ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen

ExperSite

Das Magazin für Sicherheit und Datenschutz im Gesundheitswesen

Ausgabe 01 2016

Mitarbeiterdaten schützen

Besonders kritisch für Krankenhäuser: wenn Mitarbeiter plötzlich zu Patienten werden

Tipps & Fakten
Ist mobil ungleich sicher? Studien scheinen dies für die Kommunikation im Gesundheitswesen deutlich zu machen.

Im Interview
Rechtsanwalt F.-M. Przytulla über den Stellenwert von Beschäftigtendatenschutz

Kameraüberwachung
In der vierten goldenen Regel, schauen wir uns an, worauf Sie achten müssen.

VERANSTALTUNGEN DES ISDSG

Das ISDSG bietet eine Vielzahl von Schulungen an, die auf die konkreten Bedürfnisse Ihrer Mitarbeiter zugeschnitten werden. Gerne besuchen unsere Berater Sie direkt vor Ort.

Datenschutz- und IT-Sicherheits-seminare und Workshops für

… Führungskräfte
… Verwaltungsangestellte
… medizinische Fachkräfte
… Ärzte
… Datenschutzbeauftragte
… ITler
… Informationssicherheitsbeauftragte
… Einsteiger
… Anwälte

Unsere Workshops werden dem individuellen Kenntnisstand unserer Teilnehmer angepasst, deshalb bieten wir alle Seminare und Workshops als Einsteiger- und Aufbauveranstaltungen an.

Auch brandaktuelle Problemstellungen werden immer wieder von uns aufgegriffen bei

… Business-Frühstücken
… Kaminabenden

Gemeinsam mit unseren Kooperationspartnern initiieren wir an den Bedürfnissen des Marktes orientierte Lehrgangsangebote zum

… zertifizierten Datenschutzbeauftragten (IOM)

VERANSTALTUNGSTIPPS AUS DER BRANCHE

Datenschutz in der Medizin – Update 2016
19.04.2016, Wiesbaden

UpDate! Bundesdatenschutzgesetz

conhIT – Connecting Healthcare IT
19.–21.04.2016, Berlin

conhIT

User Group „Datenschutz im Gesundheitswesen“
24.–25.04.2016, Leipzig

Gesundheitsforen Leipzig

Datenschutz in der Medizin – Update 2016
09.06.2016, Wiesbaden

UpDate! Bundesdatenschutzgesetz

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

Inhalt

Von der Bewerbung bis zur Kündigung: Das müssen Sie für den Beschäftigtendatenschutz beachten.

Veranstaltungen & Termine 2

Das Team 4

Tipps & Fakten 6

Schwerpunkt

Mitarbeiterdaten schützen 8
So schützen Sie die Daten Ihrer Mitarbeiter richtig.

Kooperationspartner

Kommunikation als Brückenbauer 12
Das Krankenhaus-Kommunikations-Centrum stellt sich vor.

Update BDSG 13
Praxisbezogene Veranstaltungen zum Thema Datenschutz im Gesundheitswesen

Gastbeitrag

IT-Lösungen vom Anbieter verwalten lassen 14
Sinnvolles Outsourcing oder Datenschutzfalle?

Voice

Interview mit Rechtsanwalt F.-M. Przytulla 16
Dem Stellenwert von Beschäftigtendatenschutz müsste eine größere Bedeutung beigemessen werden.

Der Datenschutzbeauftragte

Ihre Aufgaben im Mitarbeiterdatenschutz 18
Partner statt Verhinderer

Goldene Regeln

4. Goldene Regel: Videoüberwachung 19
Diese Punkte sollten Sie beachten

EDITORIAL

Sehr geehrte Leserinnen und Leser,

für das Jahr 2016 lässt sich in Bezug auf Datenschutz und IT-Sicherheitsthemen einiges erwarten.

Neben dem erwarteten Entwurf für Safe Harbour 2 und der neuen Datenschutzverordnung, die im März oder April verabschiedet werden soll, machen die technischen Entwicklungen das Thema in der praktischen Umsetzung immer komplizierter.

In der Grundidee von guten und praktikablen IT-Systemen fehlt die Transparenz, wodurch es unbeabsichtigt zu Datenschutzverstößen kommen kann. Auch Mitarbeiter können hiervon betroffen sein. Aus einer Protokollierung oder der Verwendung von Sicherheitskameras kann hier schnell eine Mitarbeiterüberwachung werden. Und genau hiermit beschäftigt sich die aktuelle Ausgabe der ExperSite.

Erfahren Sie mehr über das Thema Beschäftigtendatenschutz, die Aufgaben des Datenschutzbeauftragten und auch über den speziellen Fall der Videoüberwachung.

Wir wünschen 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 B. A.
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 M. Sc.
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

Dipl.-Betr. (FH) 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 B. Sc.
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 B. Sc.
Datenschutz

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

✉ beer@isdsg.de

Dipl.-Kfm. 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

Smart Home

Eine weitere wichtige Thematik, die nicht nur im Gesundheitswesen für spannenden Gesprächsstoff sorgen wird, ist das Smart Home, also das intelligent vernetzte und über mobile Endgeräte steuerbare Zuhause. Angefangen von Schließmechanismen von Türen und Fenstern bis hin zur Verwaltung der Heizung, dem Zugriff auf den Heim-PC und vielem mehr wird die Vernetzung immer bezahlbarer und dadurch auch zunehmend z. B. für die Seniorenbetreuung ein Thema. Aber für die informationelle Selbstbestimmung kann dies tatsächlich zu einem großen Problem werden.

Jegliche Geräte wie Schränke oder Kühlschränke sind in dieser Welt mit Sensoren ausgestattet, die in Kombination mit mobilen Endgeräten Daten sammeln. Es geht hier um Daten wie die des Standortes, des Alltagsverhaltens, die an Anbieter weitergeleitet werden würden, und Kameras und Lautsprecher, die theoretisch die Möglichkeit der ganz anderen Überwachung bieten. Ebenso verhält es sich mit den intelligenten Messsystemen für Strom, Wasser und Gas, auch Smart Metering genannt. Problematisch ist bei dieser Datenerhebung, dass diese nicht transparent erfolgt und der Nutzer nur in den wenigsten Fällen einen genauen Überblick über die Verwendung der Daten und die damit verbundenen Konsequenzen hat.

Buchtipp: Datenschutz im Gesundheitswesen

Im April ist es soweit. ISDSG-Vorstand Prof. Dr. Thomas Jäschkes Buch zum Thema Datenschutz im Gesundheitswesen erscheint im April 2016.

Orientierung in grundlegenden Datenschutzfragen

Das Thema Datenschutz ist heutzutage wichtiger denn je. Noch nie war der Allgemeinheit so sehr bewusst, wie begehrt persönliche Daten sind. Die Datensammelwut wird von den Big Playern wie Google und Facebook aus den USA regiert, die bereits eine Fangemeinde in absoluter Abhängigkeit um sich herum geschaffen haben. Dem Gesundheitswesen in Deutschland wird, im Vergleich zu anderen Branchen, häufig nachgesagt, technologisch knapp zehn Jahre im Innovationsrückstand zu sein. Dennoch sind Entwicklungen wie Cloud-Computing, e- und mHealth-Anwendungen auf dem schnellen Vormarsch und versprechen neue Möglichkeiten in der medizinischen Betreuung der Patienten. Der Ruf nach der Optimierung der Datenschutzorganisation in Bezug auf integrierten Datenschutz wird immer lauter. Das Buch „Datenschutz im Gesundheitswesen" soll einen ersten groben Überblick liefern, um den Einstieg in verschiedene Datenschutzthematiken zu erleichtern, um Praktiker im Berufsalltag zu unterstützen und hier eine Orientierung in Bezug auf grundlegende Datenschutzaspekte zu bieten. Worin die Herausforderungen und Rahmenbedingungen bestehen, welche Strategien, Konzepte und Instrumente sich bewähren, zeigen Praktiker und ausgewiesene Experten auf.

