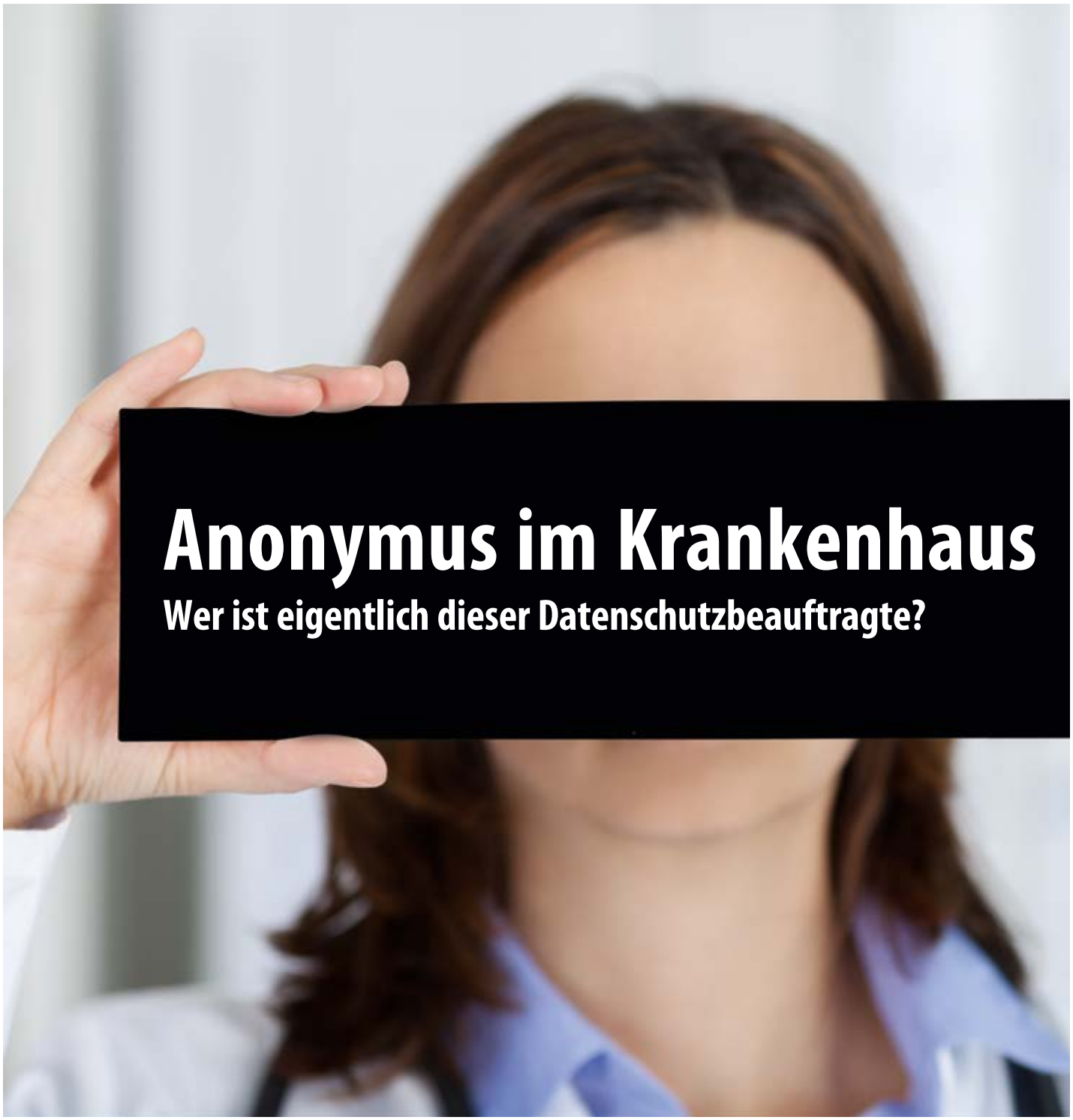
ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Ausgabe 01 2015



Anonymus im Krankenhaus

Wer ist eigentlich dieser Datenschutzbeauftragte?

Interview mit Dr. Bernd Schütze
Über den Datenschutz in Deutschlands Krankenhäusern

Schnittstelle
Datenschutz und Qualitätsmanagement

Der Datenschutzbeauftragte
Pseudobestellung

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

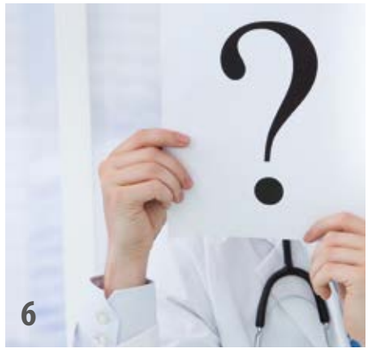
Prof. Dr. Thomas Jäschke
Der Medizin-Wirtschaftsinformatiker ist Experte im Gesundheitssektor und Datenschutzbeauftragter für namhafte Einrichtungen im Gesundheitswesen. Als Institutsleiter ist er der Kopf des ISDSG-Teams.
✉ jaeschke@isdsg.de

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



Nicht immer ist der Datenschutzbeauftragte ein bekanntes Gesicht.

Schnittpunkte von Qualitätsmanagement und Datenschutz.

Der Datenschutzbeauftragte sollte Partner sein.

Das Team 2

Tipps, Fakten & Termine 4

Schwerpunkt

Anonymus im Krankenhaus 6
Wer ist eigentlich dieser Datenschutzbeauftragte?

Gastbeitrag

Qualitätsmanagement und Datenschutzmanagement 10
Organisatorischer Schnittpunkt oder fachliche Notwendigkeit?

Voice

Interview mit Datenschutz-Auditor Dr. Bernd Schütze 12
Über den Datenschutz in Deutschlands Krankenhäusern

Der Datenschutzbeauftragte

Pseudobestellung 14
Wer besser kein Datenschutzbeauftragter werden sollte

Goldene Regeln

2. Goldene Regel: Verschlüsselte Übermittlung von Daten 15
Personenbezogene Daten im Alltag

EDITORIAL

Sehr geehrte Leserinnen und Leser,

„Wer ist eigentlich dieser Datenschutzbeauftragte?“ Eine Frage, die sich in Krankenhäusern und Kliniken mit Sicherheit der ein oder andere Patient stellt; aber selbst die eigenen Mitarbeiter kennen ihn häufig nicht, diesen Datenschutzbeauftragten. Auch wenn die Auseinandersetzung mit Pseudonymisierung und Anonymisierung zu seinen täglichen Aufgaben gehört, dürfen diese Eigenschaften nicht auf ihn übergehen. Schneller gesagt als getan, denn nicht immer ist die Position des Datenschutzbeauftragten in klinischen Einrichtungen einfach. Durchsetzungskraft und Einfühlungsvermögen, dies sind nur zwei Eigenschaften, die er zwingend mitbringen sollte, um als Partner von Mitarbeitern und Patienten wahrgenommen zu werden.

