med

Recht, Steuern, Betrieb – Informationen für Gesundheitsberufe und -unternehmen

Datenschutz in der Gesundheitswirtschaft – die komplette Serie aus ECOVIS med

Themen: 1. Ärztliche Schweigepflicht | 2. Gesetzliche Erlaubnisnormen | 3. Der Datenschutzbeauftragte in der Arztpraxis | 4. Gesundheitsdatenschutz nach der europäischen Datenschutzgrundverordnung (EU-DSGVO) 5. Der Einsatz von EDV und die Zusammenarbeit mit Dritten | 6. Der neue Beschäftigtendatenschutz

Digitalisierung und Datenschutz – das eine geht nicht ohne das andere!

Die Digitalisierung unserer Arbeitswelt und unseres Privatlebens schreitet mit Höchstgeschwindigkeit voran. Immer mehr Daten und Informationen liegen digital vor, immer weniger analog. Digitale Daten lassen sich aber viel leichter kopieren, transportieren, verfälschen und missbrauchen als analog abgelegte Informationen.

Insbesondere im Gesundheitswesen, wo wir immer mit höchst sensiblen Daten hantieren, muss der Schutz dieser Informationen ein besonders wichtiges Anliegen sein. Neben der ärztlichen Schweigepflicht setzt die Europäische Datenschutzgrundverordnung seit 25. Mai 2018 hier den Rahmen für den Umgang mit personenbezogenen Daten.

Was das neue Recht für Sie in der Praxis bedeutet, haben wir in einer Serie in ECOVIS med in sechs Teilen vorgestellt. In diesem Sonderdruck sind alle Teile nochmals für Sie zusammengefasst.

Wenn Sie weitere Fragen haben, wenden Sie sich gern an uns:
www.ecovis.com/datenschutzberater/

Eine interessante Lektüre wünschen Ihnen

Tim Müller
Rechtsanwalt und Fachanwalt
für Medizinrecht bei Ecovis in München

Axel Keller
Rechtsanwalt und Datenschutzbeauftragter
bei Ecovis in Rostock

SERIE – DATENSCHUTZ IN DER GESUNDHEITSWIRTSCHAFT

Eine der bedeutendsten Entwicklungen der nächsten Jahre ist die Digitalisierung. Diese Entwicklung wird viele Lebensbereiche grundlegend verändern. Hiervon ist auch das Verhältnis zum Patienten und der Umgang mit seinen sensiblen Daten betroffen. Im Rahmen einer Serie werden wir uns in ECOVIS med mit den wichtigsten Punkten beschäftigen:

1. **Grundlagen des Datenschutzes: ärztliche Schweigepflicht**
2. Gesetzliche Erlaubnisnormen
3. Gesundheitsdatenschutz nach der neuen EU-Datenschutzgrundverordnung
4. Einsatz von EDV und Zusammenarbeit mit Dritten
5. Arbeitnehmerdatenschutz

Grundlagen des Datenschutzes

ÄRZTLICHE SCHWEIGEPFLICHT

„Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als ein Geheimnis betrachten.“ Eid des Hippokrates

Der Eid des Hippokrates wird heute nicht mehr geleistet und er hat auch keine rechtliche Bedeutung mehr. Doch die darin zum Ausdruck kommende Pflicht des Arztes zur Verschwiegenheit über Patienteninformationen ist unverändert von grundlegender Bedeutung für das besondere Vertrauensverhältnis zwischen Behandler und Patient.

Die ärztliche Schweigepflicht gehört zum Kernbereich der ärztlichen Berufsethik. Ihre rechtliche Grundlage ist in der (Muster-) Berufsordnung beziehungsweise den Berufsordnungen der Landesärztekammern festgeschrieben. Sie wird flankiert von der Strafvorschrift, aber auch von prozessualen Zeugnisverweigerungsrechten.

„Eine wirksame Einwilligungserklärung muss schriftlich, aktuell, konkret und freiwillig erstellt sein.“

Axel Keller, LL.M., Rechtsanwalt bei Ecovis in Rostock

Die Schweigepflicht umfasst alle Daten, an deren Geheimhaltung der Patient ein schutzwürdiges Interesse hat. Sie gilt grundsätzlich gegenüber allen Dritten, also auch anderen Ärzten und Familienangehörigen, und gilt über den Tod des Patienten fort. Der berufsrechtlich geregelten Schweigepflicht unterliegen nur Ärzte, dem strafrechtlichen Verbot allerdings auch Angehörige anderer Heilberufe und Gesundheitsfachberufe sowie deren berufsmäßig tätige Gehilfen.

Datenschutz ist in Deutschland grundsätzlich als sogenanntes Verbot mit Erlaubnisvorbehalt ausgestaltet. Dieser Grundsatz gilt auch für Patientendaten. Das bedeutet, dass keine Daten weitergegeben werden dürfen, wenn hierfür keine Erlaubnis vorliegt. Als Erlaubnis kommen im Datenschutzrecht die Einwilligung des Betroffenen u nd g esetzliche Vorschriften in Betracht.

Der Arzt ist berechtigt, Patientendaten weiterzugeben, wenn eine wirksame Einwilligung des Patienten vorliegt. Die ausdrücklich erteilte Einwilligung muss auf einer mit freiem Willen getroffenen E ntscheidung des Patienten beruhen. Dazu muss der Patient umfassend informiert sein und insbesondere wissen, zu welchem Zweck welche Daten vom Behandler an wen weitergegeben werden sollen. Der Patient sollte immer auch auf die Folgen der nicht erteilten Einwilligung hingewiesen werden. Die Einwilligung sollte – jedenfalls zu Beweis- und Dokumentationszwecken – schriftlich erteilt werden.

