ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Ausgabe 02 2016

Patientenbilder nutzen

Rechte von Patienten schützen und Patientendaten intern und extern richtig nutzen.

Veranstaltungen
Diese Veranstaltungen sollten Sie sich nicht entgehen lassen.

Zertifizierung
Qualitätsmerkmal oder Augenwischerei?

Dos and Don´ts
Diese Auskünfte sollte die Pforte nicht geben.

VERANSTALTUNGSTIPPS AUS DER BRANCHE

„nrw.uniTS trifft … Gesundheitsfachberufe“
13.09.2016 | 18.00 – 20.00 Uhr,
Hochschule für Gesundheit, Bochum

nrw·uniTS

Internet Security Days 2016 – Die Plattform für internationale Online-Security-Experten
22.09.–23.09.2016 | 09.00 – 18.00 Uhr,
Phantasialand Brühl, Brühl

networker NRW Der IT Verband

ZTG-Kongress eHealth.nrw
05.10.2016 | 09.30 – 17.15 Uhr
Kongresszentrum Westfalenhallen, Dortmund

eHealth.NRW

Roadshow Cybercrime
26.10.2016 | 15.00 – 18.00 Uhr
IHK Köln, Köln

networker NRW Der IT Verband

Update-BDSG – Datenschutz in der Medizin
10.11.2016 | 09.00 – 17.00 Uhr, Berlin

esturias Fachtagungen

Update-BDSG – Datenschutz in der Medizin
15.11.2016 | 09.00 – 17.00 Uhr,
Mainz

esturias Fachtagungen

IT Sicherheitstag NRW 2016 – Der Fachkongress für Dateninformation und Sicherheit
01.12.2016 | 10.00 – 17.00 Uhr
Alter Bundestag Bonn, Bonn

networker NRW Der IT Verband

Weitere Informationen erhalten Sie unter: www.isdsg.de.

Veranstaltungen des ISDSG

WIR SIND MIT DABEI:

Internetwoche Köln 24. bis 29.10.2016

Veranstaltungsreihe 2017
Im Jahr 2018 ist es soweit – die EU-DSGVO kommt. Aktuell befinden wir uns in einer Übergangsphase, in der noch viele Unklarheiten zur Auslegung der neuen Verordnung herrschen. Die unterschiedlichen Strukturen der Akteure im Gesundheitswesen machen die Auslegung der GVO noch komplizierter.

Starke Kooperation
Zusammen mit dem Veranstalter Update-BDSG und der Agentur esturias entwickelt das ISDSG deshalb eine an die Bedürfnisse des Gesundheitswesen angepasste Schulungsreihe für 2017.

Eckdaten
Die genauen Termine sowie eine erste Agenda und Anmeldemöglichkeiten stehen ab Herbst zur Verfügung.

Veranstaltungsorte:
- Hamburg
- Berlin
- Frankfurt
- Köln
- München

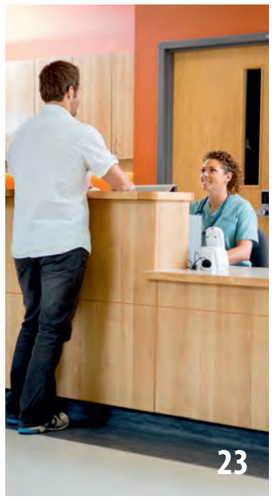
INDIVIDUELLE SCHULUNGSWÜNSCHE?

Gerne bieten wir für Sie und Ihre Mitarbeiter individuelle Workshops und Schulungen an. Sprechen Sie jetzt die Details mit uns ab.

ZERTIFIZIERTER DATENSCHUTZBEAUFTRAGTER (IOM)

Beginn:	27. September 2016
Dauer:	10 Wochen, einmal wöchentlich abends von 18.00 – 21.15 Uhr
Ort:	FOM Essen Herkulesstraße 32 | 45127 Essen

Inhalt



Achtung! Die Pforte kann Einfallstor für Datenschutzvergehen sein.

Patientenbilder: Auf die richtige Vorbereitung kommt es an.

Veranstaltungen & Termine 2

Das Team 4

Tipps & Fakten 6

Schwerpunkt

Die Nutzung von Behandlungsdaten für sekundäre Zwecke – intern und extern 8
Das ist zu beachten

Voice

Interview mit Manfred Weitz 14
Diesen Herausforderungen müssen sich Schulungen zukünftig stellen.

Gastbeitrag

Ein Datenschutz-Zertifikat ermöglicht den Austausch von Patientendaten 16
Über Qualität und Anwendervertrauen

Herausforderungen für die Pflegebranche – gut aufgestellt für die Zukunft 18
Handeln statt abwarten – sich heute schon auf morgen vorbereiten.

Der Datenschutzbeauftragte

So stärken Sie das Vertrauen Ihrer Patienten 22
Partner statt Verhinderer sein.

Goldene Regeln

5. Goldene Regel: Schulen Sie die Pforte 23
und entgehen Datenschutzpannen.

EDITORIAL

Sehr geehrte Leserinnen und Leser,

und schon wieder neigt sich das Jahr dem Ende zu und somit der Zielgeraden für 2016.

Jetzt ist der Zeitpunkt, sich nochmal die zu Beginn des Jahres gesetzten Datenschutzziele vor Augen zu führen. Haben Sie alles erreicht, was auf Ihrer Agenda stand bzw. sind Sie auf dem richtigen Weg, die noch offenen Punkte abzuarbeiten? Falls nicht, haben Sie jetzt noch die Chance, etwas zu tun.

Bei der Schulung von Mitarbeitern und Kollegen sollten auch Abteilungen auf Ihrem Plan stehen, die auf den ersten Blick nicht in direktem Kontakt mit Patienten stehen – so beispielsweise Ihre Pforte.

Auch die Bedeutung des Themas IT-Sicherheit ist in diesem Jahr größer geworden. Deshalb sollten auch Datenschutzverantwortliche dieses Thema parat haben – zeigen Sie sich aktiv.

Natürlich darf auch die Europäische Datenschutzgrundverordnung nicht fehlen. Bereiten Sie sich und Ihre Einrichtung auch hier früh genug vor.

Ich wünsche Ihnen viel Spaß bei der Lektüre.

Ihr

Prof. Dr. Thomas Jäschke
Institutsleiter ISDSG

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.

Das ISDSG ist ein Dienstleistungsbereich der DATATREE AG und beschäftigt sich mit allen Fragen zum Thema IT-Sicherheit und Datenschutz mit Schwerpunkt auf den Akteuren des Gesundheitswesens. Wir unterstützen Kunden bei der Bewältigung von Datenschutz- und IT-Sicherheitsherausforderungen, die durch die fortschreitende Digitalisierung zunehmend auftreten.

Nina Richard
Marketing & Kommunikation

Als Verantwortliche für die Bereiche Marketing und Kommunikation ist sie Ansprechpartnerin für alle Fragen rund um das redaktionelle Angebot des ISDSG und der ExperSite.

richard@isdsg.de

Jan Domnik
IT-Security

Zu seinen Kernaufgaben gehören die Durchführung und Koordination von Penetrationstests, die Auditierung von IT-Systemen und die Überprüfung von Sicherheitskonzepten.

domnik@isdsg.de

Christine Thieme
Datenschutz

Sie ist die Spezialistin für Fragestellungen aus den Bereichen Direktmarketing und Marktforschung und unterstützt Sie bei der datenschutzkonformen Umsetzung Ihrer Projekte.

thieme@isdsg.de

Magnus Welz
Datenschutz

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

Prof. Dr. Thomas Jäschke
Vorstand

Der Medizin-Wirtschaftsinformatiker ist Experte im Gesundheitssektor und Datenschutzbeauftragter für namhafte Einrichtungen im Gesundheitswesen. Als Institutsleiter ist er der Kopf des ISDSG-Teams.

dsb@isdsg.de

Alexander Vogel
Datenschutz

Mit seinem fundierten Know-how im medizinischen Umfeld und dessen Informationssystemen begleitet er Ihre Prozesse und Abläufe praxisnah und zielorientiert.

vogel@isdsg.de

Angelica Morina
Projektmanagement

Sie verfügt über ein breit gefächertes Leistungsspektrum und hat als Projekt- und Administrationsmanagerin Ihr Projekt in Bezug auf die Terminplanung und das Controlling fest im Blick.

morina@isdsg.de

Thorben Beer
Datenschutz

Als Projektleiter kann er auf seine Erfahrung in mittelständischen IT-Beratungsunternehmen zurückblicken. Angepasst an Ihre Wünsche und individuelle Situation entwickelt er die für Sie richtigen Konzepte.

beer@isdsg.de

Fabian W. Rüter
Vertrieb

Sie wünschen ein individuelles Angebot für die Themen Datenschutz oder IT-Sicherheit für Ihr Haus? Dann ist Fabian Rüter der richtige Ansprechpartner für Sie.

rueter@isdsg.de

Diese Punkte sollten Datenschutzerklärungen für Websites enthalten

Als Betreiber einer gewerblichen Internetseite sind Krankenhäuser dazu verpflichtet, eine Datenschutzerklärung für die Nutzer anzubieten. Häufig existieren hier noch Schwachstellen.

1. Information über Betroffenenrechte
Jeder Betroffene hat gegenüber der datenverarbeitenden Stelle ein Auskunftsrecht sowie ein Recht zur Löschung, Berichtigung und Sperrung seiner Daten. In der Datenschutzerklärung sollten Nutzer deshalb über diese Rechte informiert werden und darüber hinaus auch aufgeführt sein, wie sie diese Rechte wahrnehmen können.

2. Einwilligung
Falls über die Website personenbezogene Daten für andere Zwecke als die Vertragsabwicklung oder die Funktion der Internetseite genutzt werden, ist der Nutzer darüber zu informieren und seine ausdrückliche Einwilligung für die anderweitige Nutzung muss eingeholt werden. Gleichzeitig ist der Nutzer darüber zu informieren, dass er der Verwendung seiner Daten jederzeit widersprechen kann.

3. Besondere Funktionen der Website
Die Datenschutzerklärung muss alle datenschutzrechtlich relevanten Funktionen der Website berücksichtigen, mit denen der Nutzer personenbezogene Daten übermittelt. Diese Funktionen können beispielsweise Newsletter-/Bestellformulare, Kommentare, Kontaktformulare oder Gästebücher sein.