Die erste Ausgabe 2015 des Magazins ExperSite beschäftigt sich mit dem „Anonymus Datenschutzbeauftragter“. Wir werden aufzeigen, dass Datenschutz mehr ist als das reine Erfüllen von gesetzlichen Vorschriften. Vielmehr muss dieses Thema von der Organisation gelebt werden, denn Datenschutz betrifft jede Abteilung und jeden einzelnen Mitarbeiter. Unterstützende Ideen erhalten Sie in unserem Experteninterview mit Dr. Bernd Schütze. In unserem Gastbeitrag zeigt Unternehmensberaterin Stephanie Glos die Parallelen zwischen Datenschutz und Qualitätsmanagement sowie deren Verbindung zur Erleichterung im Klinikalltag. Und natürlich haben wir auch wieder Branchennews und Alltagstipps für Sie vorbereitet.

Wir freuen uns auf Ihr Feedback und wünschen Ihnen viel Spaß beim Lesen unserer ersten Ausgabe 2015. ExperSite – Das Magazin für Datenschutz und Sicherheit im Gesundheitswesen.

Ihr

Prof. Dr. Thomas Jäschke
Institutsleiter ISDSG

Europäische Datenschutzverordnung

Die Europäische Datenschutzverordnung soll im Jahr 2015 endlich verabschiedet werden. Nach Bekanntgabe des ersten Entwurfs wird klar: Sie könnte einiges einfacher machen. Hier ein kurzer Abriss zu dem, was das Gesundheitswesen erwarten könnte.

Cloud-Dienste
Die zentrale Speicherung von Daten durch Cloud-Dienste wird auch im Gesundheitswesen zunehmend wichtiger. Unternehmen, die ihren Sitz außerhalb der EU haben, könnten zukünftig dazu verpflichtet sein, die europäischen Datenschutzstandards einzuhalten.

BDSG
Die legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) lässt darauf schließen, dass das Bundesdatenschutzgesetz womöglich komplett ersetzt wird. Möglicherweise sind auch die kirchlichen Regelungen dann hinfällig.

Datenschutzbeauftragter
Die Qualifikation des Datenschutzbeauftragten wird voraussichtlich erstmals gesetzlich festgehalten.

Neues von der eGK

Der Computerchip und das Passfoto auf der eGK sind nicht unzulässig. Das entschied das BSG in seinem Urteil vom 18. November 2014. Das Bild verbessere den Schutz vor Missbrauch, da es der Identifikation des Versicherten diene. Die informationelle Selbstbestimmung des Trägers der Karte werde hierdurch nicht unverhältnismäßig eingeschränkt. Auch die weiteren Funktionen der Karte sind nicht obligatorisch und die dort gespeicherten Daten durch die geltenden Gesetze ausreichend vor unbefugtem Zugriff Dritter geschützt. Ein technischer Mangel des Schutzes könne noch nicht festgestellt werden, da sich die zugehörige Telematik-Infrastruktur noch im Testbetrieb befinde. (Urt. v. 18.11.2014, Az. B 1 KR 35/13 R)

Krankenversicherungen: Daten gegen Prämien

Die mHealth-Bewegung verspricht viel Potenzial zur Unterstützung des Behandlungsprozesses zwischen Patienten und Ärzten. Aktuell vorherrschende sinnvolle Lösungen existieren nur wenige. Als Randbereich der mHealth-Produkte können Fitness-Apps betrachtet werden, die in Verbindung mit Fitnessarmbändern den Aktivitätszustand ihres Trägers analysieren. Berichten zufolge arbeiten Krankenkassen an Programmen, die die Kunden für die Übermittlung ihrer Aktivitätsdaten belohnen. Die Idee dahinter ist simpel: Kunden erhalten Rabatte in Form von Fitnesskursen oder Preisnachlässen, wenn sie beispielsweise eine bestimmte Anzahl von Schritten tätigen und dies auch nachweisen.

Aus Datenschutzsicht könnte dies zulässig sein, vorausgesetzt, die Kunden werden ausführlich und transparent über die Nutzung der Daten informiert und stimmen dem zu.

IT-Sicherheitsgesetz

Die Bundesregierung plant die Verabschiedung eines IT-Sicherheitsgesetzes, das den Schutz kritischer IT-Infrastruktur verbessern soll. Neben der Definition kritischer Infrastruktur (im Wesentlichen geht es um die Versorgung der Bevölkerung) spielen die Veröffentlichung und Meldung von Cyber-Angriffen an das Bundesamt für Sicherheit in der Informationstechnik eine wichtige Rolle. Die DKG (Deutsche Krankenhausgesellschaft) sieht Nachbesserungsbedarf bei der Definition der kritischen Infrastrukturen: So ist der Betrieb eines Krankenhauses nicht direkt gefährdet, weil die IT nicht mehr funktioniert. Offen bleibt auch die Frage nach der Finanzierung des Mehraufwandes für Krankenhäuser.

KOMMENTAR

… zum Entwurf des e-Health-Gesetzes
Der Bundesgesundheitsminister Hermann Gröhe hat am 13. Januar 2015 den für das letzte Jahr angekündigten Referentenentwurf des e-Health-Gesetzes vorgelegt mit dem Ziel, die Qualität und die Wirtschaftlichkeit der medizinischen Versorgung durch den Ausbau und die Nutzung der Telematik-Infrastruktur zu verbessern. Durch entsprechende Vergütungsanreize soll die Telematik-Nutzung attraktiver gemacht werden. Doch wie behandelt der Entwurf die Datentransparenz der Patienten, die durch die Nutzung der Telematik-Infrastruktur immer mehr zu „gläsernen Patienten" werden könnten?

Der Entwurf reicht aus Datenschutzsicht nicht aus. Er verfolgt momentan nur die Absicht, die Telematik-Infrastruktur und die elektronische Gesundheitskarte (eGK) mit Vergütungsanreizen durchzusetzen. Um eine Telematik-Infrastruktur im Gesundheitswesen attraktiv und sinnvoll zu gestalten, ist es notwendig, dass diese genügend Sicherheit und Schutz für die sensiblen Gesundheitsdaten einer Person bietet. Auch könnten mit einem Gesetzesentwurf, der aus Datenschutzsicht Akzeptanz findet, die bisherigen Widerstände gegen die eGK und die Telematik-Infrastruktur ein wenig reduziert werden. Aus Datenschutzsicht ist es äußerst spannend, ob und wie dieser Referentenentwurf weiterentwickelt wird. Den Referentenentwurf können Sie auf unserer Homepage abrufen.

