsdaten

Personenbezogene Daten im Gesundheitsbereich werden hierbei nicht ausgespart. Vielmehr klassifiziert die DS-GVO Gesundheitsdaten als sogenannte „besondere Kategorien personenbezogener Daten“ und stuft diese Art der Daten als herausragend schützenswert ein. Denn bei Angaben, die einen Rückschluss auf Gesundheits- oder Krankheitszustand einer Person zulassen, handelt es um besonders sensible Informationen. Der Schutz dieser besonderen Daten wird nicht nur durch die DS-GVO, sondern auch durch diverse Spezialgesetze für den Bereich des Gesundheitswesens gewährleistet. Begeben sich Patienten in ärztliche Behandlung, ist dementsprechend auf Seite der Patienten das Interesse groß, dass mit den sensiblen Daten sorgfältig umgegangen wird und der Verarbeitung dieser Daten

heinz@kirchheim-verlag.de

hohe Sicherheitsstandards zugrunde liegen. Auf der anderen Seite stehen Ärzte und Krankenhäuser, die gehalten sind, sich an die strengen Verarbeitungsvorgaben zu halten und anderenfalls der Verhängung eines Bußgeldes ausgesetzt sind. Dabei ist die Tendenz erkennbar, dass der Schutz von Gesundheitsdaten vermehrt in den Fokus der Aufmerksamkeit der Öffentlichkeit und auch der Aufsichtsbehörden gerät. Dies liegt unter anderem auch darin begründet, dass in der jüngeren Vergangenheit im Gesundheitssektor einige Datenpannen unterschiedlichen Ausmaßes bekannt wurden. Ein prominentes Beispiel ist etwa der sogenannte „Patientendatenskandal“, bei dem zahlreiche (vor allem gesundheitsbezogene) Informationen, einschließlich Röntgen- und MRT-Aufnahmen mit den dazugehörigen Patientendaten im Internet zugänglich gemacht worden sind. Dies hatte nicht nur die zuständigen Aufsichtsbehörden dazu veranlasst, die Vorgänge zu prüfen – auch die Politik ist hellhörig geworden. Im Nachgang des Skandals wurden von mehreren hochrangigen Politikern grundsätzlich die Verhängung höherer Bußgelder für datenschutzrechtliche Verstöße bei der Verarbeitung von Gesundheitsdaten verlangt, gerade weil es sich um besonders sensible Daten mit einem entsprechenden Schutzbedürfnis handele.

> *„In Deutschland wurden bereits Bußgelder wegen rechtswidriger Verarbeitungen verhängt.“*

Aktuelle Beispiele für Bußgeldverfahren in Deutschland und der EU

In Deutschland wurden bereits Bußgelder wegen rechtswidriger Verarbeitungen verhängt, worunter unter anderem auch die unbefugte Offenlegung fällt. Im Dezember letzten Jahres wurde gegen die Universitätsklinik Mainz ein Bußgeld in Höhe von 105.000 Euro ausgesprochen, weil es zu einer Verwechslung bei der Aufnahme von Patienten kam, welches letztlich zu einer falschen Rechnungsstellung führte. Nach Auffassung der Aufsichtsbehörde

offenbarte dies strukturelle technische und organisatorische Defizite des Krankenhauses beim Patientenmanagement. Auch wenn die Aufsichtsbehörde in ihrem Bescheid die Bemühungen des Krankenhauses hervorgehoben hat, die Sicherheitslücken und Organisationsmängel schnellstmöglich zu beheben, so zeigt dieser Fall doch auf, dass auch ein vermeintlich geringfügiges individuelles Fehlverhalten zu hohen Bußgeldsanktionen führen kann.

© Stasique - AdobeStock

Regelmäßige Mitarbeiterschulungen zum Thema DS-GVO minimieren die Risiken.

Datenschutzrechtliche Verstöße bei der Verarbeitung von Gesundheitsdaten wurden auch in anderen EU-Mitgliedstaaten festgestellt und geahndet. So wurde etwa in Ungarn u.a. gegen ein Militär-Krankenhaus wegen unzureichender technischer und organisatorischer Vorkehrungen ein Bußgeld von 7 400 Euro verhängt. Die niederländische Aufsichtsbehörde verhängte wegen vergleichbarer Verstöße sogar ein Bußgeld von insgesamt 460 000 Euro, in Portugal betrug ein Bußgeld gegen ein Krankenhaus wegen unrechtmäßiger Offenlegung von Patientendaten ebenfalls 400 000 Euro. Im letzten Fall hatten mehrere unberechtigte Person die elektronische Patientenakte eines Prominenten eingesehen.

Wie werden Bußgelder festgelegt?

Dabei war lange Zeit (insbesondere in Deutschland) unklar, wie genau die Bußgelder der Höhe nach festzusetzen sind. Nach den Vorgaben der DS-GVO muss eine Geldbuße für den Einzelfall gelten und zugleich wirksam, verhältnismäßig und abschreckend sein. Die Datenschutzkonferenz, ein Zusammenschluss der Datenschutzaufsichtsbehörden des Bundes und der Länder, hat im vergangenen Jahr ein Konzept entwickelt, mit dem die Bußgeldhöhe nach wirtschaftlich messbaren Faktoren (etwa Größe des Betriebs, erzielte Jahresumsätze etc.) bei gleichzeitiger Zugrundelegung der in der DS-GVO genannten Kriterien - unter anderem Art, Umfang und Ausmaß des Verstoßes, Mitwirkungsbereitschaft des Verantwortlichen, Art oder Kategorie der betreffenden Daten etc.- bestimmt werden soll. Das Bußgeldkonzept ist zwar umstritten. Dennoch haben die Datenschutzaufsichtsbehörden teilweise bereits hiervon Gebrauch gemacht und mitunter empfindliche Bußgeldsanktionen verhangen, so etwa das 14,5 Millionen Euro Bußgeld gegen die Deutsche Wohnen in Berlin.