4. Auffindbarkeit der Datenschutzerklärung
Es gilt, dass die Datenschutzerklärung aussagekräftig auf der Website auffindbar ist, sodass sie jederzeit von Nutzern abgerufen werden kann. Sie sollte maximal zwei Klicks von jeder Seite entfernt sein – im Optimalfall ist sie direkt und von jeder Unterseite aus abrufbar.

5. Cookies
Die Information über die Nutzung von Cookies ist Pflicht. In der Datenschutzerklärung ist darüber aufzuklären, welche Cookies und welche Speicherdauer genutzt wird. Auch die Information über die Möglichkeit, Cookies im Browser zu löschen und zu deaktivieren darf nicht fehlen.

6. Datenverarbeitung außerhalb der EU
Falls Daten in das nichteuropäische Ausland übermittelt werden, sind die Websitenutzer darüber aufzuklären.

7. Datenaustausch mit anderen Websites
Bei der Nutzung von Social Plug-ins, wie z. B. Facebook-Like-Button, Instagram oder Google+, ist in der Datenschutzerklärung darauf hinzuweisen, da eine direkte Verbindung mit den Servern von Drittanbietern erfolgt. Um auf Nummer sicher zu gehen, sollten Zwei-Klick-Social-Media-Buttons genutzt werden.

8. Tracking-Tools
Die Datenschutzerklärung hat auf die eingesetzte Tracking-Technik hinzuweisen. Es sollte aufgeführt sein, mit welchem Ziel diese genutzt wird, welche Tools sich im Einsatz befinden und wie diese funktioniert. Hinzu kommt der Hinweis, wie die Webanalyse verhindert werden kann und dass damit ggf. Funktionen der Website nicht mehr zur Verfügung stehen.

Initiative für IT-Sicherheit im Gesundheitswesen

Die jüngsten Vorfälle haben gezeigt, dass niemand von uns vor Hackerangriffen sicher ist. Die Auslegung in den Medien war dabei nicht immer ganz korrekt. Dies führt zu Zweifeln an Deutschlands Krankenhäusern und der Sicherheit der hoch sensiblen Gesundheitsdaten. Diesem Bild soll mit der Initiative für IT-Sicherheit im Gesundheitswesen öffentlich wirksam entgegengewirkt werden.

Das ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen möchte deshalb einen Zusammenschluss von IT-Verantwortlichen, Geschäftsführern und Datenschutzbeauftragten herbeiführen, um Aufklärung zu betreiben und Transparenz im Bereich der IT-Sicherheit zu schaffen. Es sollen so praxisnahe Handlungsempfehlungen für die Krankenhauslandschaft geschaffen werden.

Ziele der Initiative:
- Verbesserung der Reputation von Krankenhäusern in Bezug auf die IT-Sicherheit
- Erarbeitung von Grundsätzen zur Lage der IT-Sicherheit in Krankenhäusern
- Krisenfälle bestmöglich vermeiden
- Stärkung des Bewusstseins für IT-Sicherheit
- Öffentlichkeitswirksame Pressearbeit
- Optional Entwicklung einer Kampagne zur IT-Sicherheit

Mögliche Arbeitsschritte:
- Aufnahme von Mitwirkenden in die Initiative und Themensammlung
- Presseerklärung zur Bekanntgabe der Initiative
- Kennenlernen aller Mitwirkenden und Besprechung der weiteren Agenda
- Treffen der Mitwirkenden zur Ergebniserarbeitung
- Veröffentlichung der Ergebnisse
- Presseerklärung zu den Ergebnissen
- Start der Aufmerksamkeitskampagnen

Mitwirkung:
Es ist kein Beitrittsbeitrag fällig. Das ISDSG übernimmt als Gründer der Initiative die Organisation und Aufbereitung der angedachten Arbeitsschritte und bietet Ihnen so eine Plattform, um Ihre Interessen zu vertreten. Um die Wirksamkeit in der Öffentlichkeit zu verstärken, ist die gemeinsame Beteiligung an Maßnahmen natürlich wünschenswert, dies bedeutet die Aktivierung Ihres Netzwerkes zur Verbreitung von Pressemeldungen und Arbeitsergebnissen.

Lassen Sie uns gemeinsam etwas verändern! Wir würden uns freuen, Sie als Mitglied der Initiative für IT-Sicherheit im Gesundheitswesen begrüßen zu dürfen.

Ihre Rückmeldung nimmt Nina Richard unter **richard@isdsg.de** gerne entgegen.

Schwerpunkt

Die Nutzung von Behandlungsdaten für sekundäre Zwecke – intern und extern

Patienten- und Behandlungsdaten sind nicht nur für die eigentlichen Erhebungszwecke – medizinische Dokumentation und Abrechnung – von Interesse, auch nachgelagerte, sogenannte sekundäre Zwecke haben eine große Bedeutung. So werden diese Daten beispielsweise für die medizinische Forschung, Versorgungsforschung oder die Aus-, Fort- und Weiterbildung von medizinischem Fachpersonal benötigt. Allerdings gilt es zu prüfen, ob eine Verwendung aus Datenschutzsicht überhaupt vertretbar ist.

Datenschutzpanne in Sicht?

Auf einem medizinischen Kongress zu Beginn des Jahres, den wir besuchten, berichtete ein etablierter Facharzt aus der Branche über den Krankheitsverlauf eines Patienten. Zur Veranschaulichung der Thematik zeigte er seinem Publikum die CT-Bilder des Patienten, die die Thematik natürlich noch spannender machten. Einen bitteren Beigeschmack erhielt dies für uns als Datenschützer aber dennoch – denn die zur Verfügung gestellten Aufnahmen des Patienten waren nicht ausreichend anonymisiert. In großen Druckbuchstaben war auf der eingeblendeten Folie, die für uns und alle anwesenden Kongressbesucher sichtbar war, deutlich der Name des Patienten zu lesen.

Aus Datenschutzperspektive ein No-Go! Oder etwa doch nicht?

Gesetzliche Grundlagen

Grundsätzlich kann festgehalten werden, dass die Nutzung von erhobenen Patienten- und Behandlungsdaten zu unterschiedlichsten sekundären Verwendungszwecken möglich ist. Voraussetzung ist hier allerdings, dass entweder eine gesetzliche Legitimation existiert oder aber die konkrete Einwilligung des Patienten für den jeweiligen Verwendungszweck. Doch auch wenn gesetzliche Regelungen für die weitere Verarbeitung oder Übermittlung von Patienten- und Behandlungsdaten existieren, sind diese nicht immer identisch geregelt und abhängig von dem Sekundärzweck und ggf. dem vorliegenden Einzelfall.

> *Zur Verfügung gestellte Aufnahmen des Patienten müssen ausreichend anonymisiert sein!*

Nutzung zur Fort- und Weiterbildung

Leistungserbringer verfügen über eine Vielzahl von Behandlungs- und Patientendaten, die insbesondere für die interne Fortbildung von Ärzten, medizinischem Personal, aber auch Verwaltungsangestellten genutzt werden. Nicht selten existieren in dieser Fülle von Informationen spannende und besondere Krankheitsbeispiele, deren Hergang und Behandlung für die Allgemeinheit zur Verfügung gestellt werden müssen, um auf Fachkonferenzen, internen Schulungen oder für die Ausbildung von medizinischem Personal, beispielsweise Assistenzärzte, Pflegepersonal oder Medizinstudenten, vorgestellt zu werden, damit der Dienst am Menschen weiter optimiert werden kann.

Länder regeln eigenständig

Der Großteil der Bundesländer regelt die Nutzung von Patientendaten für Fort- und Weiterbildung selbstständig. Grundsätzlich wird unterschieden zwischen interner und externer Nutzung bzw. Übermittlung. Daraus resultieren verschiedene Nutzungskonstellationen.

- Gesetzliche Regelung für interne und externe Nutzung
  Die für die Nutzung von Patientendaten für die Fort- und Weiterbildung unkomplizierteste Variante ist das Vorhandensein einer oder mehrerer gesetzlicher Regelungen, die sowohl die interne als auch externe Nutzung der Daten für sekundäre Verwendungszwecke erlauben.

- Gesetzliche Regelung für intern und Einwilligung für extern
  Bei der zweiten Variante ist die interne Nutzung der Daten für Fort- und Weiterbildung durch ein Gesetz geregelt. Hier besteht nur die Besonderheit, wenn Patientendaten für externe Zwecke genutzt werden. Hier werden eine Einwilligung sowie eine Entbindung von der Schweigepflicht durch den Patienten benötigt.

- Keine gesetzliche Regelung
  Existiert keine gesetzliche Regelung für das entsprechende Bundesland, können die Patientendaten nur mit Einwilligung sowie Schweigepflichtsentbindung genutzt werden.

Für den Fall, dass keine gesetzliche Grundlage zur Verwendung der Patientendaten existiert, ist eine Einwilligung des Patienten einzuholen.

Auflistung der gesetzlichen Regelungen zur Nutzung von Patientendaten für Aus-, Fort- und Weiterbildungsmaßnahmen in einzelnen Bundesländern

Land	Interne Verwendung	Externe Verwendung
BW	§45 LKHG-BW	§46 LKHB-BW
BY	§27 BayKrG	Einwilligung
BE	§27 LKG	Einwilligung
BB	Einwilligung	Einwilligung
HB	§2 Abs. 5 BremKHDSG	§4 Abs.1 BremKHDSG
HH	§10 Abs. 1 HmbKHG	Einwilligung
HE	Einwilligung	Einwilligung
MV	§16 LKHG M-V	§35 Abs.1 Satz 12 LKHG M-V*
NI	Einwilligung	Einwilligung
NW	§11 GDSG NW*	§11 GDSG NW*
RP	§36 Abs. 2 LKG*	Einwilligung
SL	§13 Abs. 3 SKHG*	Einwilligung
SN	§33 Abs. 2 SächsKHG*	Einwilligung
ST	Einwilligung	Einwilligung
SH	Einwilligung	Einwilligung
TH	§27 Abs. 3 Satz 1 ThürKHG	Einwilligung

* Nur auf Grundlage des Gesetzes, wenn der Zweck nicht in vertretbarer Weise mit anonymisierten Daten erreichbar ist

Einwilligung

Für die Einwilligungserklärung sollten die folgenden Punkte zwingend beachtet werden:

Information
Jede Einwilligung beginnt mit einer Information des Betroffenen. Hier sind die Gründe für die Nutzung und eine genaue Beschreibung, wie die Daten genutzt werden, aufzuführen.