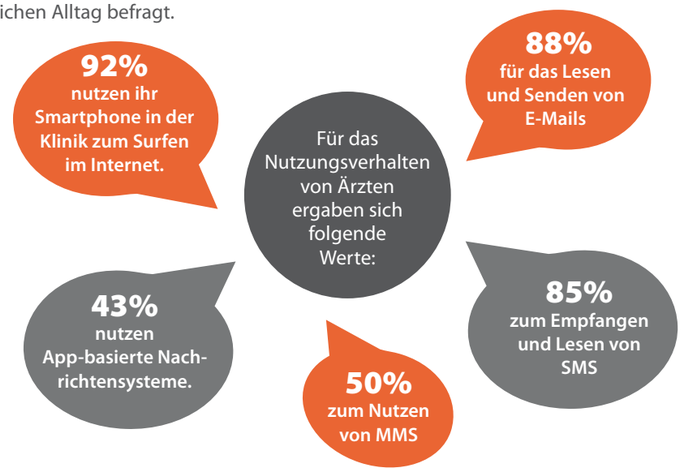
T. Jäschke (Hrsg.), Datenschutz im Gesundheitswesen.
Grundlagen, Konzepte, Umsetzung
Preis: ca. 59,95 € | ISBN: 978-3-95466-221-0

EU-Datenschutzverordnung

Im März/April 2016 ist mit der Verabschiedung der EU-Datenschutzverordnung zu rechnen, in der die europäischen und nationalen Datenschutzstandards vereinheitlicht werden sollen. Die Verordnung verspricht die Einsparung des Verwaltungsaufwandes, gleichzeitig aber eine stärkere Einbindung der Aufsichtsbehörden bei Verstößen. Hieraus ergibt sich eine erhöhte Rechenschaftspflicht für Unternehmen. Die Übergangsfrist beträgt zwei Jahre. Aufgrund der Komplexität sollten Unternehmen langsam anfangen, sich mit der neuen Verordnung auseinanderzusetzen, um ihre Prozesse und Systeme an die neuen Anforderungen anzupassen. Die Richtlinie ist konkreter als das IT-Sicherheitsgesetz. Problematisch bleibt allerdings der Schwerpunkt auf Großkonzernen. Kleine und mittelständische Unternehmen werden nicht ausreichend berücksichtigt. Gleichzeitig führen zu schwammige Formulierungen zur Praxisferne der Richtlinie.

Klinikärzte verschicken Patientendaten per WhatsApp und Co. – aus Datenschutzperspektive ist das kritisch.

Die „Ärztezeitung" berichtete über eine britische Studie, die in fünf Kliniken des National Health Services durchgeführt wurde. Insgesamt wurden 287 Ärzte und 564 Krankenschwestern zu ihrem Nutzungsverhalten von mobilen Endgeräten im beruflichen Alltag befragt.



Häufig wurden hier auch personenbezogene Patientendaten verschickt. 71% der Ärzte wünschen sich einen sicheren Kommunikationskanal zum Verschicken solcher Daten. (Quelle: „Ärzte Zeitung", 05.01.2016)

Ein Großteil von Medical-Apps ist unsicher

In der zweiten Jahreshälfte des vergangenen Jahres untersuchten Experten von ePrz die Sicherheit von Daten bei rund 140 Gesundheits-Apps.
Die Ergebnisse (Auszug):

- Abgefangene Login-Daten bei 80 % aller Apps
- 75 % aller Apps ließen eine Manipulation der Gesundheitswerte zu
- 57 % aller Apps bieten keine Datenschutzerklärung

(Quelle: http://bundesverbandinternetmedizin.de)

Mitarbeiterdaten schützen

Mitarbeiterüberwachungen innerhalb von Konzernen wie der Bahn oder Lidl sind vielen noch heute präsent. Für das Gesundheitswesen ist der Themenkomplex Mitarbeiterdatenschutz von ebenso großer Bedeutung wie in anderen Branchen – allerdings kann es hier auch Besonderheiten geben, so beispielsweise, wenn der Mitarbeiter zum Patienten wird. Aber auch bereits vor der Einstellung gibt es einige Punkte zu berücksichtigen, denn Datenschutz ist längst nicht nur in Bezug auf Patientendaten ein Thema – auch Mitarbeiterdaten sind schützenswert.

§ 32 BDSG

1. Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

2. Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

3. Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

Nach einer Vielzahl von Datenschutzverstößen im Rahmen von Beschäftigungsverhältnissen wurde bereits im Jahr 2007 die Forderung nach einer einheitlichen Gesetzesgrundlage für den Beschäftigtendatenschutz lauter. 2009 wurde als Resultat der § 32 BDSG eingeführt.

Leider definiert der Paragraf nur, dass Daten eines Mitarbeiters genutzt werden dürfen, wenn es für das Arbeitsverhältnis notwendig ist oder der (begründete) Verdacht einer Straftat vorliegt. Wie genau die Überwachung eines Mitarbeiters aber jetzt aussehen darf, welche Rolle Onlinetools hier haben oder was passiert, wenn Behörden Auskunft verlangen, wird nicht offenbart.

Es wird deutlich, dass § 32 BDSG ursprünglich nur als eine Grundlage gedacht war, die durch ein Arbeitnehmerdatenschutzgesetz konkretisiert werden sollte, das aber bis heute nicht beschlossen wurde. Datenschutzbeauftragten bleibt daher nur, sich an dem Grundgerüst von § 32 BDSG zu orientieren. Aber wie sieht dies nun in der Praxis aus?

Bewerbungsprozess

Bereits innerhalb des Bewerbungsprozesses werden Ihnen verschiedenste datenschutzrechtliche Thematiken begegnen. Neben der klassischen Papierbewerbung haben sich heute auch Onlinebewerbungen etabliert, die automatisiert Daten von Bewerbern erfassen, verarbeiten und speichern. Grundlegend ist die Speicherung und Verarbeitung personenbezogener Daten für den konkreten Zweck der Bewerberauswahl zulässig.

Abschluss der Bewerbungsphase

Nach Abschluss der Bewerbungsphase sind aus der reinen Datenschutzperspektive und unter Bezugnahme auf die Datensparsamkeit, die Daten der Bewerber zu löschen.

