ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Ausgabe 01 2014

Datenschutz ein Störfaktor?

Warum er im Gesundheitswesen von besonderer Bedeutung ist.

Interview mit RA Olaf Methner
So ist die rechtliche Situation des Datenschutzes im Gesundheitswesen in Deutschland.

IDGARD
Der rechts- und datenschutzkonforme Kommunikationsdienst stellt sich vor.

Der Datenschutzbeauftragte
Ab wann ist ein DSB verpflichtend und welche Konsequenzen mit dem Verzicht verbunden sind.

Das Team

„Fachexpertise, Professionalität und Praxisnähe“, so lässt sich das ISDSG-Team beschreiben. Aufgrund unserer Kernkompetenzen in den Bereichen IT, Datenschutz und Sicherheit sowie jahrelanger Erfahrung im Gesundheitswesen können wir Ihnen ein breites Spektrum an Unterstützung anbieten, das sich genau an Ihren Bedürfnissen orientiert.

Simon Hacks B. Sc.
Die Betreuung unserer Kunden vor Ort sowie die Unterstützung bei der Umsetzung von operativen Maßnahmen sind das Steckenpferd des Projektmanagers.
✉ hacks@isdsg.de

Alexander Vogel B. Sc.
Mit dem Schwerpunkt der medizinischen Informatik fühlt er sich im Gesundheitswesen ganz zu Hause. Dies zeigt sich in der Konzeptarbeit im Rahmen seiner Beratungstätigkeiten.
✉ vogel@isdsg.de

Prof. Dr. Thomas Jäschke
Der Medizin-Wirtschaftsinformatiker ist Experte im Gesundheitssektor und Datenschutzbeauftragter für namhafte Einrichtungen im Gesundheitswesen. Als Institutsleiter ist er der Kopf des ISDSG-Teams.
✉ jaeschke@isdsg.de

Nina Richard B. A.
Sie verantwortet die Bereiche Marketing und Public Relations. Von der strategischen Planung bis hin zur operativen Umsetzung von Kommunikationsmaßnahmen ist sie Ihre Ansprechpartnerin.
✉ richard@isdsg.de

Angelica Morina
Als Verantwortliche für alle Aufgaben in Vertrieb und Kundenmanagement sowie der Steuerung firmeninterner Abläufe ist sie Ihre erste Ansprechpartnerin bei allen aufkommenden Fragen.
✉ morina@isdsg.de

Magnus Welz
Der Projektleiter begleitet Sie direkt vor Ort und koordiniert die umzusetzenden Maßnahmen. Zudem gehört die strategische Ebene der Projektarbeit zu seinen Schwerpunkten.
✉ welz@isdsg.de

Inhalt

Datenschutz ist ein wichtiges Thema insbesondere in der digitalen medizinischen Welt.

Unverzichtbar: der Datenschutzbeauftragte

ISDSG im Interview mit Rechtsanwalt Olaf Methner

Das Team 2

Tipps, Fakten & Termine 4

Schwerpunkt

Störfaktor Datenschutz 6
Patienten dürfen nicht zu gläsernen Menschen werden

Gastbeitrag

Wie Ärzte zeitgemäß und rechtskonform kommunizieren 10
Ist es in der medizinischen Branche überhaupt möglich, rechtskonform zu kommunizieren?

Voice

Interview mit Rechtsanwalt Olaf Methner 12
Über die aktuelle Situation des Datenschutzes

Der Datenschutzbeauftragte

Achtung bei der Bestellung des Datenschutzbeauftragten 14
Was unbedingt beachtet werden sollte

Goldene Regeln

1. Goldene Regel: Betroffenenrechte 15
Betroffenenrechte im Alltag

EDITORIAL

Sehr geehrte Leserinnen und Leser,

ich freue mich, Ihnen heute die erste Ausgabe unseres Magazins „ExperSite“ vorzustellen: das Magazin für Kunden und Interessenten zum Thema Datenschutz und IT-Sicherheit im Gesundheitswesen. Die Einführung unseres Magazins ist darauf zurückzuführen, dass wir einen Informationsbedarf festgestellt haben, den wir praxisnah und leicht integrierbar decken möchten. Wir möchten weg von der reinen Wiedergabe von Gesetzestexten hin zu einer selbstverständlichen Integration in den Krankenhausalltag. Denn das Tagesgeschäft zeigt, dass eine Umsetzung von Datenschutzgesetzen und Verordnungen nicht immer mit schnellen und lückenlosen medizinischen Behandlungsprozessen Hand in Hand geht.

Unsere erste Ausgabe wird Sie daher an das Thema Datenschutz heranführen und die geschichtliche Entstehung bis zu den heutigen Standards darstellen – nicht fehlen dürfen hier natürlich praktische Tipps zur direkten Umsetzung. Die Rubrik „Der Datenschutzbeauftragte“ informiert Sie über alle Kompetenzen, die der Datenschutzbeauftragte eines Krankenhauses mit sich bringen muss. Im Bereich „Goldene Regeln“ erfahren Sie das Wichtigste über Betroffenenrechte im Alltag.

Der Fachanwalt für Beschäftigungsdatenschutz, Olaf Methner, klärt über rechtliche Risiken von Geschäftsführern auf und unser Kooperationspartner IDGARD stellt die sichere Kommunikation seines Cloud-Dienstes vor.

Sollten Sie besondere Themenwünsche haben, freuen wir uns, wenn Sie uns diese, genau wie Feedback und Anregungen, übermitteln.

Ich wünsche viel Spaß bei der Lektüre
Ihr

Prof. Dr. Thomas Jäschke
Institutsleiter ISDSG

Europäischer Datenschutz

Die Mitgliedstaaten der Europäischen Union haben bei der Umsetzung europäischer Vorgaben in nationales Recht einen gewissen Spielraum. Genau dieser führt allerdings dazu, dass starke Abweichungen innerhalb der Datenschutzpraxis auftreten. Die geplante, europaweit geltende Datenschutz-Grundverordnung soll eine umfassende Regelung schaffen und gleichzeitig den heutigen technischen Standards entsprechen. Dabei wird es sich bei der Datenschutz-Grundverordnung um das erste europäische Gesetz handeln. Deutschland können große Änderungen für den Datenschutz bevorstehen. Bis 2015/2016 soll die Verordnung verabschiedet sein, deren Einführung solche Gesetze wie das BDSG und die zugehörige Rechtsprechung ersetzen wird.

Großbritannien

Das Gesetz „Data Retention and Investigatory Powers Act ", kurz DRIP, der britischen Regierung ist im Eilverfahren verabschiedet worden, um die außer Kraft gesetzten EU-Richtlinien zum Thema Vorratsdatenspeicherung umzusetzen. Völlig neuartig wäre hier weltweit, dass das DRIP vorsieht, auch ausländische „Unternehmen und Personen (…) einem Bewachungsbefehl zu unterwerfen, weshalb auch im Ausland Kommunikationsdaten erhoben, vorgehalten und auf Anfrage herausgegeben werden müssten".