Die Einwilligung kann in bestimmten Fällen auch konkludent – stillschweigend – erteilt werden. In Betracht kommt schließlich auch eine mutmaßliche Einwilligung, beispielsweise bei der Kontaktaufnahme zu Angehörigen bewusstloser Personen. ●

In Ausgabe 2/2017 von ECOVIS med lesen Sie über gesetzliche Erlaubnisnormen.

SERIE – DATENSCHUTZ IN DER GESUNDHEITSWIRTSCHAFT

Eine der bedeutendsten Entwicklungen der nächsten Jahre ist die Digitalisierung. Diese Entwicklung wird viele Lebensbereiche grundlegend verändern. Hiervon sind auch das Verhältnis zum Patienten und der Umgang mit seinen sensiblen Daten betroffen. Im Rahmen einer Serie werden wir uns in ECOVIS med mit den wichtigsten Punkten beschäftigen:

1. Grundlagen des Datenschutzes: ärztliche Schweigepflicht
2. **Gesetzliche Erlaubnisnormen**
3. Gesundheitsdatenschutz nach der neuen EU-Datenschutzgrundverordnung
4. Einsatz von EDV und Zusammenarbeit mit Dritten
5. Arbeitnehmerdatenschutz

Grundlagen des Datenschutzes

GESETZLICHE ERLAUBNISNORMEN

Welche Patientendaten dürfen an Dritte weitergegeben werden? Das ist in einer Vielzahl von Gesetzen, Paragraphen und Bestimmungen geregelt.

Das Verarbeiten personenbezogener Daten ist nach Paragraph 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) grundsätzlich erlaubt, wenn dies gesetzlich angeordnet ist.

Im Zusammenhang mit der Behandlung von Patienten müssen (fast) immer Daten zwischen verschiedenen Beteiligten ausgetauscht werden. Täglich werden Tausende Patienten vom Hausarzt zum Facharzt oder vom niedergelassenen Arzt ins Krankenhaus überwiesen. Dabei findet naturgemäß ein Austausch besonders geschützter Gesundheitsdaten statt. Aber auch neben der eigentlichen ärztlichen Behandlung ist ein Datenaustausch mit Dritten notwendig. Stets werden hierfür Daten des Patienten weitergegeben:

- Die Honorarabrechnung wird an die Krankenversicherung gesandt.
- Ärztliche Abrechnungsstellen übernehmen den Honorareinzug von Privatversicherten.
- Es werden Wirtschaftlichkeitsprüfungen durchgeführt, Unfallschäden oder Rentenanträge geprüft.

Wichtigste Quelle gesetzlicher Erlaubnisnormen ist in diesem Zusammenhang das Fünfte Buch Sozialgesetzbuch, SGB V (siehe Kasten „Alles gut geregelt“, Seite 11).

Für viele Arten der Auskunftserteilung gegenüber Dritten, insbesondere Krankenkassen, dem Medizinischen Dienst der Krankenkassen (MDK), aber auch Sozial- und Versorgungsämtern gibt es Vordrucke. Die hierfür vereinbarten Regelungen im Bundesmantelvertrag und in der sogenannten Vordruckvereinbarung konkretisieren die gesetzliche Pflicht zur Datenübermittlung.

„Gibt es solche Vordrucke, so sollten diese in jedem Fall verwendet und auch nur die darin enthaltenen Fragen beantwortet und darauf bezogene Daten übermittelt werden“, rät Ecovis-Rechtsanwalt Axel Keller aus Rostock. Die Vordrucke gelten allerdings nicht nur für den zur Auskunft verpflichteten Arzt. Auch die anfragende Stelle hat vorhandene Vordrucke zu verwenden. Hin und wieder werden Fragen auf den Vordrucken geändert oder zusätzliche Fragen gestellt. „Diese Abweichungen

„Achten Sie sehr genau darauf, welche Patientendaten Sie an wen weitergeben dürfen. Lassen Sie sich im Zweifelsfall beraten.“

Axel Keller, LL.M., Rechtsanwalt bei Ecovis in Rostock

„Gibt es keine gesetzliche Erlaubnisnorm zur Weitergabe von Patientendaten, sind Ärzte in jedem Fall an ihre Schweigepflicht gebunden."

Susann Harder
Rechtsanwältin bei Ecovis in Rostock

entsprechen nicht den Vereinbarungen der Partner von Bundesmantelvertrag und Vordruckvereinbarung und können vom Arzt abgelehnt werden", erklärt Keller. Steht kein Vordruck zur Verfügung, so muss der Anfragende die Rechtsgrundlage für die Auskunftsverpflichtung des Arztes und die Gebührenordnungsposition mitteilen, nach der die Informationserteilung vergütet wird. Fehlt diese Mitteilung, so sollte bei der anfragenden Stelle vor der Informationserteilung um eine Ergänzung der Anfrage gebeten werden.

Anfragen des MDK beantworten

Die Datenübermittlung an Krankenkassen, die zur Klärung der Frage dienen soll, ob der MDK eingeschaltet wird, ist unzulässig. Fordert der MDK Daten an, so muss er darlegen, aus welchen Rechtsgrundlagen sich seine Auskunftsberechtigung und die Auskunftspflicht des Arztes ergeben. Er hat zudem den Zweck der erbetenen Auskunft zu erläutern und einen an ihn – den MDK – adressierten Freiumschlag beizufügen. Für einen ausführlichen Bericht an den MDK sollte in jedem Fall der entsprechende Vordruck verwendet werden.