> *Papierbewerbungen dürfen nicht einfach im Papierkorb entsorgt werden.*

Hier gilt allerdings, dass Papierbewerbungen nicht einfach im Papierkorb entsorgt werden dürfen. Aufgrund des Gleichstellungsgesetzes bleibt außerdem die Nachweispflicht des Arbeitgebers bestehen, im Falle einer Klage durch den Bewerber beweisen zu können, dass dieser nicht wegen genderspezifischer oder soziokultureller Kriterien ungeeignet für die Stelle war. Zur Erfüllung der Beweispflicht können Unterlagen daher bis zu sechs Monate zu Dokumentationszwecken aufbewahrt werden. Eine weitere Ausnahme bildet

die konkrete Einwilligung des Bewerbers in die Verwendung der Unterlagen für später ausgeschriebene Stellen. Hier bietet es sich allerdings an, die Einwilligung in Abständen von beispielsweise einem halben Jahr zu erneuern. Auch die Einsichts- bzw. Zugriffsrechte innerhalb des Krankenhauses müssen beschränkt werden.

Nur Personen, die in den Prozess involviert sind, dürfen die Unterlagen einsehen, wie beispielsweise Mitarbeiter der Verwaltung oder des Personalwesens.

Bei der Einstellung

Mitarbeiterverpflichtung
Ebenso müssen neue Mitarbeiter über den Umgang mit personenbezogenen Daten innerhalb des Krankenhauses, zu denen auch Mitarbeiterdaten gehören, und zur Geheimhaltung im Rahmen der Mitarbeiterverpflichtung verpflichtet werden.

Betriebsvereinbarung
Mit der Unterzeichnung des Arbeitsvertrages eines neuen Mitarbeiters sollte dieser mit grundlegenden Gegebenheiten und Regelungen des neuen Betriebes vertraut gemacht werden. Hierzu zählt unter anderem die Betriebsvereinbarung. Die Verhandlung der Betriebsvereinbarung erfolgt zwischen Arbeitgeber und Betriebsrat. Beispielsweise sollte hierin enthalten sein, wie die IT-, E-Mail-, Social-Media- oder Telefonnutzung etc. geregelt ist.

Ausgehend von einem fiktiv gewählten Beispiel, in dem Medikamente und Behandlungsmaterialien im Wert von mehreren tausend Euro entwendet wurden und ein begründeter Verdacht entsteht, weil Mitarbeiter einer bestimmten Station als Einzige Zugang hatten, kann es rechtmäßig sein, Durchsuchungen durchzuführen. Es gilt allerdings, dass die Persönlichkeitsrechte der Mitarbeiter gewahrt werden müssen. So müsste die Auswahl der kontrollierten Mitarbeiter einem Zufallsprinzip entsprechen und eine Durchsuchung in vor Einsicht geschützten Räumlichkeiten stattfinden.

> *Das Anfertigen einer Kopie des Personalausweises ist nicht zulässig.*

Kopie des Personalausweises
Eine simple Möglichkeit, eine Vielzahl von Daten für die Personalakte zu hinterlegen, ist eine Kopie des Personalausweises. Nach der Einführung des Personalausweisgesetzes im Jahr 2011 ist das Anfertigen einer Kopie des Personalausweises allerdings nicht zulässig. Ausnahmen bilden Fälle, in denen andere Rechtsvorschriften höher angesiedelt werden. Gleichzeitig sollten auch in der Personalakte nur Daten erhoben werden, die zur Ausübung der Geschäftstätigkeit notwendig sind (Stichwort: Datensparsamkeit).

Während des Arbeitsalltages

Mitarbeiter als Betroffener
In Gesundheitseinrichtungen kommt es nicht selten zu dem Fall, dass Mitarbeiter die Rolle des Patienten einnehmen. Dies kann datenschutzrechtlich kritisch werden, wenn Mitarbeiter oder Vorgesetzte sich über den Gesundheitsstand des Mitarbeiters informieren möchten. Es gilt jedoch, dass keine Auskünfte zum Gesundheitszustand an Kollegen oder Führungskräfte erteilt werden dürfen, die nicht in die Behandlung involviert sind. Gemäß § 32 BDSG dürfen Mitarbeiterdaten nur für die Begründung, die Durchführung und Beendigung des Arbeitsverhältnisses genutzt werden. Zu diesen Daten zählen beispielsweise Aufzeichnungen über Erfahrungen und Kenntnisse sowie Urlaubsdaten.

Allerdings ist die Veröffentlichung dieser Daten ebenso wie von Geburtstagen, Fotos und privaten Telefonnummern nur mit konkreter Zustimmung des Betroffenen erlaubt. Die Speicherung von ärztlichen Diagnosedaten des Mitarbeiters innerhalb der Personalakte ist nicht zulässig.

> *Jeder Mitarbeiter hat das Recht, die Daten einzusehen, die die Personalabteilung von ihm gespeichert hat.*

Einsicht in die Personalakte
Jeder Mitarbeiter hat das Recht gegenüber seinem Arbeitgeber, die Daten einzusehen, die die Personalabteilung von ihm gespeichert hat. Für Arbeitnehmer ergeben sich daraus folgende Rechte:

- Einsichtnahme in die vollständige Personalakte
- Kopieren der Akte erlaubt (auf Kosten des Arbeitnehmers) aber keine Herausgabe der Originalakte!
- Ergänzungen und Richtigstellungen sind auf Verlangen des Arbeitnehmers hinzuzufügen
- Entfernung von Teilen der Akte (z. B. missbilligende Aussagen oder nicht gerechtfertigte Abmahnungen können entfernt werden)

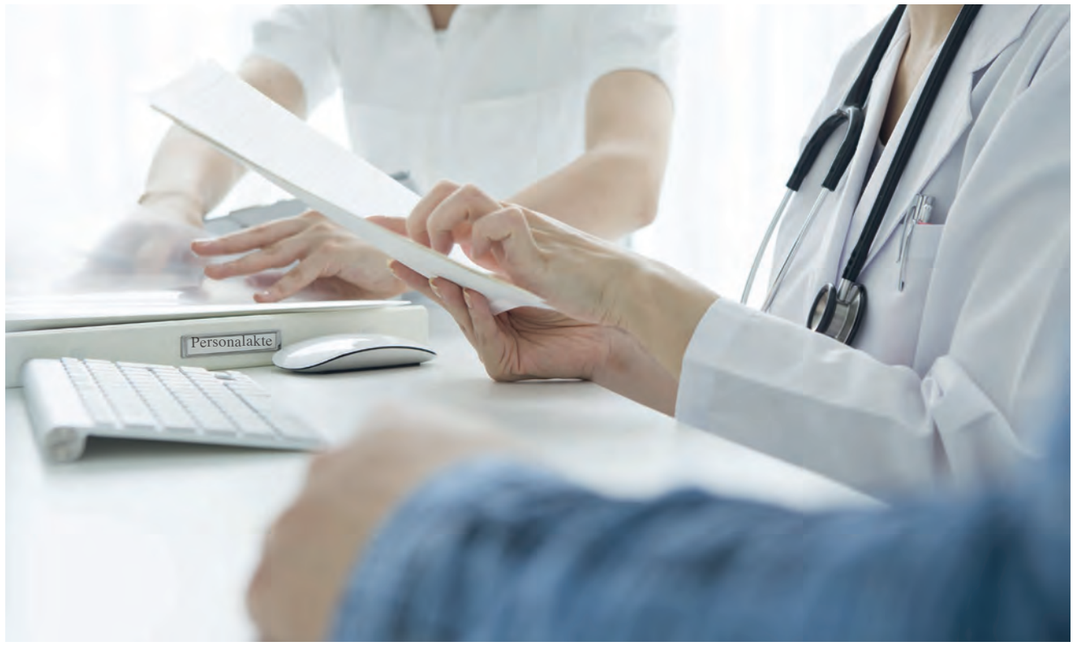
Die grundsätzliche Einsicht in die Personalakte durch den Betriebsrat ist nicht zulässig. Nur in Sonderfällen und mit Zustimmung des Arbeitnehmers kann das Einsichtsrecht eingeräumt werden.