Zweckbestimmung
Eine allgemeingültige Einwilligung zur Verwendung der Bilder ist nicht möglich. Deshalb gilt es, den konkreten Zweck der Verwendung aufzuführen. Beispiel: Konferenzen, interne Fortbildungen, externe Veranstaltungen/Fortbildungen. Auch ist eine Abgrenzung zwischen der Verwendung für reine Präsentationszwecke oder aber der Veröffentlichung der Bilder und Daten vorzunehmen. Auch das Abdrucken und Bereitstellen der Präsentation für Dritte kann bereits hierunter fallen. Zusätzlich sollte auch auf das Widerrufsrecht für die zukünftige Verwendung der Patientendaten hingewiesen werden. Auch der Hinweis, dass sobald die Präsentation oder die Bilder im Internet veröffentlicht ist, eine Löschung faktisch nicht möglich ist, sollte dem Patienten gegeben werden.

> *Eine allgemeingültige Einwilligung zur Verwendung der Bilder ist nicht möglich.*

Widerrufsbelehrung
Am Schluss einer Einwilligungserklärung steht die Belehrung über das Widerrufsrecht des Betroffenen. Eine Einwilligung kann jederzeit und ohne die Angabe von Gründen für die Zukunft widerrufen werden.

Nutzung von anonymisierten Daten

Werden für die Fort- und Weiterbildung Daten genutzt, die keinen Rückschluss auf eine bestimmte Person zulassen – sogenannte anonymisierte Daten –, so ist weder eine gesetzliche Grundlage noch die Einwilligung/ Schweigepflichtsentbindung des Patienten notwendig. Eine solche Nutzung ist immer möglich.

Anonym bedeutet in diesem Zusammenhang, dass sämtliche patientenidentifizierende Merkmale entfernt werden. Demnach ist auf Daten wie:

- Vor- und Nachname
- Geburtsdatum
- Anschrift
- Patientennummer (intern)
- Versichertennummer

komplett zu verzichten, damit der Patient unter keinen Umständen identifizierbar ist.

Nutzung von Bild- und Videodateien

Bei der Nutzung von Bild und Videomaterial gilt es, das Recht am eigenen Bild zu berücksichtigen. Dies bedeutet, dass der Patient selbst darüber bestimmen soll und kann, wie sein Bild genutzt wird. Aus diesem Grund gilt, dass dieses Material unbedingt in anonymisierter Form zu nutzen ist. In dem Fall ist es nicht ausreichend, wenn Namen, Geburtsdatum etc. entfernt wurden. Auch physische Merkmale, durch die eine Identifikation des Patienten möglich wäre, gilt es zu

Auf die richtige Vorbereitung kommt es an.

entfernen, so z. B. Narben, Prothesen, Tattoos, Piercings oder Muttermale. Sollten diese Merkmale jedoch den Zweck der Präsentation darstellen, ist ein Unkenntlichmachen natürlich sinnlos.

> *Die ursprünglich für die Behandlung von Patienten erhobenen Daten dürfen nicht ohne Weiteres für Forschungszwecke eingesetzt werden.*

Natürlich sollten ebenfalls das Gesicht und die Augen unkenntlich gemacht werden. Ebenso ist hier eine Einwilligung des Patienten zur Veröffentlichung des Materials notwendig.

Nutzung zu Forschungszwecken

Auch bei der Nutzung von Patientendaten zu Forschungszwecken gilt es, datenschutzrechtliche Bestimmungen sowie die Persönlichkeitsrechte der Patienten zu wahren.

Die ursprünglich für die Behandlung von Patienten erhobenen Daten dürfen nicht ohne Weiteres für Forschungszwecke eingesetzt werden. Hierzu bedarf es einer gesonderten Einwilligung des Patienten sowie der ausführlichen Information über den Verbleib der Daten.

Verwendung von Forschungsdaten

Einen ersten Anhaltspunkt über die Verwendung von Forschungsdaten bietet hier das Bundesdatenschutzgesetz. In § 40 BDSG wird aufgeführt, dass Daten, die für Forschungszwecke erhoben und gespeichert wurden, auch nur für die wissenschaftliche Forschung eingesetzt werden dürfen. Zudem sind die Daten zu anonymisieren, sobald dies der Forschungszweck zulässt. Bis zu diesem Punkt sind die Merkmale, die Rückschlüsse auf eine Person geben können, gesondert zu speichern und dürfen nur unter bestimmten Voraussetzungen mit den Forschungsergebnissen zusammengefügt werden. Darüber hinaus dürfen personenbezogene Daten von der Forschungsstelle nur veröffentlicht werden, wenn:

- eine Einwilligung des Betroffenen vorliegt und
- dies für die Darstellung der Forschungsergebnisse unerlässlich ist.

Anonymisierung

In der Forschung können drei verschiedene Arten von Anonymisierung unterschieden werden: formale, faktische und absolute Anonymisierung.

Bei der formalen Anonymisierung sind direkte Identifikationsmerkmale, wie der Name der Person, Ort oder Bilder, aus den Forschungsergebnissen zu entfernen. Bei der faktischen Anonymisierung hingegen sind die Daten so zu verändern, dass die Re-Anonymisierung nur mit einem unverhältnismäßigen Aufwand durchgeführt werden kann. Bei der absoluten Anonymisierung ist eine Re-Identifikation nicht mehr möglich.

Aus datenschutzrechtlichen Gesichtspunkten ist die absolute Anonymisierung in Kombination mit einer Zugangsbeschränkung am sinnvollsten.

Pseudonymisieren

Auch das Ersetzen von persönlichen Merkmalen durch Pseudonyme kann sich anbieten. So werden die Originalangaben mithilfe einer bestimmten Zuordnungsregel pseudonymisiert.

Ist diese Zuordnungsregel bekannt, kann dieser Vorgang in der Regel wieder rückgängig gemacht werden. Durch die Pseudonymisierung bleibt die Interpretierbarkeit der Ergebnisse erhalten, ohne dass die Person entsprechend identifiziert werden kann.

	Original-angaben	Pseudonym
Name	Tanja	Mareike
	Hubert	Jan
Beruf	Tischler	Dachdecker
Arbeitgeber	Rainers Tischfabrik	Dachdecker Mayer

Aggregation

Eine Verallgemeinerung der Forschungsdaten kann zu einem besseren Schutz vor einer Re-Anonymisierung bzw. Re-Pseudonymisierung durch Unbefugte beitragen. Dazu werden zu den einzelnen Daten Gruppen gebildet und die Datensätze in diese Gruppen eingefügt. So werden beispielsweise für das Alter Altersklassen oder für das Gewicht Gewichtsgruppen gebildet. Durch diese Gruppen- bzw. Klassenbildung werden einzelne Datensätze mit anderen aggregiert und eine Identifizierung des Einzelnen wird erschwert.

Für die Verwendung von Patienten- und Behandlungsdaten zu sekundären Zwecken existieren viele Gesetze.

Fazit

Für die Verwendung von Patienten- und Behandlungsdaten zu sekundären Zwecken existieren viele Gesetze, sowohl auf Landes- als auch auf Bundesebene. So ist vor der Nutzung von Behandlungsdaten zu sekundären Zwecken zu analysieren, ob dies auf Grundlage eines Gesetzes geschieht und wenn ja, wie die Ausgestaltung geregelt ist. Denn einige Gesetze gestatten die Verwendung ohne Einschränkungen für das verarbeitende Krankenhaus, wiederum andere fordern explizit die Einholung einer Einwilligung beim Patienten. Auch legitimiert ein Teil der Gesetze die Nutzung und Übermittlung für nachfolgende Zwecke, wenn eine Anonymisierung dem sekundären Zweck entgegensteht oder nur mit einem verhältnismäßig hohen, zeitlichen und monetären Aufwand realisiert werden kann.

Transparenz und Datensparsamkeit

Zwei wesentliche Grundsätze des Datenschutzes sind die Transparenz und die Datensparsamkeit. Diese beiden Aspekte sollten in jedem Fall bei der Verwendung von Behandlungs- und Patientendaten für sekundäre Zwecke beachtet werden, auch wenn eine gesetzliche Grundlage für die sekundäre Nutzung besteht.

Eine Information des Patienten über die Nutzung seiner Behandlungsdaten für einen nachgelagerten Verwendungszweck schafft Vertrauen und Akzeptanz. Des Weiteren sollten auch nur die Daten verwendet werden, die für den beschriebenen Zweck notwendig sind. ■

Nina Richard, Alexander Vogel

ANZEIGE

GRATIS für alle Leser

Für alle Datenschutzbeauftragten:

Das Paket für Ihre nächste Datenschutzschulung – 100% Zeitersparnis!

Sichern Sie sich heute Ihr Schulungspaket für Ihre nächste Datenschutzschulung

Die Zeit ist wie immer knapp und Sie konnten sich durch Ihre Doppelfunktion den Inhalten für die anstehende Schulung noch nicht annehmen? Wir haben DIE Lösung für Sie! Stefan Purder hat eine Schulungs-CD zusammengestellt, mit der Sie kinderleicht und Schritt für Schritt Ihre eigene Datenschutzschulung zusammenbauen können – und das sehr zeitsparend.

Stellen Sie sich vor:

- ✔ Sie sparen **8 Stunden** (und mehr) für die Aufbereitung von Schulungsunterlagen und können diese sogar noch individuell gestalten – kinderleicht!
- ✔ Sie erhalten auf der CD ein Tool, mit dem Sie Ihre **Teilnehmerliste** sowie die entsprechenden **Teilnahmezertifikate im Handumdrehen automatisiert** erstellen
- ✔ Anstatt sich mühsam durch die gesetzlichen Vorschriften zu kämpfen, stehen Ihnen **alle Informationen mit einem Mausklick** zur Verfügung

Denn im Bundesdatenschutzgesetz §4 Abs. 1 Nr.2 ist ganz klar geregelt, dass Sie als Datenschutzbeauftragter die Aufgabe haben Ihre Mitarbeiter zu schulen.

Wen müssen Sie schulen?

Zielgruppe der Schulung müssen alle Beschäftigten sein, deren Arbeit mit der Nutzung personenbezogener Daten verbunden ist. In der Regel vor allem die Mitarbeiter, die in der Personalabteilung, der EDV, der IT-Abteilung, dem Betriebsrat, dem Vertrieb oder der Beschaffung angehören. Aber auch Ihre Kollegen in der Produktion haben mit personenbezogenen Daten zu tun.

Passen Sie die Schulung individuell an!