Auch außerhalb des SGB V gibt es viele gesetzliche Regelungen, die eine Datenübermittlung erlauben. „Welche Daten weiterzugeben sind, ist jeweils in eigenen Paragraphen geregelt. Ärzte sollten diese kennen oder sich von Fall zu Fall bei ihrem persönlichen Berater informieren", sagt Susann Harder, Rechtsanwältin bei Ecovis in Rostock.

Die wichtigsten Bestimmungen sind:

- Infektionsschutzgesetz
- Landeskrebsregistergesetze
- Röntgenverordnung
- Strahlenschutzverordnung
- Betäubungsmittelgesetz
- Gesetzliche Unfallversicherung
- Personenstandsgesetz
- Gesetz zur Kooperation und Information im Kinderschutz

Für die Weitergabe von Daten an private Krankenversicherer, private Verrechnungsstellen oder externe Gutachter gibt es keine gesetzlichen Erlaubnisnormen. „Hier muss immer eine Einwilligung des Patienten vorliegen, die schriftlich, konkret und auf den Einzelfall bezogen gefasst ist und für diesen einen Fall den Arzt von seiner Schweigepflicht entbindet", erklärt Harder. Eine pauschale, auf alle denkbaren Fälle der Weitergabe von Daten bezogene Einwilligungserklärung, wie sie manchmal noch zum Einsatz kommt, ist hingegen unwirksam.

Auch im Rahmen der Praxisübergabe an einen Nachfolger gibt es keine gesetzlichen Erlaubnisnormen. Hier bedarf es der Einwilligung aller Patienten. Kann diese vor der Praxisübergabe nicht eingeholt werden, so hat sich das „Zwei-Schrank-Modell" bewährt: Der Praxisnachfolger verwahrt die Patientendaten in einem verschlossenen Schrank und übernimmt sie erst dann in seine laufende Patientenkartei, wenn der Patient dem zugestimmt hat. In der Praxis zum Einsatz kommende Software sollte eine entsprechende Funktion aufweisen.

Alles gut geregelt

Erlaubnisse (auszugsweise), die im Fünften Buch Sozialgesetzbuch geregelt sind und die Sie kennen sollten. In diesen Fällen dürfen Sie Patientendaten weitergeben:

Übermittlung an die Kassenärztlichen Vereinigungen zum Zweck der
– allgemeinen Aufgabenerfüllung
– Abrechnung
– Qualitäts- und Wirtschaftlichkeitsprüfung im Einzelfall

Übermittlung an die Prüfstellen zum Zweck der
– Wirtschaftlichkeitsprüfung

Übermittlung an die Krankenkassen zum Zweck der
– allgemeinen Aufgabenerfüllung
– Mitteilung von Krankheitsursachen und drittverursachten Gesundheitsschäden
– Unterstützung des Versicherten bei Behandlungsfehlern
– Übermittlung der Diagnose bei Arbeitsunfähigkeitsbescheinigungen

Übermittlung an den Medizinischen Dienst der Krankenkassen (MDK)
– für Prüfungen, Beratungen und gutachtliche Stellungnahmen

SERIE – DATENSCHUTZ IN DER GESUNDHEITSWIRTSCHAFT

Eine der bedeutenden Entwicklungen der nächsten Jahre ist die Digitalisierung. Sie verändert viele Lebensbereiche grundlegend. Auch das Verhältnis zwischen Arzt und Patient und der Umgang mit dessen sensiblen Daten ist betroffen. Im Rahmen der Serie werden wir uns in ECOVIS med mit den wichtigsten Punkten beschäftigen. Aus aktuellem Anlass haben wir die Serie erweitert und einen zusätzlichen Punkt aufgenommen, den wir in dieser Ausgabe besprechen:

1. Grundlagen des Datenschutzes: ärztliche Schweigepflicht
2. Gesetzliche Erlaubnisnormen
3. **Der Datenschutzbeauftragte in der Arztpraxis**
4. Gesundheitsdatenschutz nach der neuen EU-Datenschutzgrundverordnung
5. Einsatz von EDV und Zusammenarbeit mit Dritten
6. Arbeitnehmerdatenschutz

Grundlagen des Datenschutzes

DER DATENSCHUTZBEAUFTRAGTE IN DER ARZTPRAXIS

Die EU-Datenschutzgrundverordnung bringt eine massive Veränderung für Arztpraxen mit sich. Ab Mai 2018 müssen Ärzte häufig einen Datenschutzbeauftragten benennen.

Bislang war nach dem Bundesdatenschutzgesetz (BDSG) die Bestellung eines Datenschutzbeauftragten in einer Arztpraxis nur in seltenen Ausnahmefällen gesetzlich erforderlich. Dies wird sich ab 25. Mai 2018 jedoch grundlegend ändern. Die Benennung eines Datenschutzbeauftragten ist in Deutschland ab diesem Zeitpunkt dann erforderlich, wenn in der Regel mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Das fordert die EU-Datenschutzgrundverordnung (EU-DSGVO), die die nationalen Schutzgesetze weitestgehend ablöst. Diese Voraussetzung wird in vielen Arztpraxen allerdings nicht erfüllt sein.

