Datenschutz in der Medizin

Wichtige Datenschutzinformationen für Ihr Unternehmen

bits + bytes it-solutions

Inhalte | Datenschutzinformationen | März 2016

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Liebe Leserin, lieber Leser,

nur wenige Daten sind so sensibel wie unsere Gesundheitsdaten, daher sind sie auch besonders schützenswert. Schließlich kann der Missbrauch dieser Daten Betroffene in ihrer gesellschaftlichen Stellung oder ihren wirtschaftlichen Verhältnissen erheblich (bis hin zur Existenzgefährdung) beeinträchtigen.

Deshalb ist auch für den verantwortungsbewussten Unternehmer der Umgang mit den Gesundheitsdaten der Mitarbeiter enorm wichtig. Ebenso bzw. noch aufwendiger ist allerdings der Schutz dieser Daten vor Allem dort, wo sie primär verarbeitet werden: in Arztpraxen, Kliniken und Krankenhäusern, mobiler und stationärer Pflege, Krankenkassen, etc.

Hier kommen einige Regelungsbereiche auf die verantwortlichen Stellen zu: Bestellung eines Datenschutzbeauftragten, Auftragsdatenverarbeitung bei der Vernichtung von Patientendaten, Einwilligungen der Patienten zur Übermittlung an Verrechnungsstellen, Vorabkontrollen, technische und organisatorische Maßnahmen (z.B. Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, etc.), Aufbewahrungs- und Löschfristen; man könnte die Liste fast beliebig ergänzen.

Sie sehen also, beim Datenschutz in der Medizin gilt es viel zu berücksichtigen. Wir haben in dieser Ausgabe einige Aspekte für Sie zusammengestellt, die Ihnen einen geordneten Überblick verschaffen sollen.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung in Anspruch nehmen wollen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung. Sie erreichen uns unter der Telefonnummer + 49 (271) 338460 oder per E-Mail an wanja.spies@bits-bytes.de

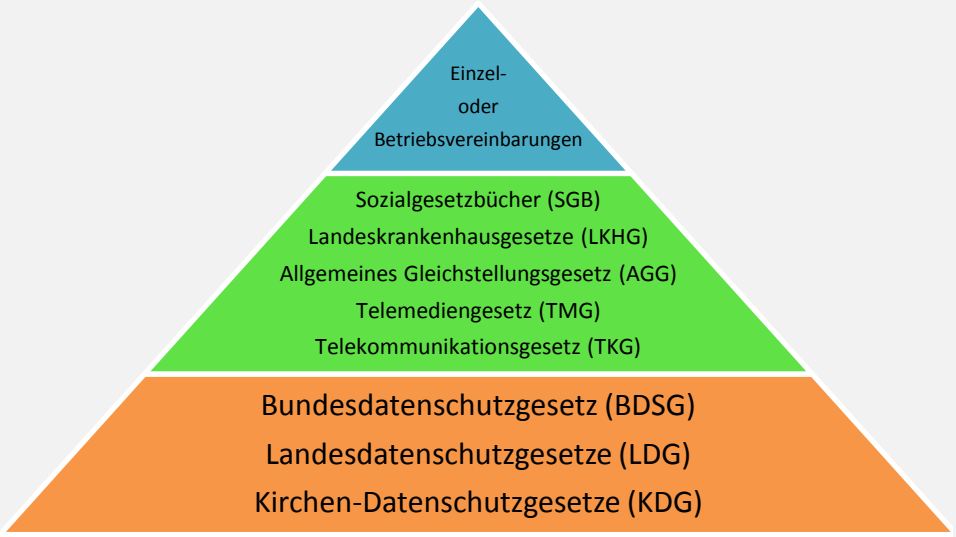
Mit besten Grüßen

Wanja André Spies
Interner / Externer Datenschutzbeauftragter (nach DIN EN ISO/IEC 17024)
Consultant für Datenschutz und Informationssicherheit

Datenschutz in der Medizin | Rechtliche Grundlagen

Grundlage ist zunächst immer das BDSG

Das Bundesdatenschutzgesetz stellt die Basis-Rechtsnorm für die Verarbeitung personenbezogener Daten dar. Dies gilt uneingeschränkt auch für medizinische Daten. Diese gelten gemäß § 3 Abs. 9 BDSG jedoch als „besondere Arten personenbezogener Daten“ und unterliegen somit einem erhöhten Schutzbedarf. Neben dem BDSG existieren jedoch noch zusätzliche Gesetze, Vorschriften und Regelungen, die dem BDSG vorrangig sind.