Was ist das ISDSG?

Das ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen in Dortmund ist deutschlandweit aktiv und 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.

BRANCHENTERMINE

conhIT
14.–16. April 2015
Berlin

11. IT-Trends Sicherheit
22. April 2015
Bochum

IT-Trends Medizin
16. September 2015
Essen

Fachsymposium „Datenschutz im Gesundheitswesen"
24. September 2015
Leipzig

Schulungstermine ISDSG
Egal ob Einsteiger oder Profi, bei uns finden Sie die richtige Fortbildung:
- Datenschutz
- IT-Sicherheit
- IT-Recht
- Initialschulung
- persönliches Coaching
- Special-Interest-Veranstaltungen
- Zertifizierter Datenschutzbeauftragter (IOM)

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

Anonymus im Krankenhaus

Der Datenschutzbeauftragte eines Krankenhauses ist nicht selten „der große Unbekannte“. Wie diese Tatsache zum Positiven verändert werden kann und warum eine Veränderung notwendig ist.

Stellen Sie sich einmal vor: Sie sind Datenschutzbeauftragter in einem Krankenhaus und beinahe niemand weiß das. Oder Sie haben als Mitarbeiter[1] in einer Klinik gerade einen Anruf erhalten, dass einem Patienten ein Fax mit vertraulichen Patientendaten eines Unbekannten zugesandt wurden. Und jetzt? Jedes Szenario für sich alleine betrachtet, ist schon kritisch zu bewerten. Treffen beide Szenarien allerdings aufeinander, kann dies negative Konsequenzen haben.

Der Worst Case

Wappnen wir uns für den Fall, dass beide Szenarien aufeinandertreffen und der besagte Mitarbeiter nicht weiß, wem er einen solchen Vorfall melden soll. Den wenigsten Mitarbeitern ist jedoch bewusst, dass bereits ein solches Versehen unverzüglich zu melden ist – und zwar

> *Der Patient, der die falschen Befunde zugeschickt bekommen hat, könnte mit dem anderen Betroffenen in Kontakt treten …*

dem Datenschutzbeauftragten des Hauses. Dieser wird in seiner Rolle die notwendigen, weiterführenden Schritte in die Wege leiten. Ist dem Mitarbeiter nicht bekannt, wer zum Datenschutzbeauftragten der Einrichtung bestellt ist, kann ein solcher Vorfall im hektischen Alltag vergessen werden. Dann muss allerdings mit Konsequenzen gerechnet werden. Der Patient, der die falschen Befunde zugeschickt bekommen hat, könnte versuchen, mit dem anderen Betroffenen in Kontakt zu treten, weil er nichts mehr von dem Krankenhaus gehört hat. Ein weiterer Patient könnte allerdings so erbost darüber sein, dass er dies an die Öffentlichkeit weiterträgt. Neben Ordnungsgeldern, kann ein solcher Vorfall bereits einen erheblichen Imageschaden Ihrer Einrichtung mit sich bringen. Betont sei an dieser Stelle, dass es sich in diesem Beispiel nicht nur um einen Datenschutzverstoß handelt, sondern gleichermaßen um eine Offenbarung des Arzt-Patienten-Geheimnisses nach § 203 des Strafgesetzbuches.

Eine erschreckende Vorstellung, die jedoch häufiger auftreten könnte, als wir zunächst angenommen haben.

Wir haben uns ausführlicher mit dieser Thematik befasst und eine Stichprobe näher betrachtet. Vorweg schicken möchten wir die Anmerkung, dass die Bestellung eines Datenschutzbeauftragten gesetzlich in § 4f des Bundesdatenschutzgesetzes geregelt ist. Diese wird notwendig, wenn in einer öffentlichen oder nichtöffentlichen Stelle personenbezogene Daten automatisiert erhoben, verarbeitet und/oder genutzt werden und mindestens zehn Personen damit betraut sind. Da dieser Umstand auf jedes Krankenhaus zutrifft, sind alle Kliniken demnach verpflichtet, einen Datenschutzbeauftragten ordentlich zu bestellen. Ist dieser aber unter den Mitarbeitern eines Krankenhauses bekannt?

Nachgefragt

Wir haben das getestet und in über 100 Krankenhäusern nachgefragt, ob die Mitarbeiter wissen, wer hausintern für den Datenschutz verantwortlich ist. Nach vielen Minuten in Warteschleifen und zahlreichen Weiterleitungen innerhalb der Einrichtungen wurde letztendlich doch jemand gefunden, der zu wissen glaubte, wer dieser Datenschutzbeauftragte ist. Bei rund 20 Prozent der von uns angerufenen Krankenhäuser konnte unser Telefonpartner nicht ohne mehrfache Umwege sagen, wer innerhalb des Hauses für den Datenschutz zuständig ist. Zwei Kliniken gaben sogar einen Namen an, der allerdings nicht identisch mit dem Namen auf der Homepage in der obligatorischen Datenschutzerklärung der Einrichtung war. Bei fünf Prozent der Krankenhäuser waren Mitarbeiter nicht einmal bereit, eine Information über den Datenschutzbeauftragten herauszugeben – obwohl dies dringend empfohlen wird, um den Patienten und Kunden die Kontaktaufnahme und die Wahrnehmung ihrer Rechte zu ermöglichen.

> *Im Bundesdatenschutzgesetz zählen die Gesundheitsdaten einer Person zu den besonders schützenswerten Informationen.*

Wie kann es sein, so muss man sich fragen, dass der Datenschutzbeauftragte den eigenen Mitarbeitern so unbekannt ist, soll er doch als Ansprechpartner für Betroffene für den Schutz der sensibelsten Daten der Patienten zuständig sein? Zur Erinnerung: Im Bundesdatenschutzgesetz zählen die Gesundheitsdaten einer Person zu den besonders schützenswerten Informationen.

Führen wir uns nochmal einige der zentralen Aufgaben eines Datenschutzbeauftragten vor Augen.[2]

1. **Schaffen von Transparenz** in der Datenverarbeitung. Damit der Datenschutzbeauftragte sich einen Überblick über die Prozesse der Informationsverarbeitung verschaffen kann, sind ihm zwingend Ansprechpartner und Zuständigkeiten mit Kontaktmöglichkeiten zur Verfügung zu stellen.