„Stellt der Datenschutzbeauftragte Defizite beim Umgang mit Daten fest, ist dies der Praxisleitung unverzüglich mitzuteilen."

Tim Müller, Rechtsanwalt und Fachanwalt für Medizinrecht bei Ecovis in München

Die Verarbeitung personenbezogener Daten von Patienten sollte nicht als umfangreich gelten, wenn dies durch einen einzelnen Arzt erfolgt.

Nach der neuen Verordnung muss ein Datenschutzbeauftragter aber auch benannt werden, wenn die umfangreiche Verarbeitung besonders geschützter Daten den Kern der Tätigkeit bildet oder eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist. Auf die Zahl der Mitarbeiter kommt es dann nicht an. Eine DSFA ist vorzunehmen, wenn ein voraussichtlich hohes Risiko mit der Verarbeitung von Daten – wie bei Patientendaten üblich – verbunden ist.

Selbstverständlich ist die Ausübung der Heilkunde der Kern der ärztlichen Tätigkeit. Allerdings gibt es, gerade für Vertragsärzte, eine Vielzahl von Dokumentations- und Abrechnungspflichten, deren Grundlage die Erhebung umfangreicher Daten bildet. Ein Unternehmen – im datenschutzrechtlichen Sprachgebrauch Verantwortlicher genannt – kann dabei durchaus mehrere Kerntätigkeiten haben. „Bereits dem Wortlaut nach spricht einiges dafür, dass Arztpraxen, in denen regelmäßig und umfangreich besonders geschützte Patienten- oder Gesundheitsdaten zu verarbeiten sind, dem Anwendungsbereich der genannten Bestimmungen unterliegen", erklärt Tim Müller, Rechtsanwalt und Fachanwalt für Medizinrecht bei Ecovis in München.

Diese Überlegung wird durch die Erwägungsgründe der EU-DSGVO gestützt. In diesen erläutert der europäische Gesetzgeber, aus welchen Motiven und mit welcher Absicht er bestimmte Vorschriften erlassen hat. Sie dienen daher als wichtige Verständnisquelle europäischen Rechts.

Erwägungsgrund 91 (Auszug)

„Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen

einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.“

Der europäische Gesetzgeber hat also erkannt, dass die Verarbeitung besonders geschützter Patienten- und Gesundheitsdaten neben der heilberuflichen Ausübung zentral für die ärztliche Tätigkeit ist. Er hat nur die Datenverarbeitung durch einen einzelnen Arzt vom Anwendungsbereich der Vorschrift ausgenommen. Der Gesetzgeber geht davon aus, dass dessen Datenverarbeitung nicht als umfangreich gilt.

„Beim Einsatz eines Datenschutzbeauftragten ist höchste Eile geboten, denn die Umsetzungsfrist endet am 25. Mai 2018.“

Axel Keller, LL.M., Rechtsanwalt bei Ecovis in Rostock

Neue Pflichten für Mehrarzteinrichtungen

Dies bedeutet im Umkehrschluss allerdings für alle Mehrarzteinrichtungen, insbesondere für alle Gemeinschaftspraxen und Medizinischen Versorgungszentren, aber auch für alle Fälle, in denen (auch) angestellte Ärzte tätig sind, dass deren Datenverarbeitung als umfangreich gilt.

„In solchen Praxen ist daher unserer Auffassung nach ab Mai 2018 zwingend ein Datenschutzbeauftragter zu benennen“, hebt Axel Keller, Rechtsanwalt bei Ecovis in Rostock und seit vielen Jahren als Datenschutzbeauftragter in Gesundheitseinrichtungen tätig, besonders hervor. „Ein Verstoß gegen die Pflicht zur Benennung eines Datenschutzbeauftragten kann erhebliche Bußgelder zur Folge haben. Da die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der jeweiligen Aufsichtsbehörde des Bundeslandes zwingend mitzuteilen sind“, erklärt Keller weiter, „ist leicht zu kontrollieren, ob die Ärzte ihren Pflichten nachkommen.“

Der Datenschutzbeauftragte kann sowohl Beschäftigter des Verantwortlichen, also der Praxis, als auch ein externer Beauftragter sein. Die EU-DSGVO bestimmt lediglich, dass der Datenschutzbeauftragte auf der Grundlage

- seiner beruflichen Qualifikation und insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie
- seiner Fähigkeit zur Erfüllung der ihm obliegenden Aufgaben

benannt wird.

Rechte und Pflichten eines Datenschutzbeauftragten

Der Datenschutzbeauftragte sollte stets unabhängig und mit einem gewissen Durchsetzungsvermögen agieren, um seine Aufgaben erfüllen zu können. Ist die Benennung eines Datenschutzbeauftragten verpflichtend, dann sind vor der Benennung eines Mitarbeiters als interner Datenschutzbeauftragter einige Besonderheiten zu berücksichtigen:

- Die Abberufung des Datenschutzbeauftragten ist nur aus wichtigem Grund zulässig.
- Der Beschäftigte genießt während der Zeit seiner Benennung und für die Dauer von einem Jahr nach deren Ende einen Sonderkündigungsschutz. Das Arbeitsverhältnis kann in dieser Zeit also nicht wirksam durch ordentliche Kündigung beendet werden.