Aus den vorgenannten Gesetzen ergeben sich die Befugnisse oder Erfordernisse der Verarbeitung medizinischer Daten, wobei die höchste Legitimation immer die ausdrückliche und informierte Einwilligung des Patienten selbst darstellt.

Dabei unterscheiden wir zwischen drei Arten von Einwilligungen:

Ausdrückliche Einwilligung Der Betroffene erklärt seine Einwilligung, idealerweise in Schriftform.

Konkludent Einwilligung Die Einwilligung wird durch schlüssiges Verhalten erteilt. Der Wille des Betroffenen muss durch sein Verhalten erkennbar sein.

Mutmaßliche Einwilligung Wenn der Betroffene seine Einwilligung nicht selbst erteilen kann, wird unter Berücksichtigung persönlicher Umstände von seinem hypothetischen Willen ausgegangen.

Ärztliche Schweigepflicht vs. Datenschutz

Ärztliche Schweigepflicht und Datenschutz gelten gleichzeitig.

Die ärztliche Schweigepflicht basiert auf verschiedenen Rechtsgrundlagen:

§ 9 Musterberufsordnung (MBO)

Die Musterberufsordnung beschränkt sich auf in Deutschland tätige Ärzte und Ärztinnen.

§ 203 Strafgesetzbuch (StGB)

Das Strafgesetzbuch nennt den Täterkreis dabei abschließend. Neben Ärzten und Apothekern zählen auch Krankenschwestern, Arzthelferinnen etc. dazu. Sogar berufsnahe Gehilfen (Sekretärinnen, Sprechstundenhilfen etc.) werden durch den § 203 StGB explizit angesprochen.

Die Ärztliche Schweigepflicht allein reicht nicht aus.

Das Vorhandensein einer beruflichen Schweigepflicht entbindet den Arzt und Praxisinhaber nicht von der Pflicht, Datenschutzvorschriften zu beachten und diese in der Praxis auch umzusetzen.

So ist die Schweigepflicht allein natürlich keine ausreichende Grundlage, um Patientendaten zu erheben, zu verarbeiten und zu speichern. Zulässig ist die Verarbeitung nur dann, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder vorschreibt; oder der Betroffene selbst seine Einwilligung erteilt hat.

Auch reicht die Schweigepflicht alleine sicher nicht aus, um die sonstigen Anforderungen des BDSG zu erfüllen. Die zum Schutz von sensiblen Daten nötigen technischen und organisatorischen Maßnahmen (§ 9 BDSG) müssen auch in medizinischen Einrichtungen ohne Einschränkung umgesetzt werden.

„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

Selbstcheck | Technische & Organisatorische Maßnahmen

Machen Sie den Selbstcheck.

Technische und organisatorische Maßnahmen müssen nicht aufwendig und kompliziert sein; sie sollen angemessen sein. Patienten können bei einem Arztbesuch schnell feststellen, ob und welche organisatorischen Maßnahmen getroffen wurden.

Selbstverständlich kann auch jeder im Gesundheitsdienst Tätige diesen Selbstcheck durchführen:

Empfang (Diskretionszone)

- Ist sichergestellt, dass Patienten ihr Anliegen schildern können, ohne dass andere Wartende mithören können?
- Kann das Personal Telefonate führen, ohne dass wartende Patienten mithören können?
- Sind Patientenakten vor dem Zugriff Unbefugter geschützt? Oft liegen sie gestapelt auf der Theke an der Anmeldung bereit.

Wartebereich

- Ist der Wartebereich von Empfang und Behandlungsräumen akustisch getrennt?

Behandlungsbereich

- Sind Patientendaten in den Behandlungsräumen gegen unbefugte Kenntnisnahme geschützt? Dies betrifft sowohl Papierakten als auch EDV-Systeme.

EDV

- Wird das Patientengeheimnis beachtet, wenn der Support IT-Umgebung durch externe Dienstleister erfolgt?

Datenübermittlung

- Achten Sie darauf, dass Patienten vor der Übermittlung ihrer Daten an Dritte schriftlich eingewilligt haben. Dies ist z.B. notwendig, wenn privatärztliche Verrechnungsstellen beauftragt werden.