Gehen Sie auf die Besonderheiten in Ihrem Unternehmen ein. Werden Sie möglichst konkret und nennen Sie praxisbezogene Beispiele. Dann wird auch die Aufmerksamkeit der Teilnehmer steigen.

Wie das geht?

Mit dem „Schulungspaket Datenschutz" haben Sie Ihre Allzweckwaffe gefunden: Auf 72 komplett ausgearbeiteten Power-Point-Folien stehen Ihnen die Inhalte übersichtlich und leicht verständlich zur Verfügung. Zu jeder Folie erhalten Sie Notizen und Hinweise für Ihren Vortrag, die Sie auf Wunsch mit Ihren eigenen Anmerkungen ergänzen können.

Schulung vorbei, aber über manche Themen wissen Sie nicht 100 %, die in der Schulung als Fragen von Ihren Mitarbeitern gekommen sind

Kein Problem, denn Sie erhalten das Geschenk „Schulungspaket Datenschutz" als CD-ROM zusammen mit einem Test-Exemplar unseres **Fachmagazins „Datenschutz aktuell"**.

„Datenschutz aktuell" informiert Sie in nur 15 Minuten über

…die wirklich effizienten Maßnahmen für Ihr Unternehmen

… und wie Sie sie ganz einfach und schnell umsetzen.

Datenschutz aktuell.

Leicht verständlich und sofort anwendbar erhalten Sie auf nur 8 Seiten alle notwendigen Tipps, Checklisten und Handlungsempfehlungen, um Datenpannen auszuschließen und maximale Sicherheit für Ihr Unternehmen, Ihre Mitarbeiter und Ihre Kunden zu gewährleisten.

Topaktuelle Datenschutz-Themen, die in Ihrer Praxis täglich auftauchen

- ✔ **Die neuesten Urteile** zum Datenschutz – und alle Handlungsempfehlungen
- ✔ **Checklisten**, mit denen Sie Ihre Arbeit schnell und effizient meistern
- ✔ **Musterschreiben und -merkblätter**, die Sie sofort übernehmen können
- ✔ **Tipps und Tricks**, wie Sie Ihre Tätigkeit noch zeitsparender ausüben

… und noch so viel mehr. **Stellen Sie in der Redaktionssprechstunde (GRATIS!) Ihre eigenen Fragen** – und nutzen Sie das Online-Portal für noch mehr Tipps und Infos.

Mein Tipp für Sie: Antworten Sie sofort und sichern Sie sich Ihr kostenloses Exemplar der „Grundlagenschulung Datenschutz" sowie Ihre Gratis-Testausgabe von „Datenschutz aktuell". So machen Sie Ihre nächste Unterweisung zum Thema Datenschutz zu einem vollen Erfolg!

Schützen Sie sich mit „Datenschutz aktuell". Sobald sich Änderungen ergeben, sobald dem Gesetzgeber wieder einmal eine „Gesetzes-Innovation" zum Thema Datenschutz einfällt ... sind Sie informiert. Und können Ihre Pflichten und Vorgaben sofort erfüllen.

Und der Bonus-Vorteil:
Ganz egal, wie Sie sich nach Ihrem 14-Tage-Gratis-Test entscheiden: Ihre Gratis-Test-Ausgabe und Ihr Gratis-Geschenk gehören für immer Ihnen!

Und ich bitte Sie, diese kostenlose Ausgabe probeweise durchzublättern. **„Datenschutz aktuell"** wurde speziell für Sie konzipiert. Für Datenschutzbeauftragte, die weder Zeit noch Lust haben, ihre knappe Arbeitszeit zwischen ihrem Hauptjob und der Zusatzaufgabe „Datenschutz" aufzuteilen.

Dieses Angebot gilt nur, solange der Vorrat reicht. Deshalb empfehle ich Ihnen, Ihr Gratis-Exemplar von „Datenschutz aktuell" zu sichern und als Geschenk das „Schulungspaket Datenschutz" sofort anzufordern.

GRATIS-Coupon

Das Schulungspaket Datenschutz

☒ **Ja,** bitte schicken Sie mir das „Schulungspaket Datenschutz" als GRATIS-Willkommensgeschenk zu. Zusätzlich erkläre ich mich bereit eine Ausgabe des Fachinformationsdienstes „Datenschutz aktuell" gratis zu testen mit einer Ansichtszeit von 14 Tagen. Die 1. Ausgabe als 14-Tage-Test darf ich gratis auf jeden Fall behalten. Wenn mich der Test überzeugt und ich Ihnen innerhalb von 14 Tagen nach Erhalt der Ausgabe nichts Gegenteiliges mitteile (Fax oder E-Mail genügt), erhalte ich bequem per Post 32 Ausgaben im Jahr plus zwei Jahresindizes zu je 19,95 € zzgl. 1,82 € Versandkosten und 7% MwSt. Ich kann den Bezug von „Datenschutz aktuell" jederzeit zum Ende eines Bezugsjahres kündigen – ganz einfach ohne Angabe von Gründen.

DAT2642

Firma .....

Vorname und Nachname .....

Straße und Hausnummer .....

PLZ und Ort .....

Datum und Unterschrift ..... ✗

Gleich einsenden an: **redaktion@datenschutz-aktuell.de**
Datenschutz aktuell, Theodor-Heuss-Straße 2-4, 53177 Bonn oder **Fax an: 0228/8205-5350**

DAT-BU-DSP-16/25

Manfred Weitz hat sich 1992 als Referatsleiter beim Hessischen Datenschutzbeauftragten beruflich dem Datenschutz verschrieben und nach der Pensionierung 2009 das Veranstaltungsformat Update-BDSG ins Leben gerufen. Damit hält er Datenschutzinteressierte insbesondere aus dem Gesundheitswesen auf dem aktuellen Stand.

Manfred Weitz

Immer auf dem aktuellen Stand von Datenschutzthemen zu sein, ist für Datenschutzbeauftragte neben der Vielzahl an Aufgaben, die das Tagesgeschäft mit sich bringt, nicht immer ganz einfach. Glücklicherweise gibt es Menschen, die sich genau dieser Herausforderung stellen. Im Interview sprechen wir mit einem von ihnen: Manfred Weitz über den Ursprung seiner Veranstaltungsreihe Update-BDSG und die Rolle und Auswirkungen der EU-DSGVO.

ISDSG: Herr Weitz, Sie sind Organisator von Datenschutz-Fachtagungen und leidenschaftlicher Datenschützer – wie kamen Sie dazu, die Veranstaltungsreihe Update-BDSG ins Leben zu rufen?
Vier wichtige Faktoren kamen 2009 zusammen: Die damalige BDSG-Novellierung rief nach ergänzenden Informationen für die Fachwelt, ich wollte die Zeit nach der Pensionierung noch etwas ausfüllen, ich hatte ein recht großes berufliches Netzwerk und schon seit 1992 lag mir die Weiterbildung im Datenschutz als nebenamtlicher Dozent sehr am Herzen.

Dass der ersten Tagung am 25.10.2009 in Wiesbaden als Versuchsballon immer mehr Veranstaltungen jährlich folgen würden, und dann ab 2013 mit der Spezialisierung im medizinischen Bereich die Entdeckung des spannendsten Themenfeldes im Datenschutz gelang, konnte ich nicht voraussehen. Bei dem zunehmenden Erfolg der Tagungsreihe half auch die Tatsache, dass insbesondere im medizinischen Bereich relativ wenig Anbieter vorhanden sind, obwohl der Informationsbedarf im Hinblick auf die Art und Menge der betroffenen Daten und die vorhandenen Probleme in der Praxis besonders ausgeprägt erscheint.

Nun steht die ab 25.5.2018 geltende EU-DSGVO quasi vor der Tür, denn die bis dahin laufende Anpassungszeit ist real recht kurz. Dies hat weitreichende Folgen auch für das Gesundheitswesen. Denn die das BDSG fast vollständig ablösende GVO enthält viele Neuerungen und zwingt den deutschen Gesetzgeber bis 25.5.2018 auch zur Anpassung der zahlreichen Folgevorschriften für den Datenschutz im Gesundheitsbereich. Was wird dies für Update-BDSG bedeuten?
Update-BDSG ist eine bereits etablierte Veranstaltungsreihe, die sich nicht nur mit aktuellen Gegebenheiten des Bundesdatenschutzgesetzes beschäftigt, sondern vielmehr eine Plattform für ein breit gefächertes Informationsangebot für Datenschutz auch im Gesundheits- bzw. Sozialwesen und Pflegebereich geworden ist. Diese beinhalten im Vergleich zu anderen Branchen viele Besonderheiten, da der Patient/Bewohner, sein Wohlergehen und seine besonders schützenswerten Daten immer im Mittelpunkt stehen müssen, nicht zuletzt natürlich wegen der ärztlichen Verschwiegenheit. Hierdurch entstehen unglaublich viele Reibungspunkte zwischen dem Datenschutz, wie er in der Theorie gefordert ist und wie er in der Praxis umgesetzt werden sollte bzw. wird – und genau das bedeutet für die Datenschutzbeauftragten, die häufig Einzelkämpfer in ihren Einrichtungen sind, mit fehlenden monetären, zeitlichen und personellen Ressourcen zu kämpfen haben, die Notwendigkeit, gebündelt und zielgerichtet aktuelle und für sie praxisrelevante Informationen zu erhalten. Und genau dies wird Update-BDSG auch zukünftig anbieten.

Im Hinblick auf die GVO wird allerdings bei Gelegenheit das Tagungsformat in „Update-Datenschutz“ umbenannt werden.

Was erwartet Ihrer Meinung nach das Gesundheitswesen in Bezug auf die EU-DSGVO?
Die DSGVO tritt am 25.5.18 ohne weitere Übergangsfrist in Kraft und wird sofort von den Aufsichtsbehörden angewendet. Im Vergleich zum Bundesdatenschutzgesetz enthält sie etliche neue Begriffe, neue Verfahrensregeln und einige Verschärfungen, wie beispielsweise höhere Bußgelder. Auch die Regeln für medizinische Forschung sind nun zum Teil neu. Die GVO wird auch den Inhalt der Datenschutzregeln bestimmen, die für den Gesundheitsbereich zahlreich neben dem bisherigen BDSG in Sondergesetzen vorhanden sind und zur entsprechenden Anpassung anstehen, wie z. B. die Krankenhausgesetze der Länder.