USA

In den USA existieren weder eine Datenschutzaufsicht, die den Datenschutz überwacht, noch gesetzliche Grundlagen zum Schutz personenbezogener Daten. Genau deshalb kann die Inanspruchnahme von US-amerikanischen IT-Anbietern (wie Serverstandorte, Cloud-Dienste, Collaboration Tools oder Social Media) zu einem großen Risiko für Unternehmensdaten und personenbezogene Daten, wie beispielsweise Patientendaten, werden. Auch andere IT-Standorte, z. B. von Tochterfirmen, sind kritisch zu betrachten, da beispielsweise das „Fünf-Augen-Abkommen" zwischen den USA, Kanada, Großbritannien, Neuseeland und Australien den Zugriff auf EU-Daten ermöglicht.

Tipps, Fakten & Termine

TIPP

Organisatorischer Datenschutz
Oft sind es bereits kleine organisatorische Maßnahmen, die den Datenschutz verbessern können:

- Sensibilisierung der Mitarbeiter
- Verschließen von Aktenschränken
- Prüfung der Patientenidentität
- Sperren der Arbeitsplätze und Behandlungsmonitore
- Vertrauliche Gespräche außer Hörweite unbeteiligter Dritter führen
- Akten nicht offen einsehbar lassen

TIPP

Social Media
Social Media wie Facebook und Co. sind nicht nur wichtige Bestandteile des Marketing-Mixes. Auch aus der Datenschutzperspektive sind sie ein Thema, das Beachtung finden muss. Mitarbeiter sind für den Umgang mit Social Media zu sensibilisieren, denn Bilder, Namen oder auch Informationen, die aufgrund ihrer Spezifikation Rückschlüsse auf Patienten oder deren Behandlungsverlauf geben – auch wenn diese mit guter Absicht veröffentlicht werden – rufen einen Verstoß gegen das Datenschutzgesetz hervor. Klinikinterna sollten auch nicht in „geschlossenen" Gruppen ausgetauscht werden. Social-Media-Richtlinien und -Schulungen können hier unterstützen.

TERMINE

Datenschutztag 2014
23.09.2014
Köln

IDACON 2014
14. WEKA-Kongress für Datenschutzbeauftragte
07.– 09.10.2014
Würzburg

Medica 2014
World Forum for Medicine – International Trade Fair with Congress
12.–15.11.2014
Düsseldorf

6. BVDST-Herbstsymposium
28.– 29.11.2014
Berlin

Gesundheitsforum Leipzig
02.– 03.12.2014
Leipzig

DuD 2015
Datenschutz und Datensicherheit
15.–16.06.2015
Berlin

Mehr Veranstaltungshinweise unter:
www.isdsg.de/informationen/veranstaltungen

Störfaktor Datenschutz

Datenschutz als Recht zur informationellen Selbstbestimmung gilt im Behandlungsalltag häufig als prozessstörend. Warum der Datenschutz aber alles andere als ein Störfaktor für Unternehmensprozesse ist und sich damit sogar Kosten einsparen lassen.

Durch die sich immer weiter entwickelnden technischen Möglichkeiten und die stärkere Vernetzung unserer heutigen Zeit bekommt der Datenschutz einen besonderen Stellenwert. Vor allem Patienten müssen davor geschützt werden, zu gläsernen Menschen zu werden.

Das Thema „Datenschutz im Gesundheitswesen" kann bis in die Zeit 460 bis 370 v. Chr. zurückverfolgt werden. Der „Eid des Hippokrates" formulierte zum ersten Mal die ärztliche Verschwiegenheit im Rahmen der medizinischen Behandlung. Auf gesetzlicher Ebene finden sich die Grundlagen des Datenschutzes im Jahr 1871 mit der Einführung der beruflichen Schweigepflicht nach § 300 StGB des Norddeutschen Bundes. Eine Weiterentwicklung der Gesetzeslage resultierte aus einer amerikanischen Debatte um den Datenschutz der US-Regierung um John F. Kennedy Anfang der 1960er-Jahre, der ein nationales Datenzentrum einrichten wollte, um das Informationswesen zu verbessern. Diese Debatte weitete sich aus und führte dazu, dass Hessen das erste Datenschutzgesetz weltweit im Jahr 1970 verabschiedete.

Das Bundesdatenschutzgesetz (BDSG) folgte 1977 mit den Schwerpunkten bei der Einführung einer Aufsichtsbehörde und der Vorrangstellung des Schutzes personenbezogener Daten. Im Zusammenhang mit dem Volkszählungsurteil 1983 wurde der Begriff der „informationellen Selbstbestimmung" geprägt, welche besagt, dass die Preisgabe und Verwendung persönlicher Daten dem jeweils Einzelnen obliegen. Die letzte Überarbeitung stammt vom 3. Juli 2009.

> *Häufig bleibt das Gefühl, dass es vielen Personen gleichgültig ist, was mit ihren Daten geschieht.*

Dies führt uns in das heutige Zeitalter, in dem der Datenschutz zunehmend ein Thema der Öffentlichkeit geworden ist. Aufgrund der zunehmenden Digitalisierung schwindet auch die Selbstbestimmung immer mehr. Häufig bleibt das Gefühl, dass es vielen Personen gleichgültig ist, was mit ihren Daten geschieht und deshalb unbedacht persönliche Daten weitergegeben werden. Studien belegen allerdings, dass es andere Faktoren sind, die zu einem vermeintlich unbedachten Umgang mit persönlichen Daten führen. Zum einen ist häufig nicht bewusst, welche Konsequenzen die Sammlung persönlicher Daten haben kann. Zum anderen ist der Großteil von technischen Schutzmaßnahmen häufig so komplex, dass deren Umsetzung ein hohes technisches Know-how voraussetzt.

Ab einem bestimmten Punkt kann die Weitergabe persönlicher Daten für alle Beteiligten spürbar unangenehm werden. Gesundheitsdaten verraten viel über den Einzelnen, was spätestens dann bewusst wird, wenn nach einem Krankenhausaufenthalt fremde Befunde ausgehändigt werden, diese bei dem Postversand bei der falschen Person ankommen oder sensible Gesundheitsdaten nicht anonymisiert veröffentlicht werden, wie zuletzt bei der Barmer Krankenkasse geschehen.

Durch solche Vorfälle wird die Bedeutung der rechtlichen Regelungen wieder deutlich. Für Krankenhäuser in öffentlicher und privater Trägerschaft gelten das BDSG sowie das SGB. Krankenhäuser in kirchlicher Trägerschaft haben eine eigene Gesetzesgrundlage.