2. Führen des internen und externen **Verfahrensverzeichnisses.**
   Mindestens die nachstehenden Kriterien sollen dort aufgeführt sein.
   - Name oder Firma sowie Anschrift der verantwortlichen Stelle, >

- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche Vertreter der mit der Datenverarbeitung beauftragten Personen,
- Geschäftszwecke, zu deren Erfüllung die Erhebung, Verarbeitung oder Nutzung dieser Daten erfolgt oder erforderlich ist,
- Beschreibung der Kategorien betroffener Personen sowie der diesbezüglichen Daten oder Datenkategorien sowie Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
- Regelfristen für die Löschung der Daten unter Berücksichtigung gesetzliche Aufbewahrungsfristen,
- geplante Datenübermittlung in Drittländer und Bewertung des jeweiligen Datenschutzniveaus,
- eingesetzte Informationssysteme mit allgemeiner Beschreibung,
- zugriffsberechtigte Personengruppen oder Personen.

3. Der Datenschutzbeauftragte führt notwendige **Vorabkontrollen** durch und ist maßgeblich an der Auswahl neuer Informationssysteme beteiligt.

4. Er ist verantwortlich für die regelmäßige **Unterweisung der Mitarbeiter** zum Thema Datenschutz. Der hohe Stellenwert bei der Verarbeitung personenbezogener Daten, insbesondere bei den besonders schutzwürdigen Gesundheitsdaten (§ 3 Abs. 9 BDSG), macht eine mindestens jährliche Weiterbildung notwendig.

5. Er ist gleichermaßen **Ansprechpartner** für Patienten und Mitarbeiter zu allen Belangen personenbezogener Datenverarbeitung. Dies gilt ausdrücklich nicht nur für die elektronische Informationsverarbeitung.

Erreichbarkeit

Unsere Stichprobe hat gezeigt, dass der Datenschutzbeauftragte im eigenen Unternehmen oft nicht jedem Mitarbeiter bekannt ist. Auch wenn es gerade in großen Krankenhäusern und Kliniken nicht möglich ist, jeden Mitarbeiter mit seinen Zuständigkeiten zu kennen, ist die Identität des gesetzlich geforderten Datenschutzbeauftragten alles andere als unbedeutend. Dieser muss als Ansprechpartner für Betroffene zur Verfügung stehen. Betroffene können Mitarbeiter sein, die ein Datenschutzvergehen begangen haben oder denen selbst eines zugestoßen ist. Aber auch und gerade die Patienten, die ein Recht auf Auskunft zu der Be- und Verarbeitung bis hin zur Löschung oder Sperrung ihrer Daten haben, müssen den verantwortlichen internen oder externen Datenschutzbeauftragten unkompliziert erreichen können. Doch einmal Hand aufs Herz – wie sollen sich Mitarbeiter an den Datenschutzbeauftragten wenden, wenn sie nicht einmal wissen, wer dies ist? Und wie ist es in einem solchen Fall um das Bewusstsein von der Notwendigkeit des Datenschutzes bestellt?

> *Wie sollen sich Mitarbeiter an den Datenschutzbeauftragten wenden, wenn sie nicht einmal wissen, wer dies ist?*

Im optimalen Fall fungiert der Datenschutzbeauftragte entsprechend seiner Rolle als Hauptansprechpartner für sämtliche Fragen und Anliegen rund um das Thema Datenschutz. Er sollte somit sowohl intern bei den Mitarbeitern als auch extern bei Patienten oder Dienstleistern bekannt sein. Ein Eintrag im Impressum bzw. im Bereich Datenschutz auf der Website des Krankenhauses sowie eine interne Bekanntgabe der Daten wird daher empfohlen. Natürlich sollte der Bereich Datenschutz auch im Intranet gut auffindbar sein. Dort kann auch das Bundesdatenschutzgesetz hinterlegt werden, welches jedem Mitarbeiter zugänglich gemacht werden muss.

Im optimalen Fall fungiert der Datenschutzbeauftragte entsprechend seiner Rolle als Hauptansprechpartner für sämtliche Fragen und Anliegen rund um das Thema Datenschutz.

Barrieren abbauen

Am Ende kann sicherlich auch die enge Zusammenarbeit mit der Unternehmenskommunikation der richtige Ansatz für einen Datenschutzbeauftragten sein, um regelmäßig auf den diversen Kanälen in der Mitarbeiteransprache präsent zu sein. Der Datenschutz als solches darf nicht in einem stillen Kämmerlein umgesetzt werden, sondern muss im positiven Sinne immer zur Stelle sein. Einer unnötigen Geheimniskrämerei oder der fehlenden Selbstverständlichkeit bestellter Datenschutzbeauftragter kann es geschuldet sein, dass der Datenschutz zu kurz kommt. Den Mitarbeitern muss die Angst vor der Kontaktaufnahme genommen werden. Es muss deutlich werden, dass der Datenschützer für und mit den Mitarbeitern arbeitet und nicht die Rolle hat, den Mitarbeitern auf die Finger zu schauen, um diese im Sinne einer Aufsicht zu kontrollieren. Im Nachfolgenden einige Hinweise zu den fachlichen und persönlichen Voraussetzungen, die ein Datenschutzbeauftragter idealerweise haben sollte.[3]

> *Den Mitarbeitern muss die Angst zur Kontaktaufnahme genommen werden.*

Kompetenzen des DSB

Der Datenschutzbeauftragte hat eine abgeschlossene Berufsausbildung und mehrjährige Praxiserfahrung. Er verfügt über die notwendigen Grundkenntnisse, wie rechtliche Grundkompetenzen, Know-how im Bereich der Informations- und Kommunikationstechnologien, und ist in der Lage, betriebswirtschaftliche Entscheidungen nachzuvollziehen. Seine Persönlichkeit ermöglicht es ihm, Managementaufgaben zu übernehmen und durch Koordinierungs- und Teamfähigkeit seine Rolle auszuüben. Dabei verfügt er über eine entsprechende Durchsetzungsfähigkeit, die er durch seine didaktischen Fähigkeiten, den Einsatz von Empathie und hoher Sozialkompetenz erreicht.

Nicht zuletzt muss der Datenschutzbeauftragte frei von Interessenkonflikten zeitlicher und inhaltlicher Natur sein, sodass leitende Mitarbeiter, wie beispielsweise die Personalleitung oder auch ein CIO, die Rolle des Datenschutzbeauftragten nicht übernehmen sollen. Lesen Sie mehr zum Thema Pseudobestellung auf Seite 14. ■

Prof. Dr. Thomas Jäschke

[1] Aus Gründen der besseren Lesbarkeit wird auf die geschlechterspezifische Differenzierung verzichtet.

[2] Das Merkblatt zum betrieblichen Datenschutzbeauftragten IHK Pfalz erhalten Sie unter: www.pfalz.ihk24.de.

[3] Das Berufsbild des DSB nach BvD e. V. ist abrufbar unter: www.bvdnet.de.

Gastbeitrag

Qualitätsmanagement und Daten s chutzmanagement – organisatorischer Schnittpunkt od er fachliche Notwendigkeit?