- Informieren Sie Patienten über mit- und nachbehandelnde Ärzte und stellen Sie sicher, dass keine Einwände gegen deren Einbeziehung bestehen.

Praxisverwaltung

- Sind abschließbare Aktenschränke vorhanden? Werden diese nach Dienstschluss verschlossen?
- Ist sichergestellt, dass das Reinigungspersonal keinen Zugang zu Patientendaten hat?

Technische Maßnahmen

EDV

- Ist der Zugang zu EDV-Geräten durch Passwörter geschützt?
- Entsprechen die Passwörter dem aktuellen Sicherheitsstandard (Empfehlungen des BSI / IT-Grundschutz)?
- Sind Systeme mit Patientendaten, die mit dem Internet verbunden sind, tatsächlich ausreichend geschützt („Firewall“)?
- Wird regelmäßig eine Datensicherung erstellt, um Daten vor Verlust oder Zerstörung zu schützen?
- Bietet Ihre Praxis-Software die Möglichkeit, Patientendaten verschlüsselt zu speichern?

Datenübermittlung

- Wird bei der Versendung von Patientendaten per Fax sichergestellt, dass ausschließlich berechtigte Dritte beim Empfänger Kenntnis von diesem Fax erhalten (z.B. durch Ankündigung beim Empfänger, regelmäßige Kontrolle von programmierten Nummern)?
- Achten Sie darauf, dass bei der Übermittlung von Patientendaten die Empfänger nicht mehr Informationen erhalten, als diese zur Erfüllung ihrer Spezifischen Aufgaben benötigen?

Datenschutzbeauftragter in der Arztpraxis

Müssen Ärzte einen Datenschutzbeauftragten (DSB) bestellen?

Wenn man Ärzte nach ihrer Einschätzung fragt, wird man häufig folgende Antwort bekommen: „Wir haben doch die berufliche **Schweigepflicht**." Mit diesem Argument glauben sie, allen Anforderungen begegnen zu können. Das ist jedoch nicht ganz so einfach.

Grundsätzlich gilt erst einmal § 4f Abs. 1 S.3 BDSG.

Dort heißt es: Sind mehr als 9 Mitarbeiter mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, so muss ein Datenschutzbeauftragter bestellt werden. Dies gilt uneingeschränkt für alle medizinischen Einrichtungen, ob Arztpraxis, Krankenhaus oder Pflegedienst.

In einer medizinischen Einrichtung kommen in der Regel alle Mitarbeiter/-innen mit personenbezogenen Daten in Berührung; Schreiben von Arztbriefen, Terminvergabe, Durchführung und Erfassung von Voruntersuchungen und vieles mehr. Es zählen dabei alle Personen, auch Teilzeitbeschäftigte und Praktikanten.

Patientendaten sind besonders **sensible Daten** (§ 3 Abs. 9 BDSG) und ihre elektronische Verarbeitung unterliegt daher grundsätzlich einer **Vorabkontrolle** (4d Abs. 5 BDSG). Dies wiederum bedeutet, dass immer ein Datenschutzbeauftragter bestellt werden muss, unabhängig der Anzahl der Mitarbeiter. Außer, der Betroffene willigt in die Verarbeitung seiner sensiblen Daten ein.

Und hier gehen die Meinungen nun zum Teil auseinander. Die Bundesärztekammer argumentiert, eine Vorabkontrolle sei nicht notwendig, da der Patient mit Abgabe seiner Patientenkarte bzw. Offenlegung seiner Daten seine Einwilligung zur Verarbeitung seiner personenbezogenen Daten erteilt. Folgt man dieser Haltung, besteht also keine Pflicht zur Bestellung eines Datenschutzbeauftragten, wenn weniger als 9 Personen sensible Daten verarbeiten.

Fazit

Es besteht keine generelle Pflicht zur Bestellung eines DSB. Aber alle Ärzte und Ärztinnen tragen die **Verantwortung** für die Wahrung des Datenschutzes und der Schweigepflicht und haben in der Regel keine Zeit, sich um die komplexen Organisationsabläufe im Datenschutz zu kümmern.

Alleine schon deshalb empfiehlt sich für medizinische Einrichtungen die Bestellung eines Datenschutzbeauftragten.