Die rechtskonforme Anwendung der GVO verlangt eine sehr frühzeitige Einarbeitung in die komplizierte Rechtsmaterie. Nur so kann mit einer rechtzeitigen Umstellung der internen Verwaltungsprozesse begonnen werden. Offen ist, wann mit den erwähnten novellierten Sonderregelungen gerechnet werden kann, der kommende Bundestagswahlkampf erzeugt jedenfalls Zeitdruck.

ISDSG: Sind bereits Tagungen zur Datenschutzgrundverordnung geplant?
Da der Text der GVO seit Frühjahr 2016 bekannt ist, konnte er in einigen Symposien bundesweit schon intensiver beleuchtet werden. Auch die jetzt geplanten Tagungen „Datenschutz in der Medizin Update-BDSG" am 10.11.16 in Berlin und „Datenschutz im Pflegebereich“ am 15.11.16 in Mainz werden die GVO in den Fachvorträgen gebührend behandeln. Nur so können wir unsere Teilnehmer auf der Basis der jeweils schon bekannt gewordenen Neuerungen auf den 25.5.2018 ausreichend vorbereiten.

ISDSG: Darüber hinaus ist aber noch ein anderes Veranstaltungsformat geplant.
Richtig. Gemeinsam mit der Agentur esturias und dem ISDSG entwickele ich aktuell ein Seminarangebot, das sich unter dem Namen Update-Datenschutz mit der EU-DSGVO beschäftigt, um das Gesundheitswesen wirklich fit für die Praxis zu machen. Es soll umfangreiches Grundlagenwissen aus der GVO vermitteln und zugleich die neuen Aspekte im Gesundheitsbereich analysieren und erläutern.

Die Zeit bis zum 25.5.2018 darf unter gar keinen Umständen von den Datenschutzbeauftragten im Gesundheitswesen verschlafen werden, damit die Umstellung überhaupt funktionieren kann. Wir wollen die inhaltlich gleichen, wahrscheinlich zweitägigen Seminare in fünf Großstädten anbieten: Hamburg, Köln, Frankfurt, Berlin und München, namhafte Fachleute werden uns dabei als Dozenten zur Verfügung stehen. Die genauen Termine, das Programm und die Anmeldemöglichkeiten werden im Herbst unter www.isdsg.de und www.esturias.de publiziert werden. ■

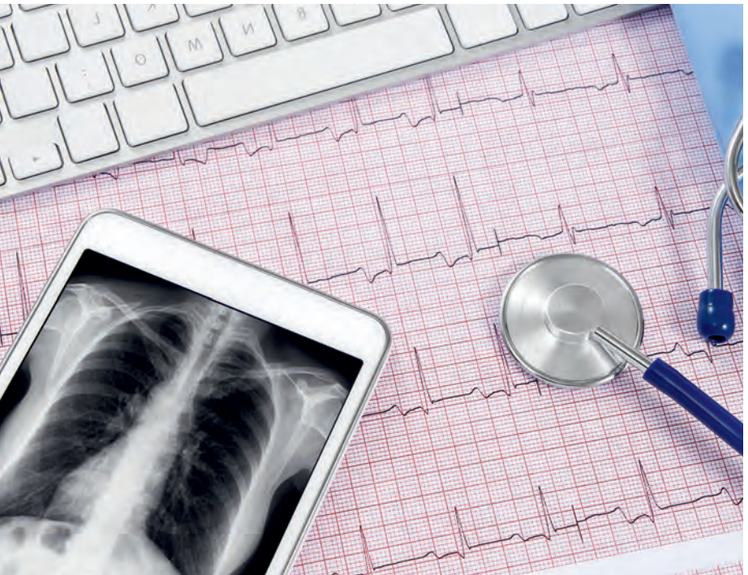
Interview: Nina Richard

Ein Datenschutz-Zertifikat ermöglicht den Austausch von Patientendaten

Da Patientendaten ein begehrtes Gut sind, müssen sie jederzeit geschützt sein – auch wenn sie digital von einer medizinischen Einrichtung zur anderen verschickt werden. Zu beurteilen, ob der dafür beauftragte Dienst den Sicherheitsansprüchen im Gesundheitswesen entspricht, gehört nicht zu den Kernkompetenzen von Medizinern. Datenschutz jedoch zählt zu den Verantwortungen der Leitung einer medizinischen Einrichtung. Jetzt hilft ein Datenschutz-Zertifikat bei der Auswahl der geeigneten Dienste.

Befunde, Krankenakten, Notfalldaten, verordnete Anwendungen oder Medikamente: Die neue elektronische Gesundheitskarte soll in den nächsten Jahren zu einem wichtigen Datenträger im Gesundheitswesen in Deutschland werden. Klagen Patienten über Herzprobleme, leiden unter Diabetes oder Depressionen – Ärzte, Kassen und Krankenhäuser speichern ihre Diagnosen heute bereits digital. Fallakten werden angelegt und Labordaten über IT-Systeme übertragen. Dadurch lassen sich der Arztbesuch oder die Behandlung im Krankenhaus effizienter gestalten, Therapien besser koordinieren. Doch es lauern Gefahren: Tauschen die medizinischen Einrichtungen diese Daten über das Internet mit externen Ärzten oder Diensten aus, sind die Daten oft ungeschützt. Patientendaten aber sind begehrt: Studien zum Gesundheitswesen in den USA zeigen, dass auf dem Internet-Schwarzmarkt bereits jede Menge Patientendaten gehandelt werden – zu einem Preis, der höher liegt als der für Kreditkartendaten.

Auch hierzulande vernetzen sich Pflegeheime und Kliniken mit externen Einrichtungen: dem Medizinischen Dienst z. B. oder den Krankenkassen. Daher gilt: Nur eine Einrichtung, die ausreichenden Datenschutz bietet, behält das Vertrauen der Patienten, Mitarbeiter und Geschäftspartner. Die Realität im deutschen Gesundheitswesen ist heute jedoch noch nicht zufriedenstellend. In der Studie „European Hospital Survey – Benchmarking Deployment of eHealth Services" der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers werden die Sicherheitslücken deutlich: Nur 40 Prozent der deutschen Krankenhäuser verschlüsseln ihre Systeme, um Patientenakten zu schützen. Nur eines von fünf Krankenhäusern verfügte über ein ausreichendes Datensicherungssystem und jede dritte Klinik konnte erst einen Tag nach einem Systemausfall die Daten wiederherstellen.



Verschärfte Strafen in neuem Gesetz

Allerdings erschweren stetig wachsende Anforderungen durch den Gesetzgeber das Einhalten von Datenschutzbestimmungen. So müssen sich medizinische Einrichtungen nicht nur an das Bundesdatenschutzgesetz (BDSG) halten, sondern seit 2015 auch den Anforderungen des IT-Sicherheitsgesetzes (IT-SiG) gerecht werden. Dadurch sind sie verpflichtet, bestimmte technische und organisatorische Sicherheitsanforderungen einzuhalten. Zudem müssen laut IT-SiG, Ausfälle und Störungen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden. Verstöße werden mit einer Strafe von bis zu 100.000 Euro geahndet.

> *Nur wer einen ausreichenden Datenschutz bietet, behält das Vertrauen der Patienten, Mitarbeiter und Geschäftspartner.*

Die Kontrolle darüber erfolgt alle zwei Jahre durch Audits und Zertifizierungen.

Sollte es tatsächlich zu einem Datenverlust kommen, trägt stets der Leiter oder die Geschäftsführung der medizinischen Einrichtung die Verantwortung. Bei grob fahrlässigen Fehlern kann sogar die Geschäftsführung persönlich belangt werden. Da könnte das richtige Datenschutz-Zertifikat helfen, eines das rechtlich anerkannt wird.

Gesammeltes Expertenwissen

Zwei Jahre lang entwickelten Experten im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) ein solches Datenschutz-Zertifikat. Ziel war es, Unternehmen ein Instrument in die Hand zu geben, mit dem sie Internet-Dienste (Cloud-Dienste) schnell und fundiert hinsichtlich ihrer Datensicherheit beurteilen können. Mit dem Zertifikat soll sich die Prozedur der Auswahl vereinfachen, im Falle, dass eine Einrichtung einen Cloud-Dienst beauftragen will.

Grundlage dieses Datenschutz-Zertifikats ist das 2015 entwickelte Trusted Cloud Datenschutzprofil (TCDP), ein Anforderungskatalog, der auf anerkannte Standards (z. B. ISO 27018) aufbaut. Dieser erfüllt alle datenschutzrechtlichen Vorgaben für die Auftragsverarbeitung in der Cloud. An der Entwicklung des Profils waren unter der Leitung der TÜV Informationstechnik GmbH (TÜViT) Vertreter aller maßgeblichen Akteure beteiligt, darunter:

- Mehrere Datenschutzaufsichtsbehörden: unter anderen der Bundesdatenschutzbeauftragte, Datenschutz Berlin, ULD, Datenschutz Brandenburg, Nordrhein-Westfalen, Bayern
- Anbieter und Anwender von Cloud-Diensten: z. B. der Telekom, regioIT, Uniscon, SAP
- Verbände wie der Branchenverband BitKOM und Eurocloud
- Ministerien: darunter das Bundesministerium des Inneren (BMI) und das BMWi
- Stiftungen und Ämter des Bundes, Standardisierungsorganisationen: z. B. das Bundesamt für Sicherheit in der Informationstechnologie (BSI), die Stiftung Datenschutz, das Deutsche Institut für Normung (DIN e. V.)
- Unternehmen aus den Bereichen der IT-Auditierung: unter anderen der TÜV Süd, TÜV Nord, TÜV Rheinland.

Das Zertifikat bezieht sich explizit auf den Datenschutz und die Datensicherheit einer Public Cloud – also eines Dienstes, der Leistungen über das Internet anbietet. Es standardisiert die Anforderungen des Datenschutzes einschließlich der allgemeinen Informationssicherheit. Damit potenzielle Cloud-Nutzer eine Wahl zwischen verschiedenen Diensten treffen und den Grad an Datensicherheit beurteilen können, brauchen sie eine Vergleichsmöglichkeit. Hierfür sieht das Zertifikat nach dem TCDP Schutzklassen vor, die auf den unterschiedlichen Schutzbedarf einzelner Unternehmen eingehen. Die Schutzklassen ergeben sich aus den technischen und organisatorischen Maßnahmen, die der Dienst zum Schutz der Daten und für die IT-Sicherheit umsetzt. Die Schutzklassen erleichtern den Cloud-Nutzern grundsätzlich die Wahl und unterstützen sie dabei, die von den Datenschutzgesetzen geforderten Kontrollpflichten zu erfüllen.