Protokollierung
Zur Nachverfolgung von Änderungen an Patientendaten werden häufig die Zugriffe von Mitarbeitern und Änderungen im KIS protokolliert. Bei einem begründeten Verdacht auf Missbrauch können die Protokolldaten ausgelesen werden. Allerdings darf dieses Vorgehen a) nicht zur Mitarbeiterüberwachung durchgeführt werden, und b) darf das Einsehen der Datei nur nach dem Vier- oder Mehraugenprinzip vorgenommen werden.

Beispielsweise sollte die Datei demnach nicht von der Geschäftsführung allein eingesehen werden dürfen, sondern zusätzlich der Datenschutzbeauftragte und die Mitarbeitervertretung anwesend sein.

Auskunft gegenüber Behörden

Das gilt auch für die Anfragen von Behörden, wie die der Polizei oder Staatsanwaltschaft in Bezug auf eine richterliche Vorladung oder ein laufendes Ermittlungsverfahren, genauso aber auch von Sozialämtern, die in der Regel prüfen, inwieweit bestimmte Bezüge gerechtfertigt waren.



Das Löschen von Daten sollte immer unter Abwägung und Berücksichtigung von möglichen Archivierungspflichten stattfinden.

Grundsätzlich gilt, dass Sie keine voreiligen Auskünfte geben sollten. Prüfen Sie zuerst, ob Sie berechtigt sind, die erhobenen Daten überhaupt weiterzugeben. Dies kann z. B. durch Vorgaben der Strafprozessordnung der Fall sein. Beantworten Sie Anfragen nicht per E-Mail oder am Telefon, und lassen Sie sich das Ermittlungsaktenzeichen geben. Bei Anfragen Externer ist immer große Vorsicht und die Einzelfallprüfung geboten.

Nach der Kündigung

Auch nach der Beendigung des Arbeitsverhältnisses hat der Arbeitnehmer das Recht zur Einsicht in die Personalakte. Gleichzeitig kann der Arbeitnehmer aber von seinem Anspruchsrecht Gebrauch machen oder Versorgungsansprüche geltend machen, woraus sich eine Archivierungspflicht bis zu 30 Jahren ergibt. Zur Archivierung von Dokumenten sollten geeignete Datenträger und räumliche Gegebenheiten genutzt werden, die bestmöglich vor externen Einflüssen, wie Überschwemmungen, Einbrüchen oder Feuer, geschützt sind.

Abschließendes

Bei Mitarbeiterdaten handelt es sich ebenso um personenbezogene Daten, wie die der Patienten. Im Behandlungsalltag existieren aber noch Verbesserungspotenziale in Hinblick auf die Mitarbeitersensibilisierung im Umgang mit anderen Mitarbeiterdaten. Eine zentrale Aufgabe kommt hier der Zusammenarbeit von Qualitätsmanagement, Personalwesen, Betriebsrat, Datenschutzbeauftragtem und Informationssicherheitsbeauftragtem zu, um gemeinsam die datenschutzrechtlichen Interessen von Mitarbeitern zu vertreten. ■

Nina Richard

Kommunikation als Brückenbauer

Vor 20 Jahren schlossen sich vier technische Fachverbände des Gesundheitswesens auf Anregung des Siemens-Managers Max Heymann zu einem Krankenhaus-Kommunikations-Centrum zusammen, um einen Gemeinschaftsstand auf der Krankenhausmesse MEDICA in Düsseldorf finanzieren zu können. Sehr schnell entwickelte sich diese lose Zusammenarbeit zu einem Erfolgsmodell, und die gemeinsame Plattform wurde zunehmend als Treffpunkt und Erfahrungsaustausch von vielen Einrichtungen des Gesundheitswesens genutzt.

Vier Jahre später wurde ein Verein mit gemeinnütziger Ausrichtung gegründet, und unter dem Motto „Brücken bauen" mit dem Ziel „über den Tellerrand schauen" entstand durch die Zusammenführung aller Kontakte und Ressourcen ein beeindruckendes Netzwerk. Der Verein versteht sich als unabhängige neutrale Plattform seiner Mitglieder und vertritt somit keine partikulären Interessen, sondern setzt sich unparteilich und kompetent für Transparenz und Effizienz ein. Die interdisziplinäre Vernetzung aller Akteure im Gesundheitswesen und deren Austausch von Standpunkten haben oberste Priorität.

Eine zentrale Aufgabe kommt hierbei der KKC-Expertengruppe IT-Sicherheit und Datenschutz zu. Deren Mitglied Prof. Dr. Thomas Jäschke ist gleichzeitig im Wissenschaftlichen Beirat des KKC vertreten. Neben dem Datenschutz und der IT-Sicherheit, insbesondere seit dem Eindringen von Big-Data- und Data-Warehouses-Konzepten in die Krankenhäuser und der elektronischen Gesundheitskarte, sind weitere komplexe Herausforderungen zu bearbeiten und mit anderen Expertengruppen des KKC zu koordinieren, als da sind:

- Telemedizin: Telemonitoring, Ambient Assisted Living
- MIT: Die Zusammenführung von Medizintechnik und IT zu einem gemeinsamen Fachgebiet
- Labormedizin: Labautomation, Lab-on-a-chip
- Medizin 4.0: Biotechnologie, personalisierte Medizin, eHealth-Apps
- Pflegemanagement: IT-Einsätze in der Pflege, Robotik
- Aus- und Fortbildung: VICENNA-Akademie des KKC, Gesundheitscontroller, Lernen 4.0, Hochschule 4.0, Zukunftswerkstätten
- Krankenhaus 4.0: Energie-, Einkaufs-, Hygiene-, Wissens-, Pflege-, Qualitäts-, Risikomanagement, Auswirkungen der neuen Krankenhausreform

Prominente Beiratsmitglieder des VDE Frankfurt, des TÜV Rheinland, der Berliner Ärztekammer, des Deutschen Pflegerates, der Fachgesellschaften, von Hochschulen und Kliniken stellen hierfür ihr Know-How und ihre Kontakte zur Verfügung. Förderpartner wie Intel Deutschland, Ingram, GS 1, AMC, ASCOM, TipGroup, ITZ-Medi und ITR Informationstechnologien GmbH unterstützen mit ihren Fachleuten und MEDICA-Ständen die Arbeit des KKC. Hinzu kommen noch Kooperationen mit mehreren Hochschulen, vier Fachverlagen und dem Fraunhofer-Institut ISST Dortmund. Durch seine Mitgliedschaft in der Mittelstandsallianz des Bundesverbandes Mittelständische Wirtschaft (BVMW) ist das KKC auch auf der politischen Bühne zur digitalen Agenda zu finden. Als aktives Mitglied in der GuiG – Gesellschaft für Unternehmensführung und IT-Service-Management in der Gesundheitswirtschaft mit ihrer „Entscheiderfabrik" hat das KKC einen guten Zugang zum Verband der Krankenhausdirektoren Deutschlands (VKD), 24 anderen Verbänden und einer Vielzahl von spezialisierten IT-Unternehmen.