Qualitätsmanagement (QM) und Datenschutzmanagement (DSM) – beides sind Herausforderungen, denen sich Organisationen des Gesundheitswesens täglich stellen müssen: weil es der Gesetzgeber so verlangt und es das besondere Vertrauensverhältnis zwischen den Handelnden in den Gesundheitsorganisationen und den Patienten erfordert.

Gesundheitsorganisationen dürfen ihr QM-System im weitesten Sinne individuell gestalten (SGB V § 137d; „ein" Qualitätsmanagement). Weitere Vorgaben ergeben sich aus speziellen Verordnungen wie der Apothekenbetriebsordnung ApBetrO, sind oft organisatorischer Art und bleiben in der Ausgestaltung innerhalb der Gesundheitsorganisation. Spezifische Modelle aus dem Gesundheitssektor sowie Normen wie die DIN EN ISO 9001 und DIN EN 15224 helfen bei der Umsetzung von QM-Systemen. Letztere übernimmt die DIN EN ISO 9001, überträgt ihre Anforderungen auf das Gesundheitswesen und ergänzt diese z. B. durch Anforderungen an Aufzeichnungen personenbezogener Art wie Patientenakten, OP-Berichte oder an den Schutz der Persönlichkeitssphäre. Beide Normen fordern die Umsetzung behördlicher und gesetzlicher Regelungen – somit auch des Bundesdatenschutzgesetzes (BDSG).

Die Vorgaben für den Datenschutz hat der Gesetzgeber im BDSG stärker konkretisiert als seine Vorstellungen von QM. In der praktischen Umsetzung stellen sich für beide Themen viele Fragen.

Allen voran lässt sich diskutieren: Sollten QM und DSM unabhängig voneinander oder miteinander verknüpft erfolgen? Inwieweit haben organisatorische Schnittpunkte oder fachliche Notwendigkeiten einen Einfluss auf diese Entscheidung?

> *Schnittstellen müssen verdeutlicht werden.*

QM und DSM treffen überall dort aufeinander, wo personenbezogene Daten in Prozessen verarbeitet, das heißt gespeichert, verändert, übermittelt, gesperrt oder auch gelöscht werden. Wenn beide Aufgaben sinnvoll miteinander verknüpft werden sollen, müssen diese Schnittstellen verdeutlicht werden. Das gilt nicht nur für Daten von Patienten, sondern auch für Mitarbeiter, Lieferanten und Partner.

Verknüpfende Prozesse

Aus dem BDSG ergeben sich Vorgaben und Dokumentationspflichten, die sich gut in QM-Systeme integrieren lassen: in Form von Vorlagen, z. B. für Anordnungen gegenüber Auftragnehmern im Rahmen von Auftragsdatenverarbeitungen (§ 11 BDSG), für das Erfassen von Einverständniserklärungen zur Datenverarbeitung oder das sogenannte Verfahrensverzeichnis (§ 4g Abs. 2 und 2a). Letzteres muss dem DSB zur Verfügung gestellt werden und beinhaltet verschiedene Angaben (§ 4e) wie die Zweckbestimmung von Datenerhebung, -verarbeitung und -nutzung oder Fristen zur Löschung von Daten. Und auch in Prozessbeschreibungen lässt sich für jeden Arbeitsschritt, bei dem personenbezogene Daten verarbeitet werden, z. B. durch Links oder Hinweise auf die erforderlichen Informationen verweisen.

Unabhängig davon, ob eine Gesundheitsorganisation verpflichtet ist, einen Datenschutzbeauftragten (DSB) zu benennen, oder nicht: Die Aufgaben QM und Datenschutz erfordern Zeit, Personaleinsatz und Wissen. Umso wichtiger ist es, klare Vorgaben zu Aufgaben und Kompetenzen zu machen. Eine Beauftragten-Übersicht sowie Aufgabenbeschreibungen für die einzelnen Beauftragten sind hilfreich. Sie unterstützen, wenn beide Themenfelder miteinander effektiv verknüpft und der offene Austausch von QM-Beauftragten und DSB gefördert werden sollen.

Datenschutz: das Qualitätsmerkmal

Aber besteht auch eine fachliche Notwendigkeit, QM und Datenschutz miteinander zu verbinden? Die Erwartungen der Patienten und der Gesellschaft an die medizinische Versorgung sind gewachsen. Die Kosten im Gesundheitswesen steigen, die Patienten müssen zunehmend Kosten selbst übernehmen und verfügen im Medienzeitalter über immer mehr Möglichkeiten, sich selbst zu informieren und Leistungen öffentlich zu bewerten. Zu Recht wird aus medizinischer und menschlicher Sicht eine hohe Qualität erwartet.

Die DIN EN ISO 9001 und DIN EN 15224 fordern Kundenorientierung – und damit Patientenorientierung – ein. Gesundheitsorganisationen müssen sich die Frage stellen: Welche Erwartungen haben unsere Patienten und Kunden? Der Grad der Erfüllung dieser Erwartungen bestimmt das wahrgenommene Maß der Qualität. Das besondere Vertrauensverhältnis lässt als eine Anforderung Verschwiegenheit und fachgerechte Daten- und Informationsübermittlung erwarten. Für eine Arztpraxis, ein Krankenhaus etc. ist ein professioneller Datenschutz und damit berechtigtes Vertrauen ein gutes Argument, warum Menschen sich gerade bei ihnen gut aufgehoben fühlen und wiederkommen oder weiterempfehlen.

Stephanie Glos
unterstützt kleine und mittelständische Unternehmen bei der Einführung von Qualitätsmanagementsystemen und ist DGQ-Qualitätsmanagerin® und DGQ-Auditorin Qualität® gemäß DGQ-Richtlinien.

Grundsätzlich gilt: Sowohl QM als auch DSM sind keine statischen Instrumente, sondern ein lebendiger Prozess, der von technischen Neuerungen, wachsenden Kundenanforderungen, neuen gesellschaftlichen Herausforderungen bestimmt wird, aber auch vom Gedanken der kontinuierlichen Verbesserung geprägt sein sollte. Datenschutz sollte sich nicht nur auf die Erstellung von Richtlinien, deren Schulung und Transfer in den Arbeitsalltag erstrecken, sondern auch im kontinuierlichen Verbesserungsprozess des QM-Systems integriert werden. Das bedeutet, das Thema Datenschutz, wie im BDSG empfohlen, mit in interne Audits zu integrieren und im jährlichen Qualitätsbericht kritisch zu hinterfragen. Bei Zuständigkeit kann auch der DSB das QM überprüfen (z. B. bei der Datenverarbeitung aus Qualitätssicherungsgründen).