Natürlich müssen auch Arztpraxen ohne Pflicht zur Bestellung eines Datenschutzbeauftragten die nach der EU-DSGVO bestehenden Pflichten erfüllen. „Unabhängig von den zu erfüllenden Anforderungen kann die Bestellung eines Datenschutzbeauftragten für die Praxis ohnehin sinnvoll sein, um sich möglichst wenig angreifbar zu machen“, erklärt Ecovis-Rechtsanwalt Tim Müller. ●

Drastische Strafen

Die Aufsichtsbehörden können ab Mai 2018 bei Verstößen gegen das Datenschutzgesetz zwei Gruppen von massiven Bußgeldern verhängen:

- Bis zu 10 Millionen Euro oder 2 Prozent des Vorjahresumsatzes
- Bis zu 20 Millionen oder 4 Prozent des Vorjahresumsatzes

Sie haben Fragen zu diesem Thema?

- Ist bei meiner Praxisgröße ein Datenschutzbeauftragter zu benennen?
- Welche Qualifikation muss ein Datenschutzbeauftragter mitbringen und was fällt in dessen Arbeitsbereich?
- Ist eine interne oder externe Lösung für meine Praxis die bessere?
- Wer haftet für Fehler des Datenschutzbeauftragten?

Rufen Sie uns an, Telefon 089 5898-266, oder schicken Sie uns eine E-Mail: redaktion-med@ecovis.com

In dieser Ausgabe Teil 4 der Serie:
Gesundheitsdatenschutz nach der europäischen Datenschutzgrundverordnung (EU-DSGVO)

Eine der bedeutenden Entwicklungen zurzeit ist die Digitalisierung. Sie verändert viele Lebensbereiche grundlegend. Auch das Verhältnis zwischen Arzt und Patient und der Umgang mit dessen sensiblen Daten ist betroffen.

Die bereits veröffentlichten Beiträge zur ärztlichen Schweigepflicht, zu den gesetzlichen Erlaubnisnormen und dem Datenschutzbeauftragten in der Arztpraxis finden Sie unter: www.ecovis.com/medizin

Grundlagen des Datenschutzes

KEINE REGELN OHNE AUSNAHMEN

Daten von Personen dürfen nur nach deren Zustimmung verarbeitet werden. Künftig aber auch dann, wenn ein Patient körperlich oder rechtlich nicht (mehr) in der Lage ist, sein Okay zu geben.

Die Verarbeitung besonderer personenbezogener Daten wie genetische oder biometrische Daten und Gesundheitsdaten ist nach der Datenschutzgrundverordnung (DSGVO) untersagt, wenn dort keine ausdrücklich genannte Ausnahme vorliegt. Diese Daten dürfen jedoch dann verarbeitet werden, wenn eine wirksame Einwilligung der betroffenen Person vorliegt. Erstmals gesetzlich geregelt ist, dass die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person auch dann erfolgen darf, wenn die Zustimmung aus körperlichen oder rechtlichen Gründen nicht erteilt werden kann. „Damit hat beispielsweise die Datenerhebung bei der Erstversorgung bewusstloser Patienten endlich eine gesetzliche Grundlage“, betont Axel Keller, Rechtsanwalt bei Ecovis in Rostock und externer Datenschutzbeauftragter.

Die neue DSGVO sowie das neue Bundesdatenschutzgesetz (BDSG) enthalten zudem gesetzliche Erlaubnisse für die Datenverarbeitung in der Gesundheitsvorsorge und Arbeitsmedizin, bei der Beurteilung der Arbeitsfähigkeit von Beschäftigten, der medizinischen Diagnostik und der Behandlung im Gesundheits- oder Sozialbereich. Die Verarbeitung hat dabei stets durch ärztliches Personal oder sonstige Personen zu erfolgen, die einer entsprechenden Geheimhaltungspflicht unterliegen. Ab jetzt sind auch externe Dienstleister (Auftragsverarbeiter) in den Kreis der Geheimnisträger aufgenommen und die entsprechenden Regelungen ergänzt worden, beispielsweise im Strafgesetzbuch. Die Erlaubnis, solche Daten verarbeiten zu dürfen, zieht die gesetzliche Pflicht nach sich, Maßnahmen einzusetzen, die die Interessen der betroffenen Person wahren (siehe Tabelle).

Zudem ist ein Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen einzurichten. „Unabhängig von ihrer Größe müssen Arztpraxen, Krankenhäuser und Labore künftig ein Datenschutz-Managementsystem einrichten und vorhalten“, macht Susann Harder, Rechtsanwältin bei Ecovis in Rostock und externe Datenschutzbeauftragte, deutlich. „Unserer Einschätzung nach drohen auch und gerade in der Gesundheitswirtschaft erhebliche Bußgelder“, warnt Keller. ●

Die Pflichten bei der Datenverarbeitung

Welche Maßnahmen zum Schutz von Personendaten angemessen und spezifisch sind, hat der Verantwortliche unter Berücksichtigung einer Vielzahl von Aspekten zu entscheiden.

Maßgebliche Aspekte	Mögliche Maßnahmen
Stand der Technik	Technisch-organisatorische Maßnahmen zur Sicherstellung der Verarbeitung nach DSGVO
Implementierungskosten	Maßnahmen zur Zugriffsprotokollierung
Art, Umfang, Umstände und Zweck der Verarbeitung	Sensibilisierung/Schulung der an der Verarbeitung beteiligten Personen
Eintrittswahrscheinlichkeit	Bestellung eines Datenschutzbeauftragten
Schwere der Risiken für die Rechte und Freiheiten der betroffenen Person	• Zugangsbeschränkung (Berechtigungskonzepte, Zugriffshierarchien) • Pseudoanonymisierung, Verschlüsselung • Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste, Wiederherstellbarkeit von Daten und Systemen (Notfallanlaufplan)

Sie haben Fragen?