Künftig wird das KKC auf seiner Webseite www.kkc.info und über Social Media Beiträge des ISDSG und das Magazin ExperSite verlinken. ■

Manfred Kindler (KKC)

Update BDSG

Die Datenschutzbranche kann sich über ruhige Zeiten nicht beschweren. Eine Flut neuer Rechtsvorschriften, Normen und IT-Sicherheitsfragen prägt derzeit die Szene und führt naturgemäß zum erhöhten Bedarf praxisbezogener Informationsveranstaltungen für das Gesundheits- und Sozialwesen.

Dies ist der Grund, weshalb 2013 die Tagungsreihe Datenschutz in der Medizin des Veranstalters Update-BDSG ins Leben gerufen wurde. Die Menge der seit einigen Jahren neu veröffentlichten gesetzlichen Vorschriften und Regelwerke zum Datenschutz im Gesundheitswesen ist überdurchschnittlich groß und bedarf vor der Umsetzung oftmals der Erläuterung für die Fachwelt. Die Risiken für Patientendaten wachsen überproportional mit gesteigertem Einsatz der IT in den Verwaltungen medizinischer Einrichtungen. Regelmäßig veröffentlichte Studien zeigen beispielsweise, dass diese Risiken durch zu große Lücken in der Unternehmens-IT vergrößert werden. Auch der Prüfungsdruck auf betroffene Unternehmen durch die Aufsichtsbehörden steigt messbar, mit der Folge von repressiven Maßnahmen und Bußgeldverfahren.

Datenschutz in der Medizin – Update BDSG 2015: ein Rückblick

Als vierte Veranstaltung zum Thema Datenschutz in der Medizin fand die Tagung am 12.11.15 in Leipzig als letzte Tagung des Jahres, unter der Schirmherrschaft des Thüringer Landesbeauftragten für Datenschutz und Informationsfreiheit, statt und beschäftigte sich in den Fachvorträgen, wieder mit besonders aktuellen Themen.

In seinem Vortrag „Wandel in Struktur, Methodologie und Technologie des Gesundheits-und Sozialwesens – Konsequenzen für den Datenschutz" beleuchtete Herr Professor Bernd Blobel, ein Vertreter der Universität Regensburg, die besondere Veränderung der rechtlichen und IT-technischen Rahmenbedingungen des medizinischen Datenschutzes in Deutschland und damit auch die geänderten Aufgaben eines Datenschutzbeauftragten. Zum anderen wachsen permanent die Datensätze zu einem Patienten aufgrund stark personalisierter Medizin, besserer Analysemöglichkeiten und effizienter Datenstrukturen, in denen sie ausgewertet werden können.

Ein weiteres Thema, das zudem in den nächsten Jahren noch in weiten Teilen der politischen und rechtlichen Gestaltung des deutschen Datenschutzrechts auch im Gesundheitssektor bedarf, ist die EU-Datenschutzgrund-Verordnung, deren Fassung seit Jahren in den zuständigen Gremien hart umkämpft ist. Die im Entwurf bekannten Fassungen ließen für den Referenten und Datenschutzexperten Bernd Schütze den Schluss zu, dass manche, bisher selbstverständliche Regeln deutlich geändert werden, wie beispielsweise die Frage der Form einer Einwilligung, die, gemäß des Entwurfs, nicht mehr zwingend schriftlich sein muss.

Herr Bertram Raum brachte aus seiner Beratungs- und Prüfpraxis bei der BfDI die übergreifenden rechtlichen Rahmenbedingungen und Umsetzungserfahrungen mit, die sich aktuell bei großen medizinischen Forschungsprojekten ergeben, in denen Big-Data-Erfahrungen naturgemäß eine Rolle spielen. Jedes Forschungsprojekt bedarf eines rechtskonformen Datenschutzkonzepts, bei dem der Leitfaden der TMF für die klinische Forschung eine Orientierung bietet. Den abschließenden Rahmen der Tagung bot die Rechtsberatungsperspektive.

Rechtsanwalt Matthias Klein informierte über ein Thema, das leider erst langsam in das Rechtsbewusstsein von Verantwortlichen eindringt: die Compliance als übergreifender, innerbetrieblicher, rechtlicher Rahmen für alle Verwaltungsprozesse, der die Konformität mit geschriebenen und ungeschriebenen Regelwerken sicherstellen soll. Dazu gehört auch der Datenschutz. Er wies auf die Folgen bei Verstößen und auf ein angekündigtes neues Gesetz hin, das für Unternehmen und deren verantwortliche Leiter erhebliche Folgen zeitigen kann: das sog. Verbandsstrafgesetzbuch. Die letzte Referentin des Tages, Julia Dönch, griff tief in die Kiste ihrer reichhaltigen Erfahrungen bei der Rechtsberatung, insbesondere von Kliniken. Einfachste Regeln des Schutzes der Patientendaten werden oftmals nicht beachtet. Das Ergebnis ihrer Feststellungen waren konkrete Handlungsempfehlungen für den Klinikalltag.

Datenschutz in der Medizin – Update BDSG geht 2016 wieder an den Start. Weitere Informationen unter **www.update-bdsg.com.** ■

Manfred Weitz

Dariush Ansari, Geschäftsleiter bei Network Box Deutschland GmbH

IT-Lösungen vom Anbieter verwalten lassen

Managed Services im Gesundheitswesen: sinnvolles Outsourcing oder Datenschutzfalle?

Längst ist eine ausgereifte IT-Struktur eine unerlässliche Voraussetzung geworden, um den modernen Krankenhausalltag zu bestreiten und z. B. Patientendaten zu verwalten, Befunde zu sichten oder mit den Kassenärztlichen Vereinigungen (KVen) zu kommunizieren. Es steht außer Frage, dass der Großteil der hier verarbeiteten Informationen hochsensibel ist und weder in die falschen Hände geraten noch verloren gehen darf. Das macht den Faktor Sicherheit als Anforderung an IT-Systeme und Kommunikationswege unabdingbar.

Dem stehen knappe Personal- und Zeitressourcen gegenüber, die es häufig verhindern, neue IT-Lösungen zu integrieren und zu pflegen. Eine Option, trotz geringer Ressourcen technisch gut ausgestattet zu sein: das Outsourcing mittels Managed Services. Hier pflegt und aktualisiert der Anbieter die Lösung, während Einrichtungen sich auf das Tagesgeschäft konzentrieren können.

Mit der zunehmenden Digitalisierung und der immer höher werdenden Erwartung der Anwender an die IT werden auch die Forderungen nach neuen Programmen und Systemen, die den Arbeitsalltag erleichtern, lauter. Theoretisch ließen sich diese Wünsche auch erfüllen, wären da nicht die komplexen Systemeinführungen, die oftmals mit einem gewissen Grad an Individualisierung (Customizing) verbunden sind und damit monetäre, personelle und zeitliche Ressourcen in Anspruch nehmen. Bei einigen Anwendungen würden selbst große IT-Teams in Hinblick auf die Komplexität und den damit verbundenen Aufwand an ihre Grenzen stoßen. Aus diesem Grund weichen immer mehr Organisationen auf sogenannte Managed Services aus: IT-Dienstleistungen, die ein externer Anbieter bereitstellt und pflegt. Bei diesen sogenannten Managed Service Providern (MSP) kann der Kunde verschiedene standardisierte Dienstleistungen buchen, die anschließend genau auf seine Bedürfnisse abgestimmt werden. Entwicklung, Produktkonfiguration, Betrieb sowie Updates verantwortet der Provider; der Kunde nutzt den Service.