Archiv mit Krankenakten nicht ausreichend gesichert

Im ehemaligen Schwesternwohnheim der Asklepios Klinik in Bad Oldesloe wurden in einem Kellerraum bei einer Begehung durch den örtlichen Bauausschuss Hunderte alte Patientenakten, Karteikarten und Röntgenaufnahmen gefunden. Die Tür zu dem Archiv stand offen, die sensiblen Unterlagen befanden sich in Regalen, Säcken sowie Kartons und waren auf dem Boden verstreut.
Der Pressesprecher von Asklepios, Mathias Eberenz, versicherte *shz.de* zufolge, es sei kein Versäumnis des Krankenhauses, dass das Archiv offenstand, sondern Folge von Vermessungsarbeiten im Zuge des bevorstehenden Umbaus des Gebäudes.

Quellen: **shz.de vom 09.09.2015**

Gesundheitsdaten falsch kuvertiert

Eine Versicherung in Nordrhein-Westfalen hat Schreiben an die Kunden fehlkuvertiert (Juli 2015). So gingen Gesundheitsdaten an die falschen Empfänger. In diesem Fall waren 39 Personen betroffen.

Quellen: **Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen**

Datenschutzverstöße in der Medizin

Patientenunterlagen am Straßenrand gefunden

Bei der Entsorgung alter Patientenunterlagen der Klinik Weilheim ist etwas schiefgegangen: Von den 90 Säcken mit Röntgenbildern, die von einer Entsorgungsfirma abgeholt worden waren, fanden sich mindestens vier am Straßenrand in München-Neuperlach wieder. Auf den Bildern befanden sich die Namen und Geburtsdaten der Patienten. Ein Mitarbeiter der Entsorgungsfirma steht unter Verdacht, Teile der Fracht abgezweigt zu haben, um beim Recycling der Röntgenaufnahmen an Feinsilber und Silberverbindungen Geld zu kassieren.

Florian Diebel, stellvertretender Geschäftsführer der Krankenhaus GmbH, zu der die Weilheimer Klinik gehört, erklärte: "Wir stehen weiterhin im engen Kontakt mit der Polizei, um den Vorfall aufzuklären."

Quellen: **Süddeutsche.de vom 12.02.15**

Konfetti aus Patientenakten

Beim Faschingsumzug im thüringischen Dermbach kamen geschredderte Patientenakten als Konfetti zum Einsatz. Allerdings waren die Papierschnipsel nur grob zerkleinert worden, so dass personenbezogene Daten wie Namen, Adressen und Telefonnummern zu lesen waren.

Die Akten stammen offenbar aus einem zum Klinikum Bad Salzungen gehörenden medizinischen Versorgungszentrum. In einer Erklärung des Klinikums heißt es, eine Prüfung habe ergeben, "dass unter Missachtung der Vorschriften patientenbezogene Papiere nicht ordnungsgemäß entsorgt wurden".

Quellen: **Thüringer Allgemeine online vom 11.02.16**

Datenschutzverstöße in der Medizin

Patientendaten bei Einbruch in Arztpraxis entwendet

Beim Einbruch in eine nordrhein-westfälische Arztpraxis sind auch Patientendaten entwendet worden. Die Anzahl der Betroffenen ist nicht bekannt.
Der Diebstahl ereignete sich im November 2015.

Quellen: **Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen**

Patientenunterlagen im Hausmüll entsorgt

Ein Arzt hat der Kassenärztlichen Vereinigung Berlin mitgeteilt, dass sein Reinigungspersonal versehentlich Patientenunterlagen in den Hausmüll geworfen hat. Es handelte sich um Abrechnungen von Einsätzen im ärztlichen Bereitschaftsdienst.
Der Vorfall ereignete sich im Dezember 2014; die Anzahl der Betroffenen ist nicht bekannt.