- Nach welchen Kriterien ist ein Datenschutz-Managementsystem aufzubauen?

Rufen Sie uns an, Telefon 089 5898-266, oder schicken Sie uns eine E-Mail: redaktion-med@ecovis.com

In dieser Ausgabe Teil 5 der Serie:
Der Einsatz von EDV und die Zusammenarbeit mit Dritten

Eine der bedeutenden Entwicklungen zurzeit ist die Digitalisierung. Sie verändert viele Lebensbereiche grundlegend. Auch das Verhältnis zwischen Arzt und Patient und der Umgang mit dessen sensiblen Daten sind betroffen.

Die bereits veröffentlichten Beiträge zur ärztlichen Schweigepflicht, zu den gesetzlichen Erlaubnisnormen und dem Datenschutzbeauftragten in der Arztpraxis finden Sie unter: www.ecovis.com/medizin

Grundlagen des Datenschutzes

ZUGRIFF RICHTIG REGELN

In der vernetzten Welt ist die Kooperation mit Dritten der Regelfall – für den Datenschutz eine ganz besondere Herausforderung.

Beim Einsatz von EDV in der Praxis ist der Arzt verpflichtet, die Sicherheit der Patientendaten zu gewährleisten. Neben den berufsrechtlichen Vorgaben zur ärztlichen Schweigepflicht enthält die Datenschutzgrundverordnung (DSGVO) Vorgaben für die Datenverarbeitung und -sicherheit. Bundesärztekammer (BÄK) und Kassenärztliche Bundesvereinigung (KBV) hatten angekündigt, die hierfür geltenden Empfehlungen an die DSGVO anzupassen. Am 9. März 2018 haben BÄK und KVB die Änderungen veröffentlicht: www.bundesaerztekammer.de/recht/aktuelle-rechtliche-themen/datenschutzrecht.

Die DSGVO schreibt eine „Datenschutzfolgenabschätzung“ vor, wenn umfangreich besondere Kategorien von Daten verarbeitet werden, zu denen Gesundheitsdaten zählen. Im Rahmen der Datenschutzfolgenabschätzung kommt den technischen und organisatorischen Maßnahmen, die zur Einhaltung des Datenschutzes und zur Sicherheit der Datenverarbeitung getroffen wurden, erhebliche Bedeutung zu. Ärzte und andere Verarbeiter von Gesundheitsdaten, wie Kliniken oder Pflegeeinrichtungen und -dienste, sollten daher diesen Maßnahmen besondere Beachtung schenken. Beim Einsatz von EDV sollten die folgenden Punkte immer umgesetzt werden:

- der Einsatz von Passwörtern,
- ein stets aktueller Virenschutz sowie
- die Einführung eines Zugriffs- und Berechtigungskonzepts.

Passwörter richtig vergeben

Nach wie vor wird oft für die Mitarbeiter zusammen lediglich ein gemeinsames Passwort eingerichtet, zum Beispiel „Schwester“, weil häufig wechselnde Anmeldungen und die angebliche Vergesslichkeit der

Tipp

Überlegen Sie, ob an den Arbeitsplätzen tatsächlich überall USB-Anschlüsse erforderlich sind. Sie lassen sich deaktivieren, was die Datensicherheit deutlich erhöht.

„Bei der DSGVO sind alle Maßnahmen im Rahmen von Richtlinien oder Arbeitsanweisungen zu dokumentieren.“

Axel Keller
Rechtsanwalt bei Ecovis in Rostock und externer Datenschutzbeauftragter

Mitarbeiter individuelle Passwörter als unpraktikabel erscheinen lassen. „Allerdings erfüllt das nicht die Anforderungen an eine Lese- und Zugriffsprotokollierung. Dieses Vorgehen ist datenschutzrechtlich problematisch“, sagt Axel Keller. Um angemessenen Schutz zu erhalten, empfiehlt Rechtsanwalt Keller:

- Für jeden Mitarbeiter ist ein eigenes, individuelles Passwort einzurichten;
- Passwörter sind regelmäßig zu erneuern und
- dabei ist auf die Länge und die Verwendung von verschiedenen Zeichen (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen) zu achten.

Sich gegen Angriffe von außen gut wappnen

In jüngster Zeit hat es immer wieder größere Angriffe mit Schadsoftware gegeben, die auch Auswirkungen auf den Endanwender solcher Software hatten. „Aktuelle Viren-Schutzprogramme sind unverzichtbar. E-Mails und jegliche Kommunikation über das Internet sollten zentral auf Viren untersucht werden“, empfiehlt Keller. Zusätzlich sollte jeder Computer mit einem lokalen Viren-Schutzprogramm ausgestattet sein, das ständig im Hintergrund läuft. Im Rahmen eines Zugriffs- und Berechtigungskonzepts sollten daher

- rollen- oder personenbezogene Zugriffsrechte auf das EDV-System eingeräumt werden, die sich auf das Notwendigste beschränken, und
- keine Administratorrechte für einfache Nutzer vergeben werden.

„Daneben sind Vorgaben zur Datensicherung und -wiederherstellung zu erarbeiten, damit im Notfall kurzfristig zumindest eine eingeschränkte Funktionsfähigkeit des Betriebs und der Patientenversorgung hergestellt werden kann“, rät Keller.