> *Eine Option: das Outsourcing mittels Managed Services*

Als Managed Services werden oftmals Dienstleistungen angeboten, die den täglichen Betrieb und die Verwaltung von Netzen und Diensten effizienter machen. Das können unternehmenskritische und sicherheitsrelevante Anwendungen sein, aber auch Lösungen für Netzwerkbetrieb und -verwaltung mit Fernüberwachung, die Bereitstellung von Diensten und die Unterstützung der User. Beispiele dafür sind Firewalls, VPN-Verbindungen, Anti-Malware-Systeme und Content Filtering. Mittels Managed Services profitieren Anwender von professionellen IT-Services – auch dann, wenn sie nur ein kleines Budget haben, im Tagesgeschäft oder zum tiefgreifenden Erlernen der Technologien zu wenig Zeit bleibt.

Brennpunkt IT-Sicherheit

Eine wichtige Grundlage des Krankenhausalltags ist die IT-Sicherheit, ein heutzutage sehr komplexes Thema im Bereich der Informationstechnologie. Die IT-Sicherheit gehört zweifelsohne in das Risikomanagement mit direktem Einfluss auf die Betriebskontinuität und benötigt daher eine besondere Betrachtung. In wohl keinem anderen Bereich der IT ist die lückenlose Verwaltung der Sicherheitssysteme so abhängig von der zu investierenden Zeit bzw. Pflege und notwendigen Kompetenz. Relevante Sicherheitsupdates, Patches und ein ganzheitliches, proaktives Monitoring der Systeme durch eigene Ressourcen sind meist kaum etabliert und daher bei Weitem keine Routine. Es braucht Ressourcen, um die unterschiedlichen Gefahrenpotenziale erkennen und bannen zu können.

> *Es braucht Ressourcen, um die unterschiedlichen Gefahrenpotenziale erkennen und bannen zu können.*

Allein die Instandhaltung der Sicherheits-Appliances (Netzwerkkomponenten und Endgeräte, deren Software auf eine Anwendung ausgerichtet ist) kann kaum noch in Eigenleistung erbracht werden. Die Buchung eines passenden Managed Services kann den Vorteil haben, in diesem Bereich Kompetenzen gezielt zu ergänzen und das Personal zu entlasten. Vermeintlich „einfache" Aufgaben wie Hotfixes, Patches, Updates etc., die Routine sind, können problemlos an externe Dienstleister gegeben werden. Danach bleibt für die IT-Abteilungen der Einrichtungen mehr Zeit, Arbeitsabläufe zu implementieren.

Finanziell planbar

Zudem profitieren Kliniken und Krankenhäuser bei Managed Services von finanzieller Transparenz. Für die ausgelagerten Dienste müssen keine Lizenzkosten getragen werden, da die Produkte nicht selbst gekauft werden. Die Mitarbeiter der IT können sich auf ihre Kernkompetenzen konzentrieren, da die externen IT-Experten des jeweiligen Dienstleisters die Geschäftskontinuität sichern. Seriöse MSP bieten überschaubare, transparente Kostenmodelle, mit denen Kunden zuverlässig planen können. Sollte sich herausstellen, dass bestimmte Services überflüssig sind oder auch dringend gebraucht werden, lassen sie sich flexibel abbestellen bzw. hinzubuchen – ohne Mehrarbeit.

Gemanagte KV-SafeNet-Anbindung

Besonders interessant für Krankenhäuser ist ein Provider mit einer KV-SafeNet-Zertifizierung. Der KV-SafeNet-Anschluss stellt einen geschützten, vom Internet getrennten „Tunnel" her, der eine datenschutzgerechte Anbindung aller Rechner der jeweiligen Einrichtung ermöglicht.

Dieser besonders abgesicherte Anschluss ist in vielen Bundesländern bereits verpflichtend. Benötigt werden dazu lediglich internetfähige Computer und ein herkömmlicher Internetanschluss. Über den KV-SafeNet-Router wird dann ein virtuelles privates Netzwerk (VPN) aufgebaut. Dies funktioniert mit nahezu allen Betriebssystemen wie Windows und Linux. Manche MSP bieten die Möglichkeit, zusätzlich zum KV-SafeNet-Anschluss weitere Managed Services zum Schutz der IT-Infrastruktur zu buchen. Hier lohnt sich ein Vergleich der Anbieter im Hinblick auf Preise und Angebotsumfang.

Sehr wichtig: Datenschutz!

Doch wie steht es generell um den Datenschutz, wenn eine dritte Partei hochsensible Daten verarbeitet und überträgt? In Bezug auf den KV-SafeNet-Anschluss ist sichergestellt, dass die Webserver der KVen so konfiguriert sind, dass sie ein Höchstmaß an Sicherheit gewährleisten und Daten nur über geschützte Verbindungen zwischen Server und Nutzer übertragen werden. Dass der Internetzugang sicher ist, muss die Einrichtung aber selbst sicherstellen. Hinsichtlich weiterer Managed Services eines MSP ist konkret zu prüfen, welche Datenschutzanforderungen der Anbieter erfüllt; ob er z. B. alle Daten in Deutschland hostet und damit den deutschen Gesetzen unterliegt oder ob Gesetze aus dem Ausland gelten, weil in einem anderen Land gehostet wird. Einen ersten Eindruck über das Sicherheitslevel geben Zertifizierungen z. B. nach den DIN-Normen ISO 9001 (Qualitätsmanagement), 20000 (IT-Service-Management) und 27001 (Informationssicherheit).

Wenn vorhanden, sollten der Datenschutzbeauftragte oder der IT-Sicherheitsbeauftragte unbedingt mit in die Entscheidung für einen MSP einbezogen werden. Zudem ist die Abstimmung mit der IT-Abteilung etc. notwendig.