Für viele ist das Thema Datenschutz noch immer ein Bereich, der im Widerspruch zu den eigentlichen Unternehmenszielen steht. Anstatt als Unterstützung wird der Datenschutz eher als prozessbehindernd gesehen. Zudem fallen zunehmend Kosten an. So werden beispielsweise Datenschutzbeauftragte berufen, die nicht die gesetzlichen Anforderungen erfüllen, aber kostengünstig sind. Problematisch wird es, wenn es tatsächlich zu einem Zwischenfall kommt und sensible Daten unbefugten Dritten verfügbar gemacht werden.

Auf den ersten Blick verursacht Datenschutz also Kosten, weil zeitliche, monetäre und personelle Ressourcen zur Verfügung gestellt werden müssen.

Der zweite Blick zeigt aber, dass letztendlich Kosteneinsparungen durch die Datensparsamkeit, also die Verringerung der Datenmenge, sowie systematische und effizientere EDV-Systeme erzielt werden. Wobei hier immer eine Abwägung zwischen den eingesparten Kosten und dem zu erbringenden Aufwand zu treffen ist.

Besonders im Gesundheitswesen ist das Konfliktpotenzial sehr groß. Auf der einen Seite bedarf es einer möglichst barrierefreien Kommunikation und des Austauschs von Daten zwischen Krankenhäusern, Zuweisern und Krankenkassen, um eine bestmögliche medizinische Versorgung von Patienten zu ermöglichen. Auf der anderen Seite steht der Datenschutz, der für die Ärzte und anderen Verantwortlichen im Krankenhaus häufig als Hemmschuh gesehen wird. Doch ist es nicht vielleicht sogar möglich, eine erstklassige Versorgung unter Berücksichtigung der datenschutzrechtlichen Aspekte, explizit der informationellen Selbstbestimmung der Patienten, durchzuführen? >

> *Bereits kleine Änderungen der Prozesse können zu einer erheblichen Verbesserung des Datenschutzniveaus führen.*

Bereits kleine Änderungen der Prozesse können zu einer erheblichen Verbesserung des Datenschutzniveaus führen.

Diskretion

Während der Aufnahme innerhalb eines Krankenhauses geht es vor allem um schnelles Handeln, um das Patientenwohl gewährleisten zu können. Für die Best-Practise bedeutet dies, dass Patientennamen bei der Anmeldung nicht laut genannt werden sollten. Alternativ lässt sich die Versichertenkarte übergeben, um die Privatsphäre zu wahren. Auch die Patientenakten sollten nicht einsehbar auf dem Anmeldetresen liegen.

Um die schnelle und einfache Verfügbarkeit der Patientendaten zu gewährleisten, müssen diese allerdings griffbereit für die behandelnden Ärzte sein. Dies kann erreicht werden, indem Patientenakten verdeckt werden, um so die vertraulichen Daten der Patienten zu schützen. Bestenfalls sollte gewährleistet werden, dass diese nie unbeaufsichtigt sind oder von anderen Patienten eingesehen werden können.

Auch wenn es im Krankenhausalltag schwierig ist, sich komplett zurückzuziehen, sollten vertrauliche Gespräche über Patienten nicht dort stattfinden, wo sie von unbeteiligten Dritten mitgehört werden können, wie auf dem Flur. Eine Alternative stellt beispielsweise der Aufenthaltsraum des Pflegepersonals dar.

Das Stationszimmer

Das Stationszimmer des Pflegepersonals sollte nicht unbeaufsichtigt sein. Da dies in der Regel nicht umsetzbar ist, ist hier darauf zu achten, dass Aktenschränke stets verschlossen sind, Hardware gesichert oder weggeschlossen ist und PCs durch Passwörter geschützt sind. Besonders wichtig ist, dass es sich bei den Accounts des Pflegepersonals für die Dokumentation etc. nicht um Sammelaccounts handelt, sondern jeder Mitarbeiter seinen eigenen Benutzer hat. Sammelaccounts sind auf den ersten Blick sehr praktisch, da Ein-, Aus- und erneutes Einloggen nicht erforderlich sind. Eine Ausnahme für solche Sammelaccounts wird häufig z. B. im OP oder in der Notaufnahme gesehen, wo zum einen strikte Zugangsbeschränkungen gelten und zum anderen die Zeit einen extrem kritischen Faktor darstellt. Allerdings bieten Sammelaccounts darüber hinaus auch potenzielle Angriffsstellen, da ein unbeaufsichtigter PC dazu führen kann, dass sich Patienten oder jede beliebige andere Person Zugriff zu vertraulichen Patientendaten verschaffen kann, ohne dass eine sinnvolle und nachvollziehbare Protokollierung stattfindet. Der Schweregrad von nicht vorhandenen Zugriffsbeschränkungen

> *Sammelaccounts stellen einen kritischen Faktor dar.*

wird dann deutlich, wenn z. B. an der Pforte bereits die komplette Patientenakte eingesehen werden kann und nicht nur, wie es eigentlich ausreichend wäre, die eingeschränkten Stammdaten, wie Vor- und Nachname, das Geburtsdatum und die Zimmernummer des Patienten.

Auftragsdatenverarbeitung

Unter die Auftragsdatenverarbeitung fallen jegliche ausgelagerte Arbeiten, wie die Beauftragung externer Abrechnungsgesellschaften, Wartungsfirmen oder die Auslagerung medizinischer Dienstleistungen, wie beispielsweise Labore, bei denen der Auftragnehmer im Rahmen der Anweisungen des Auftraggebers die personenbezogenen Daten verarbeitet. Durch die Beauftragung externer Personen kommt es zu einer Offenbarung von Patientendaten, welche nach § 203 StGB nicht zulässig ist. Unproblematisch ist die Auftragsdatenverarbeitung, wenn eine Einwilligung des Patienten vorliegt oder die Daten anonymisiert oder pseudonymisiert verarbeitet werden. Andernfalls macht der Arzt sich, auch bei einer bestehenden Auftragsdatenverarbeitung, strafbar.

Versenden von Unterlagen

Um eine nahtlose Kommunikation mit Zuweisern und Laboren zu ermöglichen, ist es notwendig, moderne Kommunikationsmittel zu nutzen.

Das Faxgerät

Faxgeräte sind für die Übermittlung von vertraulichen Daten nicht geeignet, da es sich hierbei um einen offenen Kommunikationskanal handelt. Trotzdem werden diese regelmäßig genutzt. Wenn auf die Nutzung eines Faxgerätes nicht verzichtet werden kann, sollte zumindest die manuelle Nummerneingabe vermieden

Die Patientenakten sollten nicht offen einsehbar sein.