Der Dritte im Bunde

In der Zusammenarbeit mit Dritten ist vor allem der Auftragsverarbeiter von Bedeutung. In aller Regel sind dies Rechenzentren oder die Abteilung Fernwartung von Softwareunternehmen, aber auch – im Rahmen der Lohn- und Finanzbuchhaltung – der Steuerberater. „Zwischen Auftraggeber und Auftragsverarbeiter ist ein Vertrag über die Auftragsverarbeitung zu schließen, in dem verschiedene Aspekte zwingend geregelt sein müssen“, sagt Keller. Dazu gehören beispielsweise, dass die Verarbeitung von Daten nur auf dokumentierte Weisung des Verantwortlichen stattfinden darf, die Verpflichtung der Mitarbeiter zur Vertraulichkeit sowie die Gewährleistung der Sicherheit der Datenverarbeitung. ●

Tipp

Haben Sie Ihren Laptop oder PC mit einem Passwort geschützt? Sehr gut! Leider schützt dies die Daten auf der Festplatte gar nicht. Denken Sie daher an den Einsatz einer Festplattenverschlüsselung.

Sie haben Fragen?

- Welche Abläufe sind im Rahmen der DSGVO zu dokumentieren?
- Wie sind Verträge mit externen Dienstleistern zu gestalten?

Rufen Sie uns an, Telefon 089 5898-266, oder schicken Sie uns eine E-Mail: redaktion-med@ecovis.com

SERIE – DATENSCHUTZ IN DER GESUNDHEITSWIRTSCHAFT

In diese Ausgabe Teil 6 (letzte Folge der Serie):
Der Beschäftigtendatenschutz

Eine der bedeutenden Entwicklungen zurzeit ist die Digitalisierung. Sie verändert viele Lebensbereiche grundlegend. Auch das Verhältnis zwischen Arzt und Patient und der Umgang mit dessen sensiblen Daten sind betroffen.

Die bereits veröffentlichten Beiträge zur ärztlichen Schweigepflicht, zu den gesetzlichen Erlaubnisnormen und dem Datenschutzbeauftragten in der Arztpraxis finden Sie unter: www.ecovis.com/medizin

Grundlagen des Datenschutzes

DER NEUE BESCHÄFTIGTENDATENSCHUTZ

Im Rahmen der Einführung der EU-Datenschutzgrundverordnung am 25. Mai 2018 wurde auch der Beschäftigtendatenschutz neu geregelt.

„Wer beim Beschäftigtendatenschutz noch nichts unternommen hat, sollte das dringend nachholen. Sonst drohen Abmahnungen und Schadenersatzansprüche."

Dr. Gunnar Roloff
Rechtsanwalt bei Ecovis in Rostock

Am 25. Mai 2018 trat die EU-Datenschutzgrundverordnung (EU-DSGVO) in Kraft. Der Beschäftigtendatenschutz – oder auch Arbeitnehmerdatenschutz – ist in der DSGVO allerdings nicht eigenständig geregelt. Durch eine sogenannte Öffnungsklausel war es den Mitgliedstaaten überlassen, neue Vorschriften zu formulieren. Die DSGVO sieht aber vor, dass die jeweils geschaffenen Vorschriften

- angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde beinhalten,
- die berechtigten Interessen und die Grundrechte der betroffenen Person wahren. Dies gilt insbesondere im Hinblick auf die Transparenz bei der Verarbeitung und Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben.

Der deutsche Gesetzgeber hat die ihm eingeräumte Möglichkeit genutzt und in Paragraph 26 eine Regelung zum Arbeitnehmerdatenschutz in das überarbeitete, ebenfalls ab dem 25. Mai 2018 geltende Bundesdatenschutzgesetz (BDSG – neu) aufgenommen. Künftig gilt der Arbeitgeberdatenschutz nicht nur für Beschäftigte in den unterschiedlichsten Formen – von Festangestellten bis Mini-Jobber –, sondern auch für Bewerber und ehemalige Mitarbeiter.

Wie bisher dürfen personenbezogene Daten von Beschäftigten dann verarbeitet werden, wenn dies erforderlich ist

- für die Entscheidung über die Aufnahme eines Beschäftigungsverhältnisses,
- für dessen Durchführung oder Beendigung oder
- zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten.

In diesen oben genannten Fällen ist die Einholung einer Einwilligung für die Verarbeitung der personenbezogenen Daten der Mitarbeiter nicht erforderlich. Zudem ist unter bestimmten Voraussetzungen die Verarbei-

Tipp

Die Ecovis-Rechtsanwälte beraten Unternehmen bundesweit bei der Umsetzung der DSGVO. Mehr dazu:
www.ecovis.com/datenschutzberater

tung personenbezogener Daten erlaubt, wenn es darum geht, Straftaten im Beschäftigungsverhältnis aufzudecken.

Freiwillige Einwilligung erforderlich

Sollte eine Datenverarbeitung über die vorstehend genannten Fälle hinausgehen, dürfen personenbezogene Daten verarbeitet werden, wenn die Beschäftigten freiwillig einwilligen. Um zu erkennen, ob eine Einwilligung freiwillig getroffen wurde, sind insbesondere die im Arbeitsverhältnis bestehende Abhängigkeit der beschäftigten Person zu berücksichtigen sowie die Umstände, unter denen die Einwilligung erteilt wurde. Von einer freiwilligen Einwilligung ist auf jeden Fall auszugehen, wenn der Betroffene einen Vorteil davon hat oder die Arbeitsvertragsparteien gleiche Interessen verfolgen. „Mitarbeiter sind in Textform über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht aufzuklären. Dies ist entsprechend zu dokumentieren“, sagt Gunnar Roloff, Rechtsanwalt bei Ecovis in Rostock.