Eine Einzelfallbetrachtung

Sowohl aus organisatorischer als auch aus fachlicher Sicht macht die Integration von QM und DSM Sinn, weil Schnittstellen verknüpft werden und Fehleraufkommen oder Redundanzen gesenkt oder gar verhindert werden können. Dennoch muss jede Organisation für sich prüfen, ob die Größe ihres Managementsystems überschaubar bleibt oder eine Trennung von QM und DSM hilfreicher ist. In diesem Fall sollten die Schnittstellen in beiden Managementsystemen deutlich herausgearbeitet werden. Eine regelmäßige Überprüfung, ob Änderungen oder Aktualisierungen in einem System Auswirkungen auf das andere System haben, ist notwendig.

Die DIN EN ISO 9001 wird im Herbst 2015 grundlegend überarbeitet neu erscheinen. Viele Informationen hierzu findet man u. a. bei der Deutschen Gesellschaft für Qualität unter www.dgq.de. ■

Stephanie Glos

Tipps zum Abbau von Hemnissen im QM und Datenschutz:

- Lassen Sie Ihre Managementsysteme von den Anwendern mitgestalten. So werden Vorgaben besser akzeptiert.
- Sensibilisieren Sie im Alltag für Schweigepflicht und Schutz der Persönlichkeitssphäre, stellen Sie kritische Punkte in den Fokus.
- Integrieren Sie QM und Datenschutz-Schulungen möglichst häufig in den Arbeitsalltag. Schulungen und Unterweisungen lassen sich in regelmäßige Teambesprechungen einbinden.
- Fördern Sie den Austausch von DSB und QM-Beauftragten, Verantwortlichen für die Bereiche IT und Verwaltung sowie der Leitung, um Ihr System zu optimieren und ein offenes Miteinander zu fördern.
- Holen Sie sich bei Bedarf externe Unterstützung.

Dr. Bernd Schütze ist Mitglied in verschiedenen Gesellschaften und Berufsverbänden, in denen er auch aktiv in verschiedenen Arbeitsgruppen mitarbeitet. Weiterhin ist er als Datenschutzbeauftragter und -auditor tätig. Derzeit arbeitet Dr. Schütze bei der Deutschen Telekom Healthcare and Security Solutions GmbH (DTHS) im Bereich Datensicherheit und Datenschutz im Gesundheitswesen.

Im Interview mit …

Dr. Bernd Schütze

Welche Bedeutung schreiben Sie dem Datenschutz im Gesundheitswesen zu?
Der Datenschutz ist ein wesentlicher Bestandteil der Patientenbehandlung: Nur, wenn der Patient das Vertrauen in die behandelnde Einrichtung hat, dass seine intimen Gesundheitsdaten nicht öffentlich verfügbar werden, ist eine erfolgreiche Behandlung möglich. Nur dann wird der Patient seinen Behandlern alles anvertrauen, was diese zur Diagnose und Therapie der Erkrankung wissen müssen.

Welche Erfahrungen haben Sie mit der Akzeptanz und dem Umsetzungswillen von Datenschutzrichtlinien beim Klinikpersonal gemacht?
Dies hängt nach meiner Erfahrung davon ab, inwieweit es dem Datenschutzbeauftragten gelingt, das Personal „abzuholen". Die Klinikmitarbeiter, insbesondere diejenigen, die in der medizinischen Versorgung beschäftigt sind, haben in der Regel selbst großes Interesse am Datenschutz – vielleicht nennen sie es nur anders. Allen ist bewusst, dass der Schutz der sensiblen Patientendaten notwendig ist. Gleichzeitig arbeiten die Mitarbeiter in der Patientenversorgung auch unter enormem Zeitdruck. Die Umsetzung datenschutzrechtlicher Vorgaben, wie z. B. das automatisierte Einschalten eines Bildschirmschoners mit Passwortsperre, verschärft diesen zeitlichen Druck noch.

Das muss einem Datenschutzbeauftragten bewusst sein. Die Maßnahmen des Datenschutzbeauftragten müssen sich in den Workflow der Patientenversorgung integrieren, nicht diesen behindern. Ein „so geht es nicht" alleine führt dazu, dass der Datenschutzbeauftragte als Behinderung in Kliniken angesehen wird; dies ist die „schlimme" Form des Datenschutzbeauftragten.

Ein guter Datenschutzbeauftragter wird vom Personal als Partner angesehen, weil er gemeinsam mit dem Personal Lösungen erarbeitet.

Für wie wichtig halten Sie das Thema „Integrität beim DS"?
Neben „Verfügbarkeit" und „Vertraulichkeit" ist Integrität ja eines der drei klassischen Ziele der IT-Sicherheit. Im Sinne von IT-Sicherheit ist Integrität die Verhinderung unautorisierter Manipulationen von Information, somit gehört die Integrität auch zu den wichtigsten Forderungen des Datenschutzes: Jeglicher unautorisierter Zugriff auf personenbezogene Informationen ist zu unterbinden. Die Sicht der IT-Sicherheit geht bezüglich Integrität ggf. über die Sicht des Datenschutzes hinaus, da die IT-Sicherheit verschiedene Formen der Integrität kennt, die nicht alle direkt etwas mit einem autorisierten/unautorisierten Zugriff zu tun haben:

- Richtige Abbildung der realen Welt, also korrekte Sachverhalte
- Unmodifizierte Inhalte
- Erkennung von Modifikationen
- Temporale Korrektheit (z. B. bei CDA-Dokumenten).

Aus dieser Sicht gesehen, ist die Integrität für IT-Abteilungen für datenschutzrelevante Daten im Gesundheitswesen, also personenbeziehbare Daten, natürlich unabdingbar: Im überwiegenden Teil handelt es sich hierbei um patientenbezogene Daten, deren Integrität unabdingbare Voraussetzung für deren Verwendung in der Patientenbehandlung darstellt.

Leider bieten die meisten klinischen Informationssysteme hier noch nicht die kryptografischen Verfahren an, mit denen die Integrität zweifelsfrei festgestellt werden kann: Prüfsummen, sei es für die Daten selbst oder auch für die Protokolldaten, die man zum Nachweis des Datenzugriffs (also wer griff wann auf welche Patientendaten zu) benötigt, werden heute von Herstellern nur selten zur Verfügung gestellt.

Ist der Datenschutz Ihrer Meinung nach überhaupt in den klinischen Alltag zu integrieren?
Datenschutz ist ein substanzieller Bestandteil des medizinischen Alltags. Einen Hinweis, wie wichtig das Patientengeheimnis für die Patientenversorgung ist, bietet ja auch die jeweilige Berufsordnung für Ärzte.