> *Für personenbezogene Daten kommt nur ein Dienst infrage, der mit der höchsten Schutzklasse 3 zertifiziert ist.*

Für Patientendaten – personenbezogene Daten – kommt nur ein Dienst infrage, der mit der höchsten Schutzklasse, Schutzklasse 3, zertifiziert ist. Falls aber die medizinische Einrichtung schon mit anonymisierten Daten arbeitet, vermindert sich die benötigte Datenschutzklasse. Um die Ermittlung der passenden Schutzklasse zu erleichtern, stellt die Stiftung Datenschutz einen Schutzbedarfsrechner zur Verfügung. Beauftragt die Leitung eines Krankenhauses dann z. B. einen Dienst, der mit jener Schutzklasse zertifiziert ist, die dem Schutzbedarf der Daten entspricht, sind die Haftungsrisiken für die Verantwortlichen erheblich verringert. Denn in diesem Fall gelten die Kontrollpflichten vor dem Gesetz als erfüllt.

Nähere Informationen zum Zertifikat nach dem TCDP:

- **www.trusted-cloud.de**
- **stiftungdatenschutz.org/?s=schutzbedarfsrechner**
- **www.idgard.de/service/downloads/datenschutzzertifizierung-von-cloud-diensten** ■

Claudia Seidl

AMEOS-Vorstandsmitglied
Michael Dieckmann

Herausforderungen für die Pflegebranche – gut aufgestellt für die Zukunft

Im Gesundheitswesen ist der demografische Wandel besonders zu spüren. Dem zunehmenden Anteil betagter Menschen in der Gesellschaft stehen eine erhöhte Nachfrage an Pflegefachkräften, der sinkende Anteil erwerbstätiger Pflegefachkräfte sowie der Mangel an Bewerbungen gegenüber. Dazu kommen die sich ständig verändernden informations- und kommunikationstechnischen Anforderungen an sämtliche Ebenen der Gesundheitsbranche.

„Der Pflegesektor ist der Jobmotor der Zukunft" so formulierte die Bundesagentur für Arbeit im Herbst 2013 in ihrem Arbeitsmarktbericht. Dass die Pflege eine Zukunftsbranche ist, darüber sind sich Experten einig. Aber auch über die Herausforderungen, die damit verbunden sind. Wer soll zukünftig die Patienten pflegen? Wie kann man junge Menschen für eine Tätigkeit im Gesundheitswesen motivieren? Einerseits der demografische Wandel, der steigende Anteil betagter Menschen in der Gesellschaft, die dadurch erhöhte Nachfrage an Pflegefachkräften, der sinkende Anteil erwerbstätiger Pflegefachkräfte, der Mangel an Bewerbungen. Andererseits ist eine weitere Herausforderung die vehement zunehmende Digitalisierung auf sämtlichen Ebenen der Gesundheitsbranche. Nicht nur entsprechende Kompetenzprofile der Pflegekräfte werden gefordert (z. B. die Anwendung von IT-Software), sondern auch der sensible Umgang mit Gesundheitsdaten.

> *Arbeitsplätze im Gesundheitswesen sind unabhängig von wirtschaftlichen Schwankungen und deshalb krisenfest und zukunftssicher.*

Die Statistiken sind eindeutig

Das Thema Datensicherheit spielt somit, auf Grundlage der sich ständig (weiter-) entwickelnden informations- und kommunikationstechnischen Anforderungen, eine wichtige Rolle. Die Arbeitsplätze im Gesundheitswesen – insbesondere der Altenpflege – sind unabhängig von wirtschaftlichen Schwankungen und deshalb krisenfest und zukunftssicher. Doch um dem wachsenden Personalbedarf gerecht zu werden, müssen Menschen für Berufe in der Pflege gewonnen werden. Hier stellt sich die Frage, ob die Gesundheitsberufe attraktiv genug sind, ausreichend Bewerberzahlen zu generieren. Nach einer Umfrage des Krankenhaus-Barometers aus dem Jahr 2013 haben 34 Prozent der Krankenhäuser Probleme, offene Stellen im Pflegedienst für die Normalpflege zu besetzen. Verglichen mit den Zahlen aus dem Jahr 2009 (16 Prozent) hat sich der Anteil der Krankenhäuser mit Personalengpässen im Pflegedienst innerhalb von vier Jahren verdoppelt. Zudem hat die Umfrage ergeben, dass Einrichtungen unter 300 Betten am stärksten vom Fachkräftemangel in der Pflege betroffen sind. Hier konnten 40 Prozent der Krankenhäuser vakante Stellen in der Pflege nicht besetzen. Insbesondere die Intensivpflege ist betroffen.[1]

Berechnungen des Statistischen Bundesamtes aus dem Jahr 2010 haben ergeben, dass der demografische Wandel langfristig zu einem Personalmangel in den Pflegeberufen führt. Im Jahr 2025 werden laut Prognose 125.000 Beschäftigte fehlen.[2]

Qualifizierte Nachwuchskräfte

Das Forschungsinstitut Betriebliche Bildung hat ermittelt, dass 56 Prozent der befragten Pflegedienstleitungen angeben, dass das erfahrene Personal ein hohes Durchschnittsalter aufweist. 59 Prozent rechnen mit zunehmenden Leistungseinschränkungen und Fehltagen angesichts des erwartbaren Altersanstiegs der Pflegekräfte.[3] „Das durchschnittliche Rentenzugangsalter für Gesundheitsdienstberufe liegt derzeit bei 58,5 Jahren (Männer: 59,7, Frauen: 58,2).Fest steht: Die Mehrheit der Pflegenden vollerwerbstätig und vollerwerbsfähig erreicht nicht einmal das 60. Lebensjahr."[4]

Aufgrund dieses Fachkräfteengpasses ergeben sich für Interessierte in der Pflegebranche vielfältige Beschäftigungsmöglichkeiten. Junge Fachkräfte können sich angesichts des Personalmangels häufig aussuchen, wo und bei wem sie arbeiten möchten. Um sich als attraktiver Arbeitgeber im Gesundheitsbereich zu positionieren, ist ein gezieltes Personalmarketing erforderlich.

> *Junge Fachkräfte können sich angesichts des Personalmangels häufig aussuchen, wo und bei wem sie arbeiten möchten.*

Dadurch, dass viele neue und verantwortungsvolle Aufgaben in den vergangenen Jahren in den Pflegeberufen hinzugekommen sind, differenzieren und spezialisieren sich die Berufsbilder in der Gesundheits- und Krankenpflege immer stärker. Eine Folge davon ist, dass seit einigen Jahren über die Notwendigkeit der Akademisierung der Pflegeberufe diskutiert wird. Aufgrund dieser Entwicklungen ist damit zu rechnen, dass in Kliniken zukünftig zunehmend akademisch qualifizierte Pfleger Aufgaben übernehmen werden.

Deshalb hat die AMEOS Gruppe bei der Gestaltung neuer Tätigkeitsprofile innovative Wege eingeschlagen. Ärzte werden zukünftig von akademisierten Pflegerinnen und Pflegern unterstützt, die für Spezialaufgaben wie Dokumentation, Planung, Nachsorge oder Belegungs- und Entlassungsmanagement zuständig sind. Ein Belegungsmanager ist z. B. dafür verantwortlich, die Betten auf den Stationen zuzuteilen, Aufnahmetermine zu steuern und für eine gleichmäßige Auslastung der OP-Kapazitäten zu sorgen. Ein Entlassmanager organisiert zum Beispiel alles Erforderliche für die Zeit nach dem Klinikaufenthalt, wie Nachsorgetermine oder Reha-Maßnahmen. Der Einsatz von Social Media in Unternehmen oder aber technische Entwicklungen, die Mitarbeitern auch außerhalb des Büros den Zugriff auf Unternehmensinterna ermöglichen, spielen eine wachsende Rolle. In Anlehnung an das bereits positionierte Thema Datenschutz stellt sich hier die Frage: Was gilt es, bei der Nutzung und Verarbeitung personenbezogener Daten für Unternehmen und Einrichtungen zu beachten? Diese neuen Aufgaben erfordern eine entsprechende Qualifikation der Mitarbeiter. Um die hierfür erforderliche akademische Qualifizierung sicherzustellen, arbeitet die

> *Ärzte werden zukünftig von akademisierten Pflegerinnen und Pflegern unterstützt, die für Spezialaufgaben zuständig sind.*

AMEOS Gruppe mit der FOM Hochschule zusammen.

Von großer Bedeutung ist das Angebot eines dualen Studiums für Auszubildende. Durch diese Verbindung von Studium und klassischer Pflegeausbildung sollen junge Menschen für Pflegeberufe begeistert werden. Gleichzeitig möchte man so den vorhandenen Mitarbeitern neue Chancen und Entwicklungsmöglichkeiten bieten.

> *Durch die Verbindung von Studium und klassischer Pflegeausbildung sollen junge Menschen für Pflegeberufe begeistert werden.*

Was in anderen Wirtschaftsbereichen seit vielen Jahren gängige Praxis ist, bedeutet für die Pflegebranche ein Novum. Mit dem Angebot eines dualen Studiums hofft die AMEOS Gruppe, auch vermehrt (Fach-) Abiturienten für die Pflegebranche gewinnen zu können. Ein Erfolgsbeispiel dieses Modells ist das AMEOS-Klinikum Hildesheim, wo die Zusammenarbeit mit der FOM Hannover bereits vor einem Jahr begonnen hat. Dort ist seitdem ein Anstieg an Bewerbungen von Abiturienten zu verzeichnen.