> *Die Kommunikation per E-Mail ist mit einer Postkarte vergleichbar, die von jedem gelesen werden kann, bei dem sie vorbeikommt.*

werden, da hier die Praxis zeigt, dass es häufig zu Tippfehlern kommt und so Dokumente den falschen Empfänger erreichen. Deshalb sollte der Nummernspeicher genutzt werden. Des Weiteren sollte der Empfänger vorher telefonisch kontaktiert werden, sodass die Korrektheit der Nummer sichergestellt werden kann und der Empfänger nach Erhalt des Faxes, selbiges sofort aus dem Druckerschacht entfernen kann.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) empfiehlt außerdem, den eigentlichen Daten ein Deckblatt vorauszuschicken, das den Empfänger und den Absender klassifiziert und darauf hinweist, dass bei einem abweichenden Empfänger der Empfang des Faxes sofort abzubrechen und der Absender zu informieren ist.

E-Mail

Die Kommunikation per E-Mail ist mit einer Postkarte vergleichbar, die von jedem gelesen werden kann, bei dem sie vorbeikommt. Um die Sicherheit von E-Mails zu erhöhen, bedarf es einem größeren technischen Verständnis. Die bisher vorherrschenden Lösungen sind nicht wirklich praxistauglich. Aber auch hier wird zunehmend an verbraucherfreundlichen Lösungen gearbeitet. In Zusammenarbeit zwischen der Uniscon GmbH und dem Bundesministerium für Wirtschaft ist hier beispielsweise ein Web-Service entstanden, der den sicheren Austausch von Dokumenten als Ergänzung zum E-Mail-Versand ermöglicht (mehr dazu auf Seite 10).

Das Aushändigen von Unterlagen

Das Aushändigen von Untersuchungsbefunden direkt an den Patienten ist die einfachste Möglichkeit, Unterlagen sicher zu übermitteln. Wichtig ist, sich zu vergewissern, dass es sich tatsächlich um den Patienten selbst handelt oder der Patient eine Einverständniserklärung abgegeben hat, dass die Unterlagen einem Dritten, z. B. Familienangehörigen, ausgehändigt werden dürfen. ■

Nina Richard

Über ISDSG

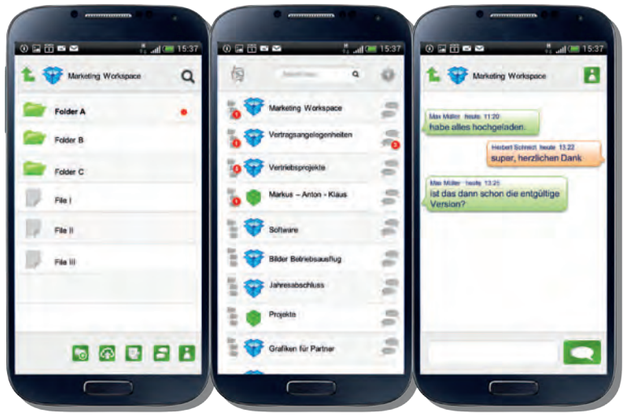
Das ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen in Dortmund beschäftigt sich mit allen Fragen zum Thema Informationssicherheit und Datenschutz mit Schwerpunkt auf den Akteuren des Gesundheitswesens. Das Institut wurde vom Medizin-Wirtschaftsinformatiker Prof. Dr. rer. medic. Thomas Jäschke gegründet. Das Portfolio des ISDSG umfasst neben den frei zugänglichen Informationen und Dienstleistungen auch besonders für Praxen und Unternehmen ausgerichtete Angebote. Die fortschreitende Digitalisierung in der Medizin aufgrund der Potenziale der neuen Informationstechnologien ist der Motor des spezialisierten Teams.

Institutsadresse:
ISDSG –
Institut für Sicherheit und Datenschutz im Gesundheitswesen
Prof. Dr. Thomas Jäschke
Westfalendamm 251
44141 Dortmund

Fon +49 231 4499599-91
Fax +49 231 4499599-99
M@il kontakt@isdsg.de
www www.isdsg.de

Wie Ärzte zeitgemäß und rechtskonform kommunizieren

Die Schweigepflicht zwingt zu einem vorsichtigen Umgang mit modernen Kommunikationsformen. Ärzte können diese aber benutzen, wenn sie rechtliche Vorgaben beachten.



Über den Kommunikationsdienst IDGARD können Daten und auch Nachrichten betreibersicher und für Dritte uneinsehbar untereinander versendet werden.

Patientin Husch* (38) sitzt vor der Neurochirurgin zur Vorbesprechung ihrer Operation. Ihre Befunde hat sie mitgebracht, es sind so einige. Bis zum tatsächlichen Operationstermin wird es noch zwei Wochen dauern. Die Ärztin möchte Husch jedoch eine Möglichkeit geben, in der Zwischenzeit Kontakt mit ihr aufzunehmen: Besonders dann, wenn plötzlich Fragen auftauchen, wäre es gut, eine E-Mail schicken zu können, um eventuelle Ängste in den Griff zu bekommen. Gleichzeitig hat sie aber gehört, dass die Kommunikation per E-Mail nicht sicher sein soll und so im Zweifelsfall unbefugte Dritte intime Behandlungsdetails erfahren könnten.

Auch die gesetzliche Schweigepflicht erlaubt es der Chirurgin nicht, der Patientin personenbezogene Details per E-Mail zukommen zu lassen, es sei denn, die Patientin erklärt sich damit – nach Aufklärung der Risiken – einverstanden. Außerdem braucht das Ärzteteam in der Klinik noch weitere Unterlagen vom Hausarzt und Befunde externer Kollegen. Dass die Ärzte Befunde einfach per E-Mail weiterleiten, erscheint zwar zeitgemäß, wäre zeitlich effizient und für die Vorbereitung des Eingriffs nützlich, ist aber gemäß § 203 StGB und § 16 in Verbindung mit § 9 BDSG nicht zulässig.

Krankenhauskommunikation aktuell

Dies beruht auf der Tatsache, dass die verschiedenen Online-Kommunikationsformen wie E-Mails, File-Sharing oder Messaging, die Ärzte, Krankenhäuser und Patienten miteinander vernetzen könnten, den jeweiligen Betreibern (Provider) der Anwendung im Internet ermöglichen, auf die übermittelten Patientendaten zuzugreifen. Daher ist der Gebrauch von E-Mail & Co. im Gesundheitswesen rechtlich bisher nicht geeignet: Zuweiser, Krankenhäuser und alle anderen Institutionen im Gesundheitswesen müssen die normativen Rahmenbedingungen beachten, wie z. B. Datenschutz- und Strafgesetze. „Wenn es dem Provider grundsätzlich möglich ist, im Rahmen seiner Leistungserbringung auf personenbezogene Gesundheitsdaten zuzugreifen, müssen zumindest die Voraussetzungen für eine Datenverarbeitung im Auftrag gemäß § 11 BDSG erfüllt sein.“ [1] Zu beachten ist, dass neben der Auftragsdatenverarbeitung weiterhin das Offenbarungsverbot gilt. Um dem absoluten Offenbarungsverbot des Strafgesetzbuches zu genügen, darf der Provider

> *Ist es im Gesundheitswesen überhaupt möglich, im Internet rechtskonform zu kommunizieren?*

keine technische Möglichkeit zur Kenntnisnahme der Daten haben. Gleichzeitig bleibt der Servicenutzer in der Verantwortung, die Vertraulichkeit und Integrität der Daten zu gewährleisten.