Es ist vielmehr die Frage, wie gut sich die Vorgaben des jeweiligen Datenschutzbeauftragten in den jeweiligen Behandlungskontext integrieren lassen. Ein Beispiel: Ein Notfallzugriff auf medizinische Daten eines Patienten, das heißt, ein eigentlich unautorisierter Zugriff auf Daten, muss protokolliert und begründet werden. Nun ist mit einem Notfall in der Regel eine zeitliche Komponente beinhaltet: Muss ich die Begründung vor oder nach dem Zugriff eingeben? Aus medizinischer Sicht ist ein schnellstmöglicher Zugriff geboten, das heißt, die Begründung muss nach dem Zugriff eingegeben werden. Aus datenschutzrechtlicher Sicht hat man die Schwierigkeit, dass hinterher selten eine Begründung eingegeben wird und vonseiten der Krankenhausführung auch keine Konsequenzen aus der Nichteingabe gezogen werden. Eine vorherige Eingabe der Begründung bei einem Notfallzugriff wird sich nur in den Alltag integrieren lassen, wenn der Mehraufwand aus ärztlicher Sicht vertretbar ist.

Damit kommen wir auf den oben angesprochenen Punkt: Gut einsetzbare datenschutzrechtliche Lösungen, die gelebt werden, können nur im partnerschaftlichen Umgang von Datenschutzbeauftragten und medizinischem Personal gefunden werden.

Haben Sie unterstützende Tipps für Datenschutzbeauftragte zur internen Umsetzung?
Nehmen Sie die Krankenhausverwaltung und das medizinische Personal mit in die Verantwortung, das heißt, machen Sie ihnen klar, dass die Verantwortung für den Datenschutz nicht beim Datenschutzbeauftragten liegt, sondern bei jedem Einzelnen. Verdeutlichen Sie der Krankenhausleitung, dass datenschutzrechtliche Verstöße (z. B. fehlende ADV-Verträge) Ordnungswidrigkeiten sind, deren Kosten bei einem Verstoß die Krankenhausverwaltung tragen muss. Begleiten Sie Ärzte bei ihren Projekten, z. B. Forschungsprojekten, und zeigen Sie, wie man mit einfachen Mitteln eine Pseudonymisierung durchführen kann, ohne das Forschungsziel aus den Augen zu verlieren. Unterstützen Sie die IT-Abteilung, indem Sie ihnen Materialien für Ausschreibungen/Neuanschaffungen zur Verfügung stellen, mittels derer datenschutzrechtliche Fragen ohne größeren Mehraufwand beantwortet werden können.

Kurz: Seien Sie Partner im klinischen Alltag, nicht „Schreibtischtäter"!

Weitere Anworten von Bernd Schütze zur OH-KIS und dem integrierten Datenschutz in medizinischen Einrichtungen erhalten Sie unter www.isdsg.de. ■

Interview: Nina Richard

Pseudobestellung

Verantwortliche einer Einrichtung im Gesundheitswesen sind für die Datenverarbeitung nach Bundesdatenschutzgesetz (BDSG) persönlich haftend. Bei der Bestellung des internen Datenschutzbeauftragten sollte daher ein besonderes Augenmerk auf die ausreichende Qualifizierung gelegt werden. Ebenso darf kein Interessenkonflikt des Datenschutzbeauftragten vorliegen, denn dies oder die rein formale Benennung können zu einer Pseudobestellung führen. Worauf Sie achten sollten, um dies zu verhindern.

Der Datenschutzbeauftragte sollte sorgfältig ausgewählt werden.

In Einrichtungen, die gemäß der aktuellen Gesetzeslage einen Datenschutzbeauftragten zu bestellen haben, ist darauf zu achten, dass die Bestellung rechtlich bedenklich sein kann. Die Wahl des Datenschutzbeauftragten darf deshalb nicht willkürlich erfolgen.

Voraussetzungen des DSB

Halten wir deshalb vorab fest, welche Voraussetzungen ein Datenschutzbeauftragter erfüllen sollte. Per Gesetz hat der betriebliche Datenschutzbeauftragte grundlegende Voraussetzungen zu erfüllen: Er muss die datenschutzrechtlichen Bestimmungen im Gesundheitswesen nicht nur kennen, sondern sie auch sicher anwenden. Zusätzlich sind vertiefte Kenntnisse im Bereich der Informationstechnik vorzuweisen. Ein weiterer wichtiger Aspekt ist die Zuverlässigkeit.

Ein Datenschutzbeauftragter muss also in der Lage sein, den Bedürfnissen von Mitarbeitern und Patienten gerecht zu werden und sich gleichzeitig gegenüber diesen sowie der Geschäftsführung behaupten.

Interessenkonflikt

Nachdem die Anforderungen an den Datenschutzbeauftragten beschrieben wurden, richtet sich die weitere Betrachtung auf die Interessenkonflikte, die in Einrichtungen auftreten könnten: Interne Datenschutzbeauftragte gehen dieser Tätigkeit in der Regel nicht Vollzeit nach, sondern üben noch eine weitere Stelle aus. Es darf daher nicht zu der Situation kommen, dass der Datenschutzbeauftragte sich selbst kontrolliert.

Beispielsweise kann die Bestellung eines Mitarbeiters im Interessenkonflikt mit seiner eigentlich auszuübenden Tätigkeit stehen, wenn sowohl zeitliche als auch inhaltliche Aspekte der notwendigen, datenschutzrechtlichen Aufgabenerfüllung entgegenstehen. Nachfolgende Mitarbeitergruppen sollten nicht zum DSB berufen werden:

- EDV/IT
- Personalabteilung
- Einheiten mit besonders hohem Aufkommen datenverarbeitender Tätigkeiten
- Geheimschutzbeauftragte
- Ggf. Juristerat

Dies soll nur als Hilfestellung und zum Schutz des DSB dienen. Grundsätzlich gilt, dass ein Interessenkonflikt immer im Einzelfall geprüft werden muss.

Quellen zur weiteren Recherche:
www.datenschutzzentrum.de
www.bfdi.bund.de

Nina Richard

2. Goldene Regel: Verschlüsselte Übermittlung von Daten

Wenn es erforderlich ist, Patientendaten an andere Personen oder Praxen über das Internet zu übermitteln, verschlüsseln Sie die Daten und versehen diese mit einer digitalen Signatur.

Zu personenbezogenen Daten zählen alle Einzelangaben, die Auskunft über persönliche oder sachliche Verhältnisse des Patienten und dessen Behandlung geben. Die Übermittlung von personenbezogenen Daten geschieht heutzutage nicht mehr nur per Post. Die Versendung per E-Mail kann um einiges schneller erfolgen als der gewohnte Postweg. Ganz gleich, welchen digitalen Kommunikationskanal Ihr Krankenhaus nutzt, um beispielsweise Patientenbefunde oder Ähnliches zu versenden, muss hier immer gelten: Personenbezogene Daten nur gesichert übermitteln!