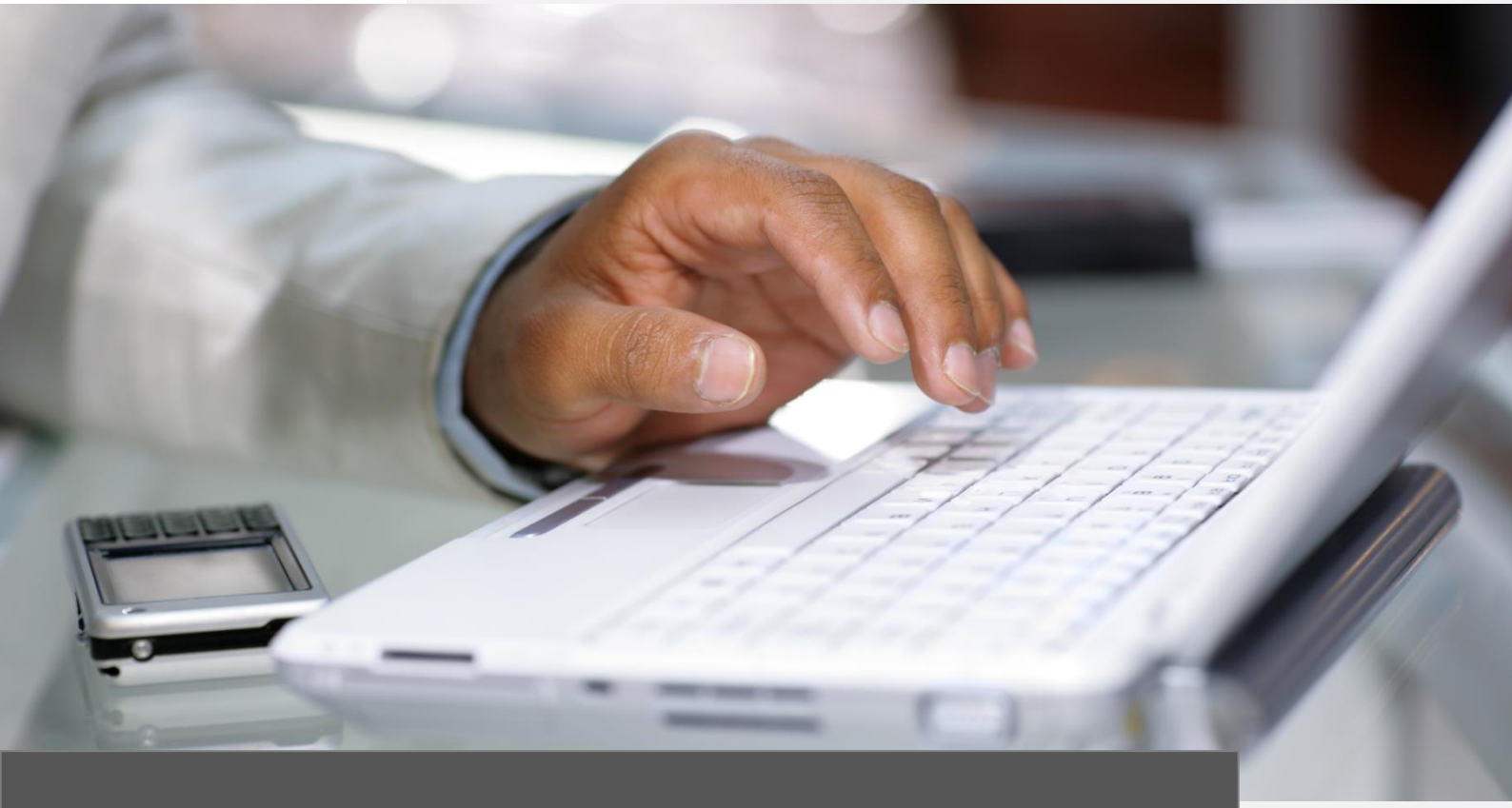
Quellen: **Berliner Beauftragte für Datenschutz und Informationsfreiheit**

Gesundheitsdaten öffentlich zugänglich

Ein nordrhein-westfälisches Industrieunternehmen hat Gesundheitsdaten von Mitarbeitern auf einem öffentlich zugänglichen Laufwerk gespeichert (Juli 2015). Dieser Fall betraf 5 Personen.

Quellen: **Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen**

März | 2016



Impressum

bits + bytes it-solutions GmbH & Co.KG
Bahnhof Weidenau 6
57076 Siegen
Tel.: +49 (271) 33846 - 0
Fax: +49 (271) 33846 - 15
Web: www.bits-bytes.de
E-Mail: info@bits-bytes.de

Amtsgericht Siegen, HRA 7243
Ust-IdNr.: DE126561391
Geschäftsführer: Stephan Schneider

Redaktion:
bits + bytes it-solutions GmbH & Co.KG

Bildnachweise:
Diese Datenschutzbroschüre wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei der Firma ccvision.de gekauft und lizensiert.