Da die Schweigepflicht ein so wichtiger Aspekt bei der Verarbeitung von Gesundheitsdaten ist, würde Patientin Husch einen E-Mail-Verkehr auf keinen Fall akzeptieren, da „Provider die Daten mitlesen können und außerdem die Verbindungsdaten (Metadaten) nicht geschützt sind“. Informationen zu einigen E-Mails würden Menschen mit passenden Analysetools genügen, um herauszufinden, dass sie in neurochirurgischer Behandlung ist. Bei ihrem Beruf könne sie sich „gar nicht leisten, dass das publik wird“, sagt sie.

Verschlüsselter Kommunikationsdienst

Für die Ärzte aber stellt sich die generelle Frage: Ist es im Gesundheitswesen überhaupt möglich, im Internet rechtskonform zu kommunizieren? Steffen Kroschwald, wissenschaftlicher Mitarbeiter bei der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel, sieht eine Möglichkeit: „Durch eine sichere kryptografische Verschlüsselung können personenbezogene Daten pseudonymisiert werden.“ Voraussetzung hierfür sei aber, dass eine „entsprechende zukunftsgerichtete Risikoprognose ein Hacking der Verschlüsselung hinreichend ausschließt, unbemerkte Datenkopien verhindert werden und der Schlüssel sicher und ausschließlich beim Cloud-Nutzer verbleibt“. Außerdem darf nicht erkennbar sein, welcher Arzt mit welchem Patient kommuniziert, da auch diese Metadaten als Geheimnis gelten und durch das Offenbarungsverbot des Strafgesetzbuches geschützt sind.

Kommunikationslösung

Auf diese Weise könnten die Ärzte z. B. über einen Datenraum des Cloud-Dienstes IDGARD die medizinischen Daten der Patientin Husch allen beteiligten Parteien zur Verfügung stellen. Dies würde die einrichtungsinterne wie -externe Kommunikation zwischen behandelnden Ärzten, einzelnen Fachabteilungen und dem medizinischen Fachpersonal erheblich erleichtern: Sie können jederzeit auf die Unterlagen zugreifen, sogar neue hochladen oder aber auch nur Einsicht in vorhandene Dokumente nehmen, je nachdem, wie sie den Zugang zum Datenraum einrichten. Dadurch bleibt dieser aktuell wie eine Krankenakte, sogar gemeinsam mit den Befunden externer Ärzte. Husch kann außerdem mit der Neurochirurgin chatten, die bei jedem neuen Dokument oder jeder neuen Nachricht informiert wird.

Möglich ist das, weil der Kommunikationsdienst IDGARD auf der in Europa und den USA bereits patentierten Sealed-Cloud-Technologie basiert. Mit ihr sind die Daten nicht nur vor den Blicken Außenstehender geschützt, sondern auch vor den Blicken des Betreibers selbst. Kroschwald: „Sollen Daten im Rahmen des Cloud Computing verarbeitet werden, so kann dies innerhalb der Basistechnologie Sealed Cloud ‚betreibersicher‘ erfolgen." Bei IDGARD hat also niemand Einblick in die Daten eines Anwenders, der nicht explizit die Erlaubnis vom Anwender erhalten hat. Damit Außenstehende wie auch eigene Mitarbeiter des Sealed-Cloud-Providers Uniscon keine unverschlüsselten Daten einsehen können, hat das Münchner Unternehmen weitreichende technische Maßnahmen entwickelt, die über die üblichen organisatorischen Regelungen und technischen

Mit IDGARD sind alle Kommunikationsbeziehungen geschützt.

Maßnahmen von anderen deutschen Cloud-Betreibern weit hinausgehen. Mit IDGARD sind sogar die Kommunikationsbeziehungen (wer mit wem wie lange verbunden ist) – mittlerweile als Metadaten bekannt – geschützt. Daher gilt der Dienst als „auch für Berufsgeheimnisträger einsetzbar“, wie das Institut für Wirtschaftsrecht der Universität Kassel festgestellt hat.

Zur Implementierung in die Vernetzungskommunikation zwischen den Beteiligten ist die Anschaffung neuer Technik nicht erforderlich. Man kann so einen Datenraum sofort und ohne großen Finanz- oder Verwaltungsaufwand nutzen. Die Anwender greifen über die Website www.idgard.de oder eine der Apps für Smartphones und Tablets auf das speziell abgesicherte Datenzentrum – die Sealed Cloud – zu und richten diesen dann ein. Dazu sind keinerlei technische Kenntnisse nötig. Der Dienst ist laut Dr. Ralf Rieken, Geschäftsführer der Firma Uniscon, „mit Fokus auf einfache Bedienung konzipiert, weil Sicherheit erfahrungsgemäß nur dann erfolgreich umgesetzt und akzeptiert wird, wenn die Lösungen leicht und komfortabel nutzbar sind“. ■

> *Bei IDGARD hat niemand Einblick in die Daten eines Anwenders, der nicht explizit die Erlaubnis vom Anwender erhalten hat.*

*Name von der Redaktion geändert

Dr. Hubert Jäger

Dr. Hubert Jäger hat an der Universität Stuttgart und an der ETH Zürich studiert. Er war in leitenden Funktionen der Produktentwicklung, des Innovations- und Produktmanagements sowie des Vertriebs bei großen Hightech-Unternehmen tätig. Er ist Erfinder und Autor zahlreicher Patente.

[1] Prof. Dr. Thomas Jäschke: Datenschutz in der Cloud. Auf den richtigen Partner kommt es an. In: iSOFT Magazin, Januar 2012

Wie kommunizieren medizinische Teams effizient und sicher im Internet?

E-Mail

Zunächst müssten Ärzte für alle Beteiligten die E-Mail-Verschlüsselung klären, wenn sie die Datenschutzgesetze und auch die ärztliche Schweigepflicht im Internet ernst nehmen. Probleme: Patientenakten, Röntgenbilder und Ähnliches sind oft zu groß für E-Mail-Anhänge. Außerdem sind die Metadaten nicht geschützt. Ein gemeinsamer Speicherplatz für Behandlungsteams fehlt.

Bestehendes Informationssystem eines Klinikums

Diese Alternative sichert die Daten wirkungsvoll ab, solange sie im Haus bleiben. Deshalb ist es in Krankenhäusern das gängigste System. Es hat sich allerdings als schwierig erwiesen, externen Nutzern einen Zugriff auf interne Systeme zu gewähren oder die Systeme verschiedener Kliniken und Ärzte miteinander zu verbinden.