Fazit

IT-Sicherheitsmaßnahmen sind nur dann effektiv, wenn sich Experten kontinuierlich darum kümmern. Im hektischen Krankenhausalltag ist dies aus verschiedenen Gründen meist jedoch kaum zu schaffen. Für Abhilfe können Managed Services sorgen, über die IT-Aufgaben auf einen vertrauenswürdigen Dienstleister übertragen, sprich outgesourct werden. Maßgeschneiderte Leistungspakete tragen dazu bei, dass die Betriebskosten sinken und die Einrichtung trotz limitierter eigener Kapazitäten voll geschützt ist, da sich die Experten des Dienstleisters um Konfiguration und Pflege kümmern. Der Leistungsnehmer nutzt die angebotenen Funktionen und kann sie bestenfalls flexibel ab- bzw. hinzubuchen. Durch die individuelle Anpassung sind diese Leistungen prinzipiell für jede Einrichtung im Gesundheitswesen interessant. ■

Dariush Ansari

Network Box Deutschland GmbH

Network Box liefert umfassende und gemanagte IT-Sicherheitslösungen am Gateway und sorgt mit skalierbaren und modularen Systemen für ein Höchstmaß an Sicherheit. Dazu betreibt das Kölner Unternehmen ein weltweites Netzwerk von Security Operation Centern (SOC). Auch für kleine Unternehmen und den Mittelstand bietet Network Box Managed Security Services auf Basis eigener Hard- und Software an. Alle Sicherheits-Features werden über die patentierte PUSH-Technologie vollautomatisch auf dem neuesten Stand gehalten und bei Updates in Sekundenschnelle aktualisiert. Interessant für Einrichtungen aus dem Gesundheitswesen: Network Box ist zertifizierter KV-SafeNet-Anbieter und hält ein spezielles Anschluss-Bundle mit verschiedenen Security-Dienstleistungen, darunter erweitertes Firewalling, Content Filter oder Anti-Malware bereit. Die Lösungen sind modular aufgebaut und lassen sich so auf verschiedene Bedürfnisse und Budgets ausrichten.

Die Network Box ITP-S-68i

Die Kanzlei Przytulla & Kollegen wurde 1999 von Herrn Rechtsanwalt Fritz-Martin Przytulla LL.M. gegründet.

Wir sind vornehmlich im Zivilrecht für Mandantinnen und Mandanten, seien dies gewerbliche Unternehmen oder Privatpersonen, tätig. Selbstverständlich bearbeiten wir auch Vorgänge des öffentlichen Rechtes. Bei notariellen Fragen steht Ihnen der Notar, Fritz-Martin Przytulla LL.M., gern mit Rat und Tat zur Seite.

Im Interview mit …

RA Fritz-Martin Przytulla LL.M.

Fachanwalt für Arbeitsrecht

ISDSG: Welchen Stellenwert hat das Thema „Beschäftigtendatenschutz" Ihres Erachtens im Gesundheitswesen?
Der Beschäftigtendatenschutz müsste einen sehr viel höheren Stellenwert im Gesundheitswesen einnehmen. Damit würde nicht nur den Beschäftigten verdeutlicht werden, welche besondere Sensibilität, Aufmerksamkeit und Vorsicht beim Datenschutz insgesamt geboten sind. Damit würde auch erreicht werden, dass der Respekt vor den Daten anderer Menschen, insbesondere den sensiblen Gesundheitsdaten, eine absolute Priorität im Gesundheitswesen haben muss.

Der Beschäftigtendatenschutz ist auch deshalb von Bedeutung, weil damit die Möglichkeit unzulässiger Einflussnahmen, Personaldruck oder Manipulationen durch Kenntnis von Daten der Beschäftigten vermieden werden können. Wer z. B. über die Vergabe von Transplantationsgut zu entscheiden hat, muss persönlich unangreifbar sein!

Die Videoüberwachung ist in der Praxis ein häufig eingesetztes Mittel zum Schutz vor beispielsweise Einbrüchen – kann aber (in begründeten Fällen) auch zur Mitarbeiterüberwachung eingesetzt werden. Oder?
Es ist sicherlich richtig, dass derartige Videoobjektüberwachung zur Kontrolle von Gebäuden/Gebäudeteilen sehr häufig praktiziert wird und auch notwendig ist. Im Bereich des Gesundheitswesens, z. B. bei Krankenhäusern oder auch Pflegeeinrichtungen, erscheint die Mitarbeiterüberwachung nicht in jedem Falle sofort möglich. Etwas anderes gilt nur, wenn z. B. in Großraumbüros, die aber im Gesundheitswesen vermutlich seltener sind, derartige Videoüberwachungen ganztägig laufen würden und damit auch die jeweilige tägliche Arbeitszeit – während der normalen Arbeitsstunden – kontrolliert werden könnte, d. h. das Verhalten der einzelnen Beschäftigten am jeweiligen Arbeitsplatz.

Nach der Rechtsprechung des Bundesarbeitsgerichtes dürfen derartige Überwachungsmaßnahmen nicht „rund um die Uhr" in einem permanenten Einsatz erfolgen. Vielmehr ist das zeitweilige Laufen derartiger Überwachungssysteme dann zulässig.

Es müssen aber auch Pausen davon gegeben sein, und die Beschäftigten müssten darüber auch informiert werden. Videoüberwachungen in Objekten – etwa an den Eingangstüren – müssen nach dem Bundesdatenschutzgesetz ausdrücklich durch entsprechende, deutlich lesbare Hinweise kenntlich gemacht werden.

Im Übrigen kann der Arbeitgeber die Dinge entkrampfen, wenn er z. B. den Arbeitnehmer schon bei einer Einstellung auf Videoüberwachungen hinweist, aber eben auch die Durchführung derartiger Kameramaßnahmen jeweils angezeigt wird.

Es bietet sich auch für die Unternehmen in diesen Bereichen an, die Arbeitnehmer in die Erhebung von Daten jeweils durch eine entsprechende Erklärung einwilligen zu lassen oder betriebliche Vereinbarungen abzuschließen. Heutzutage muss man aber an neue elektronische Systeme denken, die zwar einerseits den Patienten dienen; andererseits aber auch eine Mitarbeiterüberwachung auslösen können, wie z. B. Rufsysteme für Patienten, die zugleich den Rückschluss zulassen, wann etwa die betreffende Krankenschwester auf den Ruf reagiert hat. Insoweit ergeben sich vielfältige Kontrollmöglichkeiten.

Die Erhebung von welchen Mitarbeiterdaten halten Sie für unkritisch? Und an welcher Stelle muss der Mitarbeiter sie zur Verfügung stellen?
Die Erhebung von Mitarbeiterdaten halte ich grundsätzlich für bedeutsam. Schon ein simples Datum wie der Geburtstag kann durchaus eine Bedeutung haben. Normalerweise muss der Arbeitnehmer aber sein Geburtsdatum, die Sozialversicherungsdaten, seinen Familienstand und seine Adresse mitteilen. Im Übrigen wird dies ja auch über die Lohnsteuerdaten dem Arbeitgeber bekannt. Auf derartige Daten hat der Arbeitgeber einen Anspruch, weil er eben die Abrechnung mit der Abführung von Sozialversicherungsbeiträgen und Steuern durchzuführen hat. In diesem Zusammenhang werden dann auch in aller Regel die Kinder genannt. Soweit es sich um besondere Vertrauenspositionen handelt, kann der Arbeitgeber auch Spezialfragen stellen. Die Frage nach der Schwangerschaft bzw. von körperlichen Gebrechen wird heutzutage als unzulässig angesehen – soweit nicht ein besonderer Grund in der Funktion, die der Arbeitnehmer ausfüllen soll, gegeben ist. Der Grad der Behinderung müsste aber nach Eintreten des Kündigungsschutzes entsprechend KSchG dem Arbeitgeber mitgeteilt werden, damit dieser die Beschäftigung auch im Hinblick auf die notwendigen Quoten nach dem SGB IX zugrunde legen kann.