> *„Für Klinken, Praxen und andere Einrichtungen gilt, im Vorfeld äußerst aufmerksam zu sein.“*

Fazit: Problembewusst zu mehr (Gesundheits-)Datenschutz

Redaktion: 06131/9607035

Demnach gilt für Klinken und sämtliche ambulante Einrichtungen und Praxen, bereits im Vorfeld äußerst aufmerksam zu sein, um etwaigen Datenschutzverstößen im Ansatz entgegenzuwirken. Hierzu zählt zum einen die Einhaltung der in der DS-GVO statuierten allgemeinen Anforderungen, etwa die Einhaltung gesetzlicher Aufbewahrungsverpflichtungen und das Löschen von Daten, für deren Speicherung keine Rechtsgrundlage mehr besteht, die Information von Patienten über eine Datenverarbeitung oder eine fristgemäße Beantwortung von Auskunftsersuchen.

Daneben statuiert die DS-GVO, dass auf dem konkreten Schutzniveau der personenbezogenen Daten angemessene technische und organisatorische Maßnahmen eingeführt werden müssen. Eine Implementierung solcher Maßnahmen soll ebenfalls einer unrechtmäßigen Verarbeitung im eigenen Haus, aber auch einen unbefugten Zugriff Dritter auf die betreffenden Daten verhindern. Hierzu gehören demnach nicht nur die Einrichtung technischer Sicherheitsstandards (etwa IT Sicherheitsprotokolle, Verschlüsselung der Kommunikation, Passwortschutz etc.), die dem besonderen Schutz von Gesundheitsdaten gerecht werden sowie deren regelmäßige Wartung und Überprüfung. Es sind auch organisatorische Maßnahmen zu treffen, wie etwa unter anderem regelmäßige Mitarbeiterschulungen, ein auf Basis eines need-to-know-Prinzips gestaltetes Berechtigungskonzept für den Zugriff auf personenbezogene Daten sowie einen dokumentierten Plan, wie bei Datenpannen zu verfahren ist.

Vermag die Fülle der Verpflichtungen zunächst überbordend wirken, so sollten Betreiber von Kliniken und Praxisinhaber bedenken, dass ein besonderes Augenmerk auf datenschutzrechtliche Compliance Bußgelder abwenden oder jedenfalls Einfluss auf deren Höhe haben kann. Empfehlenswert ist daher, Datenschutz als einen fortlaufenden Prozess zu begreifen und regelmäßige Überprüfungen der getroffenen Maßnahmen, insbesondere in Bezug auf Effizienz und Effektivität, vorzunehmen.

i Wichtig

Für den Umgang mit personenbezogenen Gesundheitsdaten gibt es strenge Vorgaben. Damit aus der täglichen Praxis heraus keine juristischen Schwierigkeiten entstehen, bedarf es einer kontinuierlichen Prüfung.

i Autor

Johanna Clausen
Rechtsanwältin
Kanzlei Taylor Wessing, Standort Berlin

Schulungsprogramm für die Insulinpumpentherapie

NEU!

Inhalt:

- Curriculum
- Kartenset
- Skalenset
- USB-Stick
- Patientenbuch
- Arbeitsblätter

INPUT
SO PUMPT DAS LEBEN!

INPUT – das neue Schulungs- und Behandlungsprogramm für die Insulinpumpentherapie besteht aus **12 Kursstunden à 90 Minuten**.

Mehr Informationen unter: **www.kirchheim-shop.de/input**

FIDAM
FORSCHUNGSINSTITUT DIABETES

KIRCHHEIM

In Kooperation mit: MENARINI

BERLIN-CHEMIE
MENARINI

☐ **INPUT Schulungs- und Behandlungsprogramm für die Insulinpumpentherapie**
1 Curriculum, 1 Kartenset, 1 Skalenset, 1 USB-Stick und 1 Patientenbuch mit Arbeitsblättern
KI 42800, **Preis** 220,00 €

☐ **INPUT Patientenbuch „Selbstbestimmt leben mit Diabetes und Insulinpumpe“**
ISBN 978-3-87409-677-5, **Preis** 19,90 €

☐ **INPUT-Verbrauchsmaterial für 10 Patienten**
KI 42801, **Preis** 140,00 €

Preise inkl. MwSt. zzgl. Versandkosten, Preisänderungen vorbehalten

Name _____ E-Mail _____

Straße _____ Telefon _____

PLZ/Ort _____ Datum/Unterschrift _____

Hier angegebene personenbezogene Daten, insbesondere Name, Anschrift, Telefonnummer, E-Mailadresse, Bankdaten, die allein zum Zwecke der Durchführung des entstehenden Vertragsverhältnisses notwendig und erforderlich sind, werden auf Grundlage gesetzlicher Berechtigungen erhoben und zur Abwicklung an die ausführenden Dienstleister übermittelt (Stuttgarter Verlagskontor SVK GmbH und InTime Media Services GmbH).

KIRCHHEIMSHOP.de

oder bestellen Sie bei:

SVK-GmbH
Abtlg. VA/Kirchheim-Verlag
Postfach 106016, 70049 Stuttgart
Tel. 07 11 / 66 72-14 83
Fax 07 11 / 66 72-19 74
E-Mail: svk@svk.de

121.0001 goldnetz - Fotolia