Öffentliche Dienste für einen gemeinsamen Dokumentenspeicher (File-Sharing)

Diese Dienste bieten einen einfachen und bequemen Zugang zu Dokumenten und sind einfach zu nutzen. Die Sicherheitsanforderungen für die Behandlung medizinischer Daten, die der Berufsgeheimnispflicht unterliegen, erfüllen sie nicht. Denn im Gesundheitswesen dürfen die Daten und Dokumente der Patienten nicht auf Systemen gespeichert werden, wenn der Betreiber eines Dienstes (Serviceprovider) prinzipiell auf die Dokumente zugreifen könnte.

Datenraumdienste

Diese Dienste sind bekannt als Dokumentenspeicher für vertrauliche Vertragsverhandlungen und ähnliche Anwendungsfälle. Sie bieten ein hohes Maß an Sicherheit und man könnte sie im Gesundheitswesen vielfach einsetzen. Sie sind jedoch oft sehr teuer und erfordern zumeist einen erhöhten Verwaltungsaufwand.

IDGARD-Dienst

Der Kommunikationsdienst lässt sich im Gesundheitswesen umfassend einsetzen – bei vergleichsweise geringen Kosten, einfacher Nutzung und Verwaltung. Er schließt durch die ihm zugrunde liegende Sealed Cloud Technologie den Zugriff des Anbieters (Serviceproviders) auf die Daten seiner Anwender aus. Damit kontrolliert nur der Eigentümer der Daten vollständig den Zugriff auf seine Daten.

www.idgard.de

Kanzlei Baum Reiter & Collegen

Die Kanzlei Baum Reiter & Collegen mit dem ehemaligen Bundesinnenminister Gerhart Baum hat ihre Tätigkeitsschwerpunkte u. a. in den Bereichen des Datenschutzrechts, der Datensicherheit und der Compliance. Sie führte vor dem Bundesverfassungsgericht mehrere erfolgreiche Verfassungsbeschwerden zur Wahrung des Grundrechts auf informationelle Selbstbestimmung (u. a. Online-Durchsuchung, Vorratsdatenspeicherung). Außerdem war die Kanzlei mit Sonderermittlungen bei den Datenschutzaffären mehrerer deutscher Großkonzerne beauftragt. Zu den datenschutzrechtlichen Mandanten gehören betriebliche Datenschutzbeauftragte, Unternehmensleitungen, Personalvertretungen und Arbeitnehmer.

Im Interview mit …

Rechtsanwalt Olaf Methner

ISDSG: Wie sehen Sie die aktuelle Situation des Datenschutzes im Gesundheitswesen?

Im Gesundheitswesen wird der Datenschutz durch die jahrtausendealte ärztliche Schweigepflicht maßgeblich bestimmt. Die ärztliche Schweigepflicht soll Patienten davor schützen, dass Informationen über ihren Gesundheitszustand unbefugt an interessierte Außenstehende weitergegeben werden. Im Gesundheitswesen zeigen sich aktuell aber viele datenschutzrechtliche Probleme: Medizinische Daten werden zunehmend außerhalb des besonderen Vertrauensverhältnisses zwischen Arzt und Patient verarbeitet. Telemedizin und andere Hightech-Anwendungen im Medizinbereich führen überall zu umfangreichen Datenverarbeitungen. Zudem wird unter wirtschaftlichen Gesichtspunkten oft versucht, Gesundheitsdaten auch zur Einsparung von Kosten, zur Effizienzsteigerung und zur Qualitätssicherung einzusetzen. Elektronische Führung von Patientenakten, der Einsatz von Chipkarten, die Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern (Telemedizin) sind nur einige Beispiele für datenschutzrechtlichen Gefahren, denen die verantwortlichen Stellen im Gesundheitsbereich begegnen müssen. Neben den Patienten müssen dabei auch die im Gesundheitswesen Beschäftigten hinsichtlich ihrer personenbezogenen Daten geschützt werden.

Wo sehen Sie hier Verbesserungsbedarf?

Zum einen ist der Gesetzgeber aufgerufen, bei allen neuen Regulierungen im Gesundheitswesen, gerade im Bereich der Krankenkassen und Versicherungen, die datenschutzrechtliche Rahmenbedingungen zu berücksichtigen. Zum anderen sind sowohl Krankenhäuser als auch Arztpraxen und andere verantwortliche Stellen im Bereich des Gesundheitswesens gefordert, sensibel beim Umgang mit Patienten- und Beschäftigtendaten zu sein und alle erforderlichen organisatorischen, technischen und rechtlichen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit durchzuführen.

Welche Erfahrungen haben Sie mit Verstößen und der Einhaltung von Betroffenenrechten?

Nach unserer Erfahrung besteht ein großes Problem für Krankenhäuser und andere mit Gesundheitsdaten befasste Einrichtungen erst einmal darin, ihre Pflicht zur Bestellung eines geeigneten Datenschutzbeauftragten nach § 4f BDSG zu erfüllen. Dabei kann ein geeigneter Datenschutzbeauftragter bereits dafür sorgen, dass die Betroffenenrechte eingehalten werden, wenn die Einrichtung ihn in seiner Tätigkeit unterstützt. Im Übrigen begehen betroffene Einrichtungen sogar Ordnungswidrigkeiten, wenn sie nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig einen Beauftragten für den Datenschutz bestellt haben.

Deutschland gilt im internationalen Vergleich als Vorzeigeland in Bezug auf Gesetze und Verordnungen im Rahmen des Datenschutzes und der Datensicherheit – oder?

In der Theorie der datenschutzrechtlichen Grundlagen besteht tatsächlich eine solche Vorbildfunktion. Allerdings werden diese theoretischen Vorgaben für Datenschutz und Datensicherheit nicht immer in der Praxis umgesetzt.

Man erlangt hier den Eindruck, dass in der Masse von Gesetzen die Unsicherheit für die Datenschutzpraxis immer größer wird. Wo sehen Sie die größten Unsicherheiten in der Datenschutzpraxis mit rechtlichen Konsequenzen?

Die Anwendung der rechtlichen Vorschriften im Alltag der Datenverarbeitung führt sehr häufig zu Unsicherheiten. Allerdings haben die Datenschutzbeauftragten der Bundesländer in Zusammenarbeit mit der Deutschen Krankenhausgesellschaft eine Orientierungshilfe für die Anwendung von Krankenhausinformationssystemen erstellt, die für Rechtssicherheit sorgen kann, wenn man sie beachtet. Hierfür sind allerdings sowohl Kenntnisse im rechtlichen Bereich als auch das praktische Verständnis für die Datenverarbeitungsvorgänge im Gesundheitswesen erforderlich.