Das Versenden von E-Mails ohne weitere Maßnahmen gleicht dem einer Postkarte, die jeder ohne großen Aufwand lesen kann. Wenn es erforderlich ist, Patientendaten an andere Personen oder Praxen über das Internet zu übermitteln, verschlüsseln Sie die Daten und versehen diese mit einer digitalen Signatur. Die Verschlüsselung garantiert Ihnen, dass die Daten nur von demjenigen abgerufen und gelesen werden können, für den sie bestimmt sind. Die digitale Signatur zeigt dem Empfänger, dass die Daten nach der Verschlüsselung nicht mehr geändert worden sind und von welchem Absender die Nachricht abgesendet wurde.

Es gibt drei verschiedene Möglichkeiten, vertrauliche Inhalte per E-Mail zu versenden. Generell gibt es das Problem, dass sich Empfänger und Sender auf ein Verfahren einigen müssen. Aus diesen Gründen fallen in der Regel die professionellen Verfahren PGP und SMIME weg. Praktischer ist der Einsatz von verschlüsselten ZIP-Archiven, da moderne Betriebssysteme dieses Archivformat in der Regel von Haus aus beherrschen. Dabei muss dann nur noch über einen anderen Kanal, wie z. B. durch ein Telefonat, der geheime Schlüssel übermittelt werden.

Nina Richard

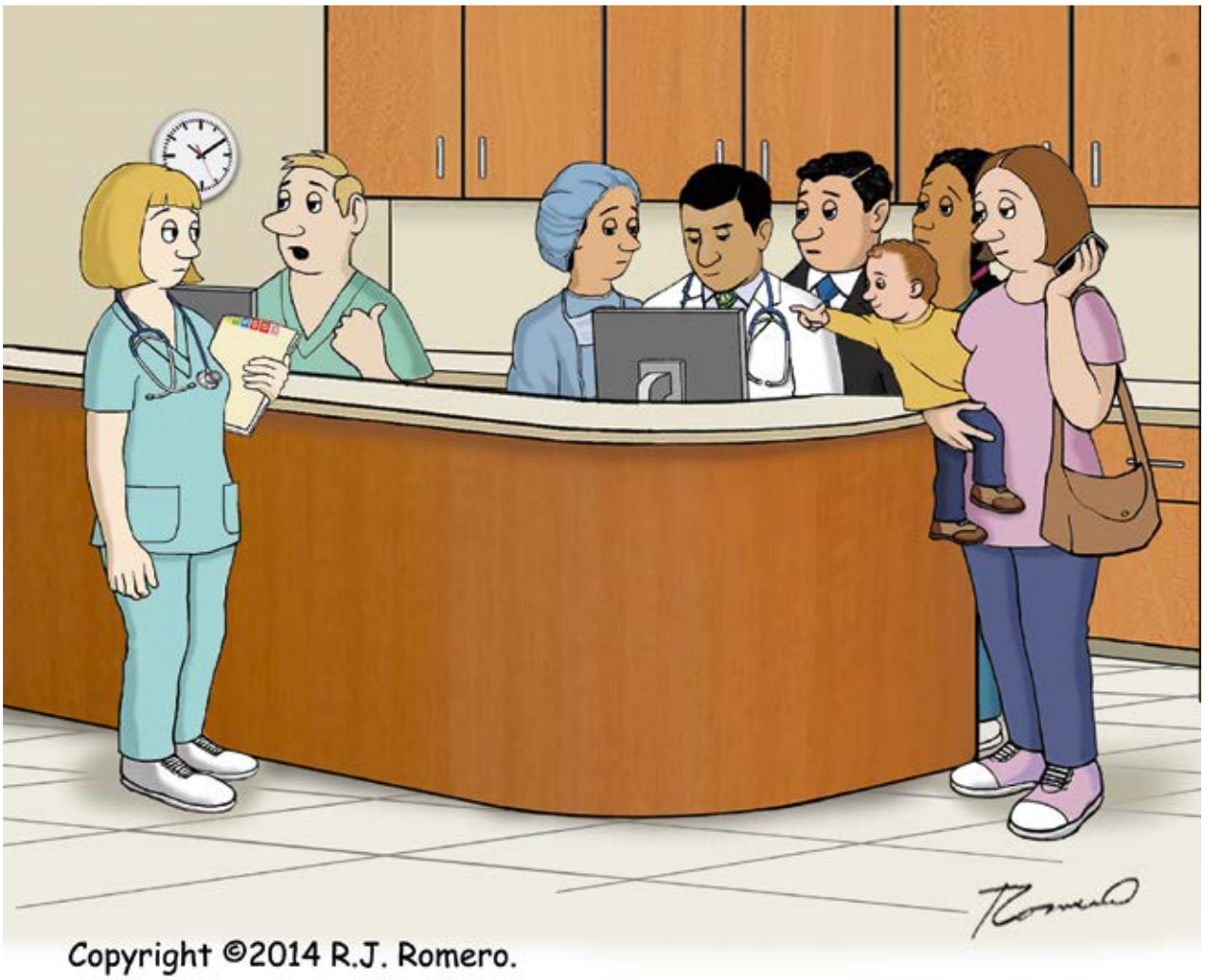
TIPP

Es gibt verschiedene unkomplizierte Verschlüsselungstechniken, die ohne großen Aufwand genutzt werden können. Bei der Entscheidung über die richtige Verschlüsselungstechnik sollte unbedingt der Datenschutzbeauftragte befragt werden.

Impressum

ExperSite Ausgabe 01 2015 | **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: shutterstock, racorn, S. 2: Falko Wübbecke, Dortmund; S. 3: Falko Wübbecke, Dortmund; shutterstock, Andrey Popov, NPFire, SL; S.4: shutterstock, Syda Productions; S. 6-7: shutterstock, Sean Locke Photography; S. 8-9: shutterstock, racorn; S.10: NPFire; S. 11: Stephanie Glos, S. 12: Bernd Schütze, shutterstock, lightwavemedia; S. 14: shutterstock, Andrey Popov, S. 15: shutterstock, Palis Michalis, John Smith Design; U4: hipaacartoons, R. J. Romero.

Einblicke & Ausblicke



Wir bedanken uns für die inhaltlichen Beiträge bei:

Dr. Bernd Schütze, Deutsche Telekom Healthcare and Security Solutions GmbH (DTHS)

Stephanie Glos, DGQ-Qualitätsmanagerin® und DGQ-Auditorin Qualität®

Die nächste Ausgabe erscheint im September 2015

Im Schwerpunkt: Datenverarbeitung im Auftrag oder doch Funktionsübertragung?

Verschlüsselung – aber richtig?