Flexible Arbeitszeitgestaltung

Um Studium und Ausbildung noch enger aufeinander abzustimmen, gibt es eine Vielzahl an Möglichkeiten zur Arbeitszeitgestaltung. Das Studium an der FOM findet wahlweise abends und an den Wochenenden, im Tages- oder Blockstudium statt. So wird die praktische Ausbildung in den Pflegefachschulen durch das Studium an der FOM nicht beeinträchtigt, sondern um akademisches Know-how ergänzt. Die Inhalte des Studiums werden in enger Absprache mit den Pflegeschulen konzipiert und abgestimmt. So sind Themen aus der Pflegeausbildung optimal in das Studien-Curriculum eingepasst. Im bilateralen Austausch zwischen der Hochschule und den Pflegefachschulen werden bestimmte Studienmodule in Kooperation mit den Pflegefachschulen durchgeführt. Die AMEOS Gruppe geht in Bezug auf die akademische Qualifizierung der Mitarbeiter noch einen Schritt weiter, denn sie hat mit der FOM das Konzept eines „akademischen Lehrkrankenhauses Pflege“ initiiert. Bisher gab es das Konzept des akademischen Lehrkrankenhauses nur in der medizinischen Ausbildung. Dieses bewährte Modell

> *Gemeinsames Ziel ist es, Lehrstandards für ein praxisbezogenes Pflegestudium zu etablieren und den Wissensaustausch zu fördern.*

übertragen die FOM Hochschule und die AMEOS Gruppe nun auch auf den Bereich der Pflege. Diese innovative Herangehensweise verstärkt den Theorie-Praxis-Transfer. Gemeinsames Ziel ist es, Lehrstandards für ein praxisbezogenes Pflegestudium zu etablieren und den Wissensaustausch zu fördern. Die Zusammenarbeit beinhaltet die Durchführung von realen Studienprojekten in Kliniken, den fachlichen Austausch mit dem Pflegepersonal vor Ort sowie den regelmäßigen Besuch von Praktikern als Gastreferenten in den Vorlesungen.

Auf Erfolg programmiert.

Wir bringen Sie im Bereich der Healthcare-IT auf die Gewinnerstraße. Profitieren Sie von unserer erstklassigen Software für den deutschsprachigen Gesundheitsmarkt und von ganzheitlichen Lösungen für Klinik, Labor und Radiologie aus der Hand eines Mittelständlers.
agil – intelligent – kundenorientiert – effizient

Erfahren Sie mehr auf www.i-solutions.de

i-SOLUTIONS HEALTH

Die FOM bietet zurzeit im Gesundheitsbereich die berufs- und ausbildungsbegleitenden siebensemestrigen Bachelorstudiengänge „Gesundheits- und Sozialmanagement“ sowie „Gesundheitspsychologie & Pflege“ an. Masterstudierende können den viersemestrigen Studiengang „Public Health“ studieren. Weitere Bachelorstudiengänge mit fachspezifischen Inhalten, wie Pflegemanagement, Angewandte Pflegewissenschaften, aber auch Gesundheitspsychologie/Medizinpädagogik sind in Planung und sollen im Herbst 2017 angeboten werden. Auch für bereits ausgebildete Pflegerinnen und Pfleger besteht die Möglichkeit, ein berufsbegleitendes Studium an der FOM zu absolvieren. Ihr Vorteil: Erbrachte Leistungen aus vorherigen Fort- und Weiterbildungen, z. B. im Bereich des Wundmanagements, können auf das Studium angerechnet werden. Dies ermöglicht erfahrenen Pflegefachkräften, den Studienabschluss schneller zu erreichen.

Kooperation

„Auf eine ausgezeichnete Fachausbildung legen wir größten Wert“, so AMEOS-Vorstandsmitglied Michael Dieckmann. „Mit der Kooperation zwischen AMEOS und der FOM setzen wir ein klares Zeichen für eine Verbesserung der Aus- und Weiterbildung unserer Mitarbeitenden und die Gewinnung der Nachwuchskräfte. In der Pflegebranche finden erhebliche demografische Veränderungen statt, die in den

> *Die Menschen werden immer älter, sodass die Nachfrage nach Pflegeleistungen kontinuierlich steigen wird.*

nächsten Jahren zu einem Fehlen qualifizierter Pflegefachkräfte führen werden. Auf der anderen Seite werden die Menschen immer älter, sodass die Nachfrage nach Pflegeleistungen kontinuierlich steigen wird. Als attraktiver Arbeitgeber bieten wir unseren Mitarbeitern interessante Perspektiven, damit sie sich stetig weiterqualifizieren können. Das duale Studium, das unser Partner seit mehreren Jahren erfolgreich anbietet, schränkt die praktische Ausbildung nicht ein, sondern verbindet vielmehr Theorie und Praxis. Den bei staatlichen Hochschulen vorhandenen Trend zur vollständigen Verlagerung der Pflegeausbildung in die Hochschule beobachten wir mit Sorge, weil praktische Aspekte zu kurz kommen.“

Nachwuchskräfte gewinnen durch Aus- und Weiterbildung.

„Die FOM verfügt mit ihren speziell auf den Gesundheitssektor abgestimmten Studiengängen über umfangreiche Erfahrungen“, so Dr. Harald Beschorner, Kanzler der FOM. „Insbesondere der gelungene Theorie-Praxis-Transfer ist für die FOM zentrales Element für den Studien- wie beruflichen Erfolg. Im Rahmen der Kooperation mit AMEOS möchte die FOM das Konzept des akademischen Lehrkrankenhauses in der Pflege gemeinsam umsetzen, um diesen Transfer zu institutionalisieren. Dazu gehört die enge Abstimmung mit den Lehrkräften, angelehnt an die individuellen Bedarfe der Pflegebranche.“ ■

Michael Dieckmann

[1] Blum K./Löffert, S./Offermanns, M./Steffen, P. (2011): Krankenhaus-Barometer Umfrage 2013, Deutsches Krankenhausinstitut e. V.
[2] Statistisches Bundesamt, Wirtschaft und Statistik, 11/2010.
[3] Forschungsinstitut Betriebliche Bildung, 2010.
[4] DBfK Zahlen-Daten-Fakten, 2010.

Über AMEOS

Die AMEOS Gruppe zählt zu den bedeutenden Gesundheitsdienstleistern im deutschsprachigen Raum. Die Gruppe mit Sitz in Zürich wurde 2002 mit dem Ziel gegründet, Krankenhäuser zu übernehmen, diese zu sanieren und für sie eine langfristige Perspektive zu entwickeln. Zur AMEOS Gruppe gehören mittlerweile 68 Einrichtungen an 38 Standorten mit über 12.000 Mitarbeitenden. Die Krankenhäuser, Pflege- und Eingliederungseinrichtungen sowie Polikliniken verbinden hochwertige medizinische und pflegerische Leistungen mit Qualität und Menschlichkeit. Sie bieten der breiten Bevölkerung in regionalen Netzwerken – den AMEOS Regionen – eine umfassende medizinische und pflegerische Versorgung. Weitere Informationen: **www.ameos.eu**

Über die FOM

Mit über 35.000 Studierenden ist die FOM die größte private Hochschule Deutschlands. Sie bietet Berufstätigen und Auszubildenden an bundesweit 28 Hochschulzentren die Möglichkeit, berufsbegleitend praxisorientierte Bachelor- und Masterstudiengänge aus den Bereichen Wirtschaftswissenschaften, Gesundheit und Soziales, IT-Management sowie Ingenieurwesen zu absolvieren. Getragen wird die FOM von der gemeinnützigen Stiftung BildungsCentrum der Wirtschaft mit Sitz in Essen. Die Hochschule ist vom Wissenschaftsrat akkreditiert und hat von der FIBAA Anfang 2012 das Gütesiegel der Systemakkreditierung verliehen bekommen – als erste private Hochschule Deutschlands.
Weitere Informationen:
www.fom.de

So stärken Sie das Vertrauen Ihrer Patienten

Der Datenschutzbeauftragte hat in Bezug auf den Patientendatenschutz eine verantwortungsvolle Aufgabe. Denn nur durch ihn kann der Stellenwert des Datenschutzes erhöht werden.

Der Datenschutz sollte für Ihre Patienten transparent gestaltet werden.

In Einrichtungen des Gesundheitswesens werden große Mengen von Gesundheits- und Sozialdaten erhoben, verarbeitet und genutzt. Der Patientendatenschutz spielt dabei eine vordringliche Rolle. Die Anfänge des Patientendatenschutzes sind bereits auf Hippokrates im Jahr 400 v. Chr. zurückzuführen und bis heute gültig. Er bildet die Basis für einen vertrauensvollen Umgang zwischen Behandelnden und Patienten sowie der alltägliche Arbeit des Datenschutzbeauftragten – denn seine Aufgabe ist es, das Vertrauen zwischen behandelnden, betreuenden Personen und Patienten zu stärken.

Patientendatenschutz im Alltag leben

Der Schutz personenbezogener Patienten- oder Gesundheitsdaten sollte eine Selbstverständlichkeit sein – so die Theorie. Das Thema Patientendatenschutz ist zunehmend auch ein Thema der Öffentlichkeit geworden – gleichzeitig schwindet mit der zunehmenden Digitalisierung aber auch die Selbstbestimmung des Patienten. Vielen Patienten ist nicht bewusst, was mit den von verschiedenen Stellen erhobenen Daten geschieht – weder bei der selbstbetriebenen Health-App auf dem eigenen mobilen Endgerät noch während oder nach einer Behandlung im Krankenhaus. Der Datenschutzbeauftragte ist deshalb nicht nur Paragrafenkenner, sondern auch Partner von Patienten, um für deren Rechte einzustehen und Transparenz aufzuzeigen.

Transparenz schaffen

Transparenz kann geschaffen werden, indem offen kommuniziert wird. Der DSB kann hier, zusammen mit anderen Abteilungen, den Behandlungsvertrag so entwickeln, dass die Patienten bereits während des Aufnahmeprozesses über die erhobenen Daten informiert werden. Am besten eignen sich hierzu Informationsblätter, die dem Behandlungsvertrag beiliegen. Es sollte z. B. erläutert werden, warum die Erhebung bestimmter Daten notwendig ist, welche Labore oder Ärzte die Daten übermittelt bekommen und welche Konsequenzen es haben kann, wenn Patienten einer Erhebung und anschließenden Verarbeitung und Übermittlung von Daten nicht zustimmen.

Hand in Hand arbeiten

Datenschutz gilt häufig als Störfaktor im Krankenhausalltag. Auf den ersten Blick nimmt er sowohl monetäre als auch zeitliche Ressourcen in Anspruch, was strategischen Zielen der Unternehmensleitung, wie beispielsweise Kostenreduzierung, entgegensteht. Der Datenschutzbeauftragte kann das ändern. Denn er hat die Möglichkeit, Datenschutz praxis- und alltagstauglich umzusetzen und als starker Partner Hand in Hand mit Mitarbeitern zu agieren. ■

Nina Richard

5. Goldene Regel: Schulen Sie die Pforte

Der zentrale Dreh- und Angelpunkt eines jeden Krankenhauses: Paketdienstleister, Kuriere, Patienten, Angehörige, Ärzte und Kollegen – sie alle müssen an ihr vorbei. Die Rede ist von der Krankenhauspforte, die einen elementaren Stellenwert einnimmt. Ein stressiger Job, bei dem dann auch noch das Thema Datenschutz hinzukommt. Wie schnell sind hier Informationen an die falsche Person weitergegeben bzw. was darf eigentlich an wen weitergegeben werden?