Wie können sich Geschäftsführer vor rechtlichen Konsequenzen schützen?

Da sich Geschäftsführer natürlich nicht persönlich um die Einhaltung aller Vorschriften kümmern können, müssen sie eine entsprechende Organisation ihrer Einrichtung durchführen, die Verstöße gegen die datenschutz- und datensicherheitsrechtlichen Vorschriften verhindert. Dazu müssen die rechtlichen und technischen Grundlagen der konkreten Einrichtung auf die erforderlichen Maßnahmen abgestimmt werden und z. B. die konkreten ausdrücklichen Einwilligungen der Betroffenen eingeholt werden. Gerade dies ist wiederum die Aufgabe des betrieblichen Datenschutzbeauftragten. Mit einer sorgfältigen Auswahl und ggf. Überwachung des Datenschutzbeauftragten hat der Geschäftsführer seine Pflichten erfüllt.

Die Telemedizin ist ein Thema, dem großes Potenzial für die Zukunft zugesprochen wird. Welche rechtlichen Aspekte sind hier für Teilnehmer des Gesundheitswesens zu berücksichtigen?

Die elektronische Kommunikation, die über die einzelne Gesundheitseinrichtung hinausgeht, wird immer wichtiger. Rechtlich sind hier insbesondere die Frage der wirksamen Einwilligung des Patienten in die Übermittlung seiner Daten, mögliche Anonymisierungen und Pseudonymisierungen sowie Maßnahmen der Datensicherheit von großer Bedeutung.

Welche rechtlichen Änderungen oder Gesetze müssen Ihrer Meinung nach her, um das Thema Telemedizin weiter voranzutreiben?

Eine spezialgesetzliche Ausgestaltung der datenschutzrechtlichen Anforderungen im Bereich der Telemedizin könnte den Anwendern eine größere Rechtssicherheit bieten und dazu beitragen, dass Patienten mehr Vertrauen in die Telemedizin haben. Andererseits wird der Gesetzgeber nicht ständig auf die technischen Änderungen und Entwicklungen in diesem Bereich reagieren können. Daher müssten durch konkrete Vorgaben, z. B. seitens der Datenschutzbeauftragten der Länder, die gesetzlichen Grundlagen ausgefüllt werden. ■

Interview: Nina Richard

Olaf Methner
ist u. a. Fachanwalt für Arbeitsrecht mit dem Schwerpunkt Beschäftigtendatenschutz. Er ist Gründungspartner der Kanzlei Baum Reiter & Collegen und Lehrbeauftragter für IT-Recht an der FOM – Hochschule für Oekonomie & Management.

Achtung bei der Bestellung des Datenschutzbeauftragten

Sowohl im Gesundheitswesen als auch in anderen Wirtschaftsbereichen herrscht häufig noch Unklarheit darüber, unter welchen Umständen die Bestellung eines Datenschutzbeauftragten verpflichtend ist.

Die Verunsicherung gilt auch für weitere Aspekte bei der Bestellung eines Datenschutzbeauftragten (DSB), z. B. in Bezug auf die Fragen, wie die Bestellung erfolgen muss oder wie sich die Anzahl der Personen berechnet, die an der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beteiligt sind. Außerdem bestehen teilweise unterschiedliche Bedingungen für öffentliche und nichtöffentliche Stellen. Unter nichtöffentliche Stellen fallen juristische (z. B. GmbH) und natürliche (Ärzte) Personen, Personengesellschaften (z. B. GbR) und auch nicht rechtsfähige Vereinigungen (z. B. Gewerkschaften).

Wer braucht einen DSB?

Der Begriff öffentliche Stellen bezeichnet Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen. Grundsätzlich ist jede öffentliche und nichtöffentliche Stelle, die personenbezogene Daten automatisiert erhebt, verarbeitet und/oder nutzt, nach § 4f des Bundesdatenschutzgesetzes zur schriftlichen Bestellung eines Beauftragten für den Datenschutz verpflichtet. Laut dem Bundesdatenschutzgesetz ist eine „automatisierte Verarbeitung [.] die Erhebung,

> *Ab 10 Personen liegt eine Verpflichtung zur Bestellung eines Datenschuztbeauftragten vor.*

Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen." Weiterhin liegt eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten vor, wenn innerhalb der Stelle mindestens 20 Personen mit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten in anderer Weise, z. B. mittels Karteien, beschäftigt sind. Allerdings gibt es Ausnahmen für nichtöffentliche Stellen. Sind in einer nichtöffentlichen Stelle höchstens neun Personen mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt, ist diese nicht verpflichtet, einen Beauftragten für den Datenschutz zu bestellen. Erhebt, verarbeitet oder nutzt das Unternehmen allerdings automatisiert personenbezogene Daten, welche einer Vorabkontrolle nach § 4d Abs. 5 BDSG unterliegen, verpflichtet dies zu einer Bestellung eines betrieblichen Datenschutzbeauftragten.

Eine Vorabkontrolle ist dann verpflichtend, wenn personenbezogene Daten der besonderen Art, wie z. B. ethische, religiöse oder politische Einstellungen, Gesundheitsdaten oder Daten zur Bewertung der Persönlichkeit verarbeitet werden. Auch Unternehmen, die personenbezogene Daten zum Zweck der Übermittlung, in anonymisierter oder nichtanonymisierter Form oder der Markt- und Meinungsforschung verarbeiten, sind zur Bestellung verpflichtet.

Ein weiteres und teilweise schwieriges Problem ist die Berechnung der Personen, die mit der Verarbeitung personenbezogener Daten beschäftigt sind. In § 4f des Bundesdatenschutzgesetzes heißt es: „Die Sätze 1 und 2 gelten nicht für die nichtöffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen." Doch welche Personen werden mitgerechnet? Und was genau bedeutet „in der Regel"?

In der Informationsbroschüre der Bundesbeauftragten für Datenschutz und Informationsfreiheit sowie in einem Merkblatt des hessischen Beauftragten für Datenschutz zum Thema betrieblicher Datenschutzbeauftragter wird erläutert, dass sämtliche Personen, unabhängig ihres arbeitsrechtlichen Status, zu berücksichtigen sind, die an der Verarbeitung von personenbezogenen Daten beteiligt sind. Somit werden auch Praktikanten, Auszubildende, Freiberufler, Zeitarbeiter sowie Voll- und Teilzeitarbeitskräfte in die Berechnung einbezogen. Da der arbeitsrechtliche Status für die Berechnung nicht entscheidend ist, werden auch Praxisinhaber mitgerechnet.