Sensible Daten verarbeiten

Auch besondere Kategorien personenbezogener Daten dürfen verarbeitet werden, wenn sich die Einwilligung ausdrücklich auf diese Daten bezieht. Sensible Daten geben beispielsweise Auskunft über die ethnische Herkunft, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit. Ebenso dürfen auch genetische und biometrische Daten verarbeitet werden. Ohne eine Einwilligung ist die Verarbeitung von sensiblen personenbezogenen Daten zulässig, wenn

- die Daten für die Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des sozialen Schutzes erforderlich sind;
- eine Interessenabwägung vorgenommen wurde, ob die Wahrung von berechtigten Interessen der verantwortlichen Stellen oder eines Dritten die Grundrechte der betroffenen Person überwiegt.

So darf sich ein Arzt als Arbeitgeber beispielsweise danach erkundigen, ob eine Krankheit oder eine Beeinträchtigung des Gesundheitszustands vorliegt, durch den die Eignung für die vorgesehene Tätigkeit auf Dauer oder in periodisch wiederkehrenden Abständen eingeschränkt ist. Er darf auch nach ansteckenden Krankheiten fragen, die zwar nicht die Leistungsfähigkeit beeinträchtigen, jedoch die zukünftigen Kollegen oder Patienten gefährden könnten. „Zudem müssen Ärzte dokumentieren, dass sie geeignete Maßnahmen ergreifen, die sicherstellen, dass sie die Grundsätze der DSGVO einhalten“, sagt Roloff.

Neue Abmahnwelle rollt an

Mit der Einführung der DSGVO ist auch das Thema „Schadenersatzanspruch des Arbeitnehmers bei Verstößen gegen den Beschäftigtendatenschutz“ im Aufwind. Es ist damit zu rechnen, dass die Gerichte künftig weit höhere immaterielle Schadenersatzansprüche zusprechen, um eine effektive Umsetzung der DSGVO zu ermöglichen. „Wir erwarten ab Mitte des Jahres 2018 eine Abmahnwelle gegen Arbeitgeber. Zahlreiche Rechtsanwaltskanzleien werden für Arbeitnehmer Datenschutzverstöße im Beschäftigungsverhältnis aufspüren und diese abmahnen“, kommentiert Roloff. ●

Sie haben Fragen?

- Was sollte in einem Formular zur Einwilligung in die Datenverarbeitung stehen?
- Wie ist eine Maßnahmen-Dokumentation zu erstellen?

Rufen Sie uns an, Telefon 089 5898-266, oder schicken Sie uns eine E-Mail: redaktion-med@ecovis.com

Ecovis – Das Unternehmen im Profil

Das Beratungsunternehmen Ecovis unterstützt mittelständische Unternehmen. In Deutschland zählt es zu den Top 10 der Branche. Etwa 6.500 Mitarbeiterinnen und Mitarbeiter arbeiten in den mehr als 100 deutschen Büros sowie weltweit in Partnerkanzleien in über 70 Ländern. Ecovis betreut und berät Familienunternehmen, inhabergeführte Betriebe sowie Freiberufler und Privatpersonen. Ärzte, Gemeinschaftspraxen sowie Medizinische Versorgungszentren, Krankenhäuser, Pflegeheime und Apotheken sind unter den von Ecovis beratenen verschiedenen Branchen stark vertreten – über 2.000 Unternehmen aus dem Bereich Gesundheit/Medizin zählen zu den Mandanten von Ecovis. Um das wirtschaftliche Handeln seiner Mandanten nachhaltig zu sichern und zu fördern, bündelt Ecovis die nationale und internationale Fach- und Branchenexpertise aller Steuerberater, Wirtschaftsprüfer, Rechtsanwälte und Unternehmensberater. Jede Ecovis-Kanzlei kann auf diesen Wissenspool zurückgreifen. Darüber hinaus steht die Ecovis Akademie für fundierte Ausbildung sowie für kontinuierliche und aktuelle Weiterbildung. All dies gewährleistet, dass die Beraterinnen und Berater ihre Mandanten vor Ort persönlich gut beraten.

Herausgeber: ECOVIS AG Steuerberatungsgesellschaft, Ernst-Reuter-Platz 10, 10587 Berlin, Tel. Tel. +49 89 5898-266, Fax +49 89 5898-294
Konzeption und Realisation: Teresa Fach Kommunikationsberatung, 80798 München; DUOTONE Medienproduktion, 81241 München
Bildnachweise für die einzelnen Ausgaben: 2/2017, 3/2017, 4/2017, 1/2018, 2/2018, 3/2018 (in der Reihenfolge): iwat1929, istockphoto.com; Sinisa92, istockphoto.com; grasundsterne GmbH; Pro Symbols, thenounproject.com; grasundsterne GmbH; Photon Photo, shutterstock.com; Rawpixel, shutterstock.com.
Redaktionsbeirat: Tim Müller (Rechtsanwalt, Fachanwalt für Medizinrecht), Kathrin Witschel (Steuerberaterin), Annette Bettker (Steuerberaterin), Axel Keller (Rechtsanwalt), Gudrun Bergdolt (Unternehmenskommunikation), E-Mail: redaktion-med@ecovis.com