Angaben zur Ausbildung werden selbstverständlich auch benötigt und sind zu erteilen, soweit dies für die Erfüllung der Arbeitsaufgaben hilfreich oder notwendig ist. Ansonsten bedarf es einer Abwägung im Einzelfall; ggf. auch der Einholung von rechtlichem Rat. Größere Datenmengen würde ich grundsätzlich niemandem zur Verfügung stellen. Insoweit gibt es ja auch keine Garantie dafür, dass nicht Daten einmal zweckentfremdet werden. Auch dies ist ein Grund für einen effektiven Datenschutz.

Stichwort: OH-KIS. Gemäß der Orientierungshilfe Krankenhausinformationssysteme müssen Zugriffe auf Patientendaten protokolliert werden. Wie sollte daher die Einsichtnahme in Protokolldaten aussehen?
Das Thema Protokollierung kann aus zwei Perspektiven betrachtet werden. Aus Perspektive des Beschäftigtendatenschutzes muss bewusst sein, dass grundsätzlich die Zugriffe von Mitarbeitern auf Patientendaten dokumentiert werden. Bei der zweiten Perspektive handelt es sich um die Patientenseite. Allgemein lässt sich zunächst festhalten, dass der Zugriff auf Patientendaten regelmäßig einer Einwilligung bedarf. Diese sollte der Patient möglichst konkret bereits in seinem Aufnahmebogen abgegeben haben. Unspezifische Formulierungen sind zu vermeiden.

Bei der Einsichtnahme von Protokolldaten sollte ein „Protokoll" geführt werden, und am besten sollte die Durchführung durch mindestens zwei Personen erfolgen, die den Gang der Einsichtnahme, den Grund hierfür und den Umfang sowie den Vollzug des Einsichtsvorganges dann ihrerseits in einem Protokoll festhalten. Das Protokoll wäre durch beide Personen (oder mehr) abzuzeichnen. Bei der Einsichtnahme von Mitarbeiterdaten sollte eine andere Person anwesend sein. ■

Interview: Nina Richard

Ihre Aufgaben im Mitarbeiterdatenschutz

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

Als Ansprechpartner für Betroffene stehen Sie als Datenschutzbeauftragter auch den Mitarbeitern für Datenschutzanliegen zur Verfügung. Das geht mit einer Reihe von Aufgaben einher.

DSB als Ansprechpartner

Jeder Mitarbeiter hat gegenüber seinem Arbeitgeber die gleichen Rechte nach § 33 bis § 35 BDSG. So kann ein Mitarbeiter Einsicht in seine Personalakte nehmen, diese ggf. korrigieren oder löschen bzw. sperren lassen. Mit der Inanspruchnahme dieser Rechte kann sich jeder Mitarbeiter direkt an den betrieblichen Datenschutzbeauftragten wenden.

OH-KIS fordert VIP-Kennzeichen

Die Orientierungshilfe Krankenhausinformationssysteme fordert für Patientendaten von Mitarbeitern eine entsprechende Kennzeichnung (VIP-Kennzeichen) mit eingeschränkten Zugriffsberechtigungen (siehe Anforderung 1.12 Teil 2 der OH-KIS). Die Zugriffe auf diese Daten sind entsprechend zu protokollieren. Unter keinen Umständen darf das VIP-Kennzeichen dazu genutzt werden, eine gekennzeichnete Person zu suchen.

Sensibilisierung der Mitarbeiter durch den DSB

Neben der Begleitung der Umsetzung des VIP-Kennzeichens kann der betriebliche Datenschutzbeauftragte die Mitarbeiter dahingehend sensibilisieren, dass ein unbefugter Zugriff auf Patientendaten von Mitarbeitern organisatorisch geregelt wird, z. B. durch Schulungen oder Informationsschreiben. In konkreten Spezialschulungen für Mitarbeiter der Personalabteilung, aber auch für medizinische Fachkräfte und Mitarbeiter der Verwaltung sollte über den Datenschutz aufgeklärt werden. Des Weiteren kann die enge Zusammenarbeit mit anderen Abteilungen wie Personalwesen, Qualitätsmanagement oder Betriebsrat hilfreich sein. ■

Alexander Vogel

4. Goldene Regel: Videoüberwachung

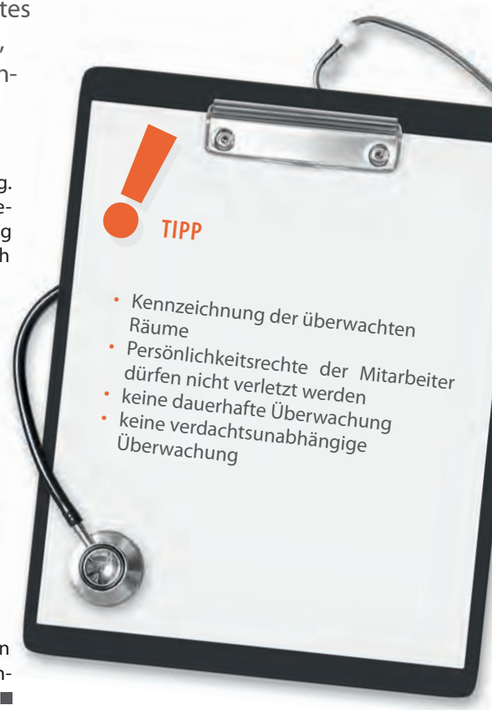
Die sogenannte optisch-elektronische Überwachung kann ein probates Mittel zur Aufklärung von kriminellen Handlung wie bspw. Diebstahl, Einbruch oder Vandalismus darstellen. Aus Perspektive des Arbeitnehmerdatenschutzes sollte die Installation wohlüberlegt sein.

Das Bundesdatenschutzgesetz regelt in § 6b die Videoüberwachung. Demnach ist eine Videoüberwachung von öffentlich zugänglichen Räumen, beispielsweise Haupt- und Nebeneingänge von Krankenhäusern, zwar gestattet, jedoch nur unter Einhaltung bestimmter Rahmenbedingungen. So ist die Videoüberwachung nur dann zulässig, wenn sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen, z. B. zum Schutz vor unbefugtem Betreten, Diebstahl oder Vandalismus dient.

Hierbei sind jedoch die schutzwürdigen Rechte anderer Dritter zu beachten. Des Weiteren ist die Videoüberwachung durch gut sichtbare Kennzeichnung erkennbar zu machen, z. B. durch Hinweisschilder vor Betreten des Beobachtungsraumes. Zu den schutzwürdigen Rechten gehört auch die Privatsphäre von Mitarbeitern. So ist eine dauerhafte und verdachtsunabhängige Videoüberwachung der Arbeitsplätze unverhältnismäßig und nicht zulässig. Hinzu kommt, dass der ursprünglich begründete Zweck der Videoüberwachung regelmäßig überprüft werden muss. Nach einer umfassenden Abwägung der Interessen beider Seiten (Arbeitgeber und -nehmer) mit dem Ergebnis, dass das schutzwürdige Interesse des Arbeitgebers überwiegt, kann eine vorübergehende und verdachtsabhängige Videoüberwachung der Arbeitsplätze zulässig sein.

Ein Beispiel ist die Videoüberwachung von Kassenbereichen zum Schutz vor Überfällen. Jedoch muss dafür ein konkreter Tatverdacht vorliegen und diesem durch keine andere Art und Weise Abhilfe geschaffen werden können. In jedem Fall sollten die Mitarbeiter vor der Installation einer Videoüberwachung ausreichend informiert werden. ■

Alexander Vogel