> *Der Datenschutzbeauftragte muss Wissen in BWL, IT und rechtliche Grundlagen mitbringen.*

Weiterhin ist entscheidend, dass es zur regelmäßigen Aufgabenbewältigung einer Person gehört, personenbezogene Daten automatisiert zu verarbeiten. So werden z. B. Urlaubsvertretungen oder eine kurzfristige Erhöhung der an der Verarbeitung beteiligten Personen nicht mitgezählt. Zusammenfassend lässt sich festhalten, dass grundsätzlich jede öffentliche und nichtöffentliche Stelle zur Bestellung eines Datenschutzbeauftragten verpflichtet ist. Eine Ausnahme von der Bestellung besteht für nichtöffentliche Stellen, wenn weniger als zehn Personen an der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten beteiligt sind.

Erforderliche Kompetenzen

Bei der Bestellung eines Datenschutzbeauftragten sollte darauf geachtet werden, dass die bestellte Person geeignet ist. Sie muss Wissen in BWL, IT und rechtliche Grundlagen mitbringen. Außerdem ist zu beachten, dass die bestellte Person in keinen Interessenskonflikt gerät, dadurch dass sie das Amt des betrieblichen Datenschutzbeauftragten bekleidet.

Wichtig: An dieser Stelle wird noch einmal explizit daraufhin hingewiesen, sollte ein Unternehmen nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet sein, besteht trotzdem die Pflicht zur Einhaltung des Datenschutzes im Unternehmen. Für die Einhaltung der Bestimmungen ist in diesem Fall die Geschäftsleitung verantwortlich, die bei Nichteinhaltung auch persönlich haftend ist. ■

Alexander Vogel

Jeder Betroffene hat das Recht, Einblick in die zu seiner Person gespeicherten Daten zu nehmen und diese ggf. auch zu korrigieren.

1. Goldene Regel: Betroffenenrechte

Der Schutz von sensiblen personenbezogenen Daten vor, während und nach der Behandlung ist zum Wohl der Patienten essenziell. Auf welche Auskunftsersuchen Einrichtungen sich einstellen sollten und wie das Prozedere bei der Einsicht Unbefugter gestaltet sein sollte.

Das Institut für Sicherheit und Datenschutz im Gesundheitswesen stellt in der Rubrik „Goldene Regeln" eine Reihe von Maßnahmen und Regeln vor, die im Alltag Anwendung finden sollten.

Im ersten Beitrag dieser Reihe werden organisatorische Aspekte des Datenschutzes behandelt. Aufgezeigt werden die Rechte von Betroffenen, die gegenüber Gesundheitseinrichtungen geltend gemacht werden können.

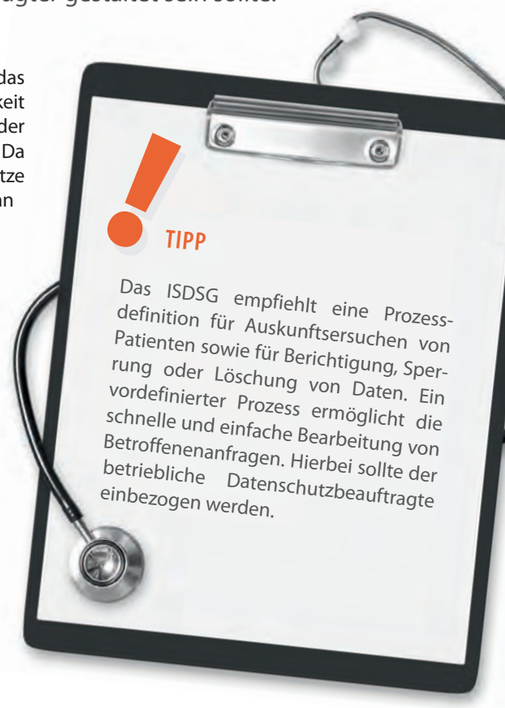
Betroffenenrechte

Das Bundesdatenschutzgesetz regelt in §§ 33 bis 35 sowie 42a die Rechte von Betroffenen. Jeder von der Datenverarbeitung Betroffene hat das Recht, jederzeit Auskunft über die zu seiner Person gespeicherten Daten und den Zweck der Datenverarbeitung einzuholen. Wird ein solches Auskunftsersuchen nicht beantwortet, kann der Betroffene dies dem zuständigen Landesdatenschützer, welcher dann weitere Maßnahmen einleitet, melden.

Des Weiteren hat jeder Betroffene das Recht, dass seine Daten bei Unrichtigkeit korrigiert oder die Daten bei fehlender Zweckbestimmung gelöscht werden. Da es im Gesundheitswesen weitere Gesetze zur Aufbewahrungspflicht gibt, kann an Stelle einer Löschung auch eine Sperrung der Daten erfolgen. Gesperrte Daten können nur mit Einverständnis des Betroffenen oder in bestimmten Ausnahmen genutzt werden.

Werden besondere personenbezogene Daten, wie z. B. Daten über die Gesundheit oder die Ethnie, durch Unbefugte eingesehen, so ist zum einen die Aufsichtsbehörde zu informieren und zum anderen der Betroffene, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden und die Strafverfolgung nicht mehr gefährdet wird. ■

Alexander Vogel



Impressum

ExperSite Ausgabe 01 2014 | **Herausgeber:** ISDSG, Postanschrift: Deintelleweg 11, 44309 Dortmund, Büroanschrift: Westfalendamm 251, 44141 Dortmund, Tel. + 49 231.4499599-91, Fax: + 49 231.4499599-99, www.isdsg.de | **Verantwortlich für den Inhalt:** Prof. Dr. Thomas Jäschke | **Redaktionsleitung:** Nina Richard | **Editorial Design und Layout:** c74 gestaltung & design, C. Robrahn, Dortmund, www.c74.org | **Druck:** Druckerzeugnisse Gerbrunn | **Auflage:** 5.000 | **Fotos:** Titel: iStock, dolgachov; S. 2: Falko Wübbecke, Dortmund; S. 3: Falko Wübbecke, Dortmund; iStock, dolgachov; shutterstock, auremar; iStock, froxx; S. 4: Fotolia, beermedia.de; S. 5: shutterstock, Jeff Metzger; S. 6/7: shutterstock, racorn; S.: 8/9: shutterstock, bikeriderlondon ; S.10/11: Uniscon GmbH; S. 12: iStock, froxx ; S.13: Kanzlei Baum Reiter & Collegen; S. 15: shutterstock, Michael Nivelet, John Smith Design; U4: hipaacartoons, R. J. Romero.

Einblicke & Ausblicke

"The sticky note? Oh, to save time and hassle, we just all use the same user name and password."

Wir bedanken uns für die inhaltlichen Beiträge bei:

Dr. Hubert Jäger, Uniscon GmbH

Olaf Methner, Kanzlei Baum Reiter & Collegen

Die nächste Ausgabe erscheint im März 2015

Im Schwerpunkt: Der integrierte Datenschutz in Krankenhäusern.

Ebenso wieder praktische Hinweise rund um den Datenschutzbeauftragten und das Rechtssystem.