Rechtliche Grundlagen, die eindeutige Regelungen festhalten, sucht man als Datenschutzbeauftragter vergeblich. Dennoch existieren einige Arbeits- und Orientierungshilfen, die der Interpretation einzelner Situationen dienen.

Auskünfte an Besucher

Grundsätzlich gilt für die Krankenhauspforte das Patientengeheimnis. Häufig ist es aber im Interesse des Patienten, dass Besucher seinen Aufenthaltsort erfahren. Deshalb kann von einer stillschweigenden Zustimmung zur Auskunftserteilung ausgegangen werden , sofern kein konkretes Auskunftsverbot vorliegt – so die Empfehlung des ULD. In Krankenhäusern mit kirchlicher Trägerschaft darf dem Gemeindepastor/-pfarrer Auskunft über den Patienten erteilt werden.

Technische Maßnahmen – OH-KIS

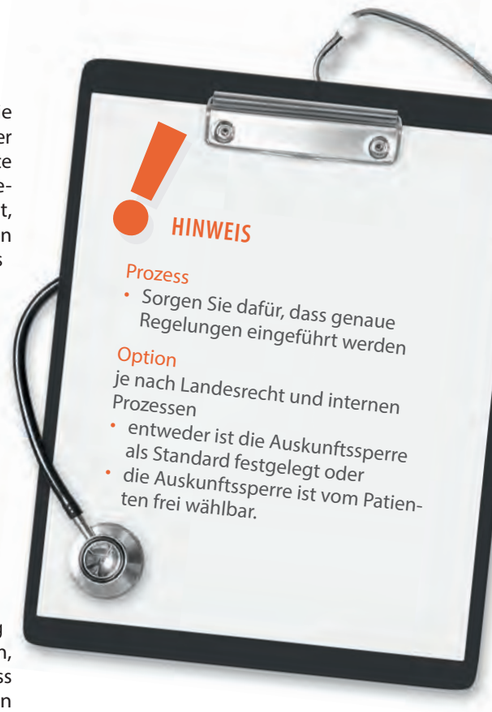
Hier heißt es, dass das Krankenhaus die Möglichkeit vorsehen muss, Auskünfte über den Patientenaufenthalt durch die Pforte sperren zu lassen. Wie die genaue Ausgestaltung dieser Sperrung auszusehen hat, hängt vom Einzelfall ab. Als Möglichkeiten werden genannt: Die Sperrung könnte als technische Regel eingerichtet sein und eine Aufhebung der Einwilligung bedürfen oder aber auch eine Widerspruchslösung genügen. Hier gilt es für den DSB, immer die Landesgesetze zu prüfen.

Auch wird für die technische Umsetzung darauf hingewiesen, dass die jeweilige Fallakte ein Kennzeichen aufnehmen könnte, aus dem hervorgeht ob und wann für den Patienten eine Auskunftssperre greift.

Handlungsempfehlungen

Wir empfehlen, eine bestimmte Regelung für Auskünfte an der Pforte zu etablieren, um hier auf Nummer sicher zu gehen, dass keine unbefugten Dritte Informationen erhalten. Ein Prozess, der sich in der Praxis bewährt hat, ist die Nennung der Station des Patienten. Auf der Station soll der Besucher sich für weitere Angaben, wie die Zimmernummer, an das Pflegepersonal wenden. Auch die Auskunft an den Pfarrer sollte nur bei explizitem Wunsch des Patienten erfolgen. Mitarbeitern, die als Patienten im Krankenhaus behandelt werden, oder VIPs ist die Auskunftssperre als Standardfall einzurichten. Für alle weiteren Auskünfte sollten die Mitarbeiter der Pforte auf eine andere berechtigte Stelle (z. B. Verwaltung) verwiesen werden. Auch sollten an der Pforte keine weiteren Informationen eingesehen werden, die den Namen und die Station bzw. Zimmernummer überschreiten. Ausnahmeregelungen gelten natürlich dann, wenn die Pforte auch andere Funktionen erfüllt. ■

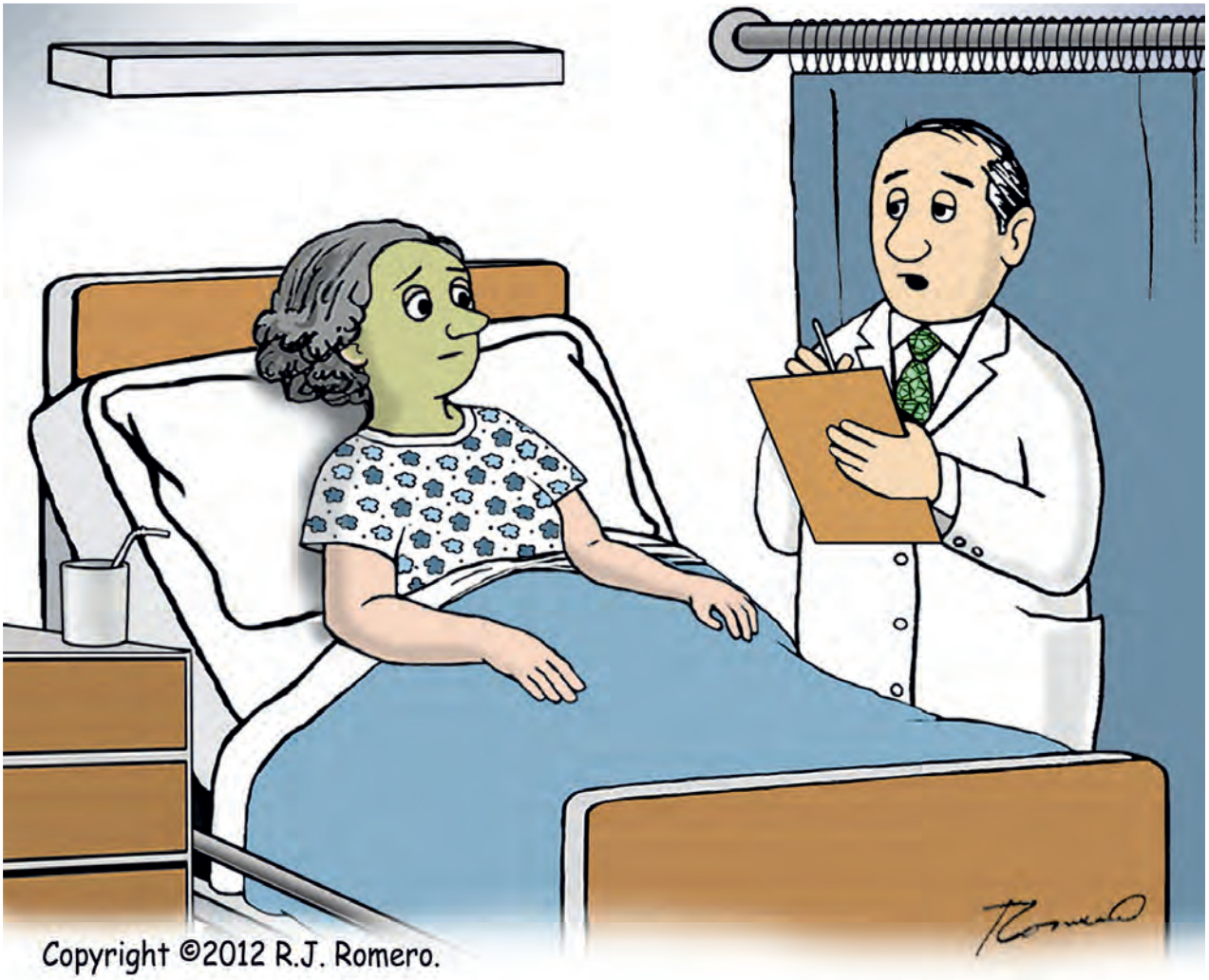
Nina Richard



Impressum

ExperSite Ausgabe 02 2016 | ISSN-Print 2364-5636 | ISSN-Internet 2364-5644 | **Herausgeber:** ISDSG – Ein Dienstleistungsbereich der DATATREE AG Datatree AG, Heubesstraße 10, 40597 Düsseldorf, T +49 211 93190-700, F +49 211 93190-799, office@datatree.eu, www.datatree.eu | **Sitz der Gesellschaft:** Düsseldorf | **Registergericht:** Amtsgericht Düsseldorf | **Registernummer:** HRB 66132 | **Umsatzsteuer-Identifikationsnummer:** DE 279402614 | **Vorstand:** Prof. Dr. Thomas Jäschke | **Vorsitzender des Aufsichtsrates:** Prof. Dr. Julius Reiter | **Inhaltlich Verantwortlicher gemäß § 1 Abs. 4 TMG, § 55 Abs. 1 RStV und § 55 Abs. 2 RStV:** Prof. Dr. Thomas Jäschke | **Redaktionsleitung:** Nina Richard | **Editorial Design u. Umsetzung:** c74 gestaltung & design, C. Robrahn, Dortmund, www.c74.org | **Druck:** Druckerzeugnisse Gerbrunn | **Auflage:** 5.000 | **Fotos:** Titel: iStock, SKapl; S. 3: iStock, Nikada | shutterstock, Tyler Olson ; S. 3: Falko Wübbecke, Dortmund; S. 4/5: Falko Wübbecke, Dortmund; S.7: Shutterstock, ArtLight Production; S. 8-9: iStock, poba; S. 11: iStock, Nikada ; S. 12: iStock, oonal; S. 14: shutterstock, Den Rise ; S.16: iStock, anilakkus; S. 21: shutterstock, Syda Productions ; S. 22: istock, sturti; S. 23: shutterstock, Tyler Olson ; U4: hipaacartoons, R.J. Romero.

Einblicke & Ausblicke



"Apparently you contracted a virus from your computer, so we had to erase your memory. I trust you had a backup copy?"

Wir bedanken uns für die inhaltlichen Beiträge bei:

Manfred Weitz, Update BDSG | **Claudia Seidl,** Uniscon | **Michael Dieckmann,** AMEOS | **Harald Beschorner**, FOM | **Vanessa Schulz,** FOM

Die nächste Ausgabe erscheint im April 2017

Schwerpunkt: Der Datenschutzaudit – von der Vorbereitung bis zur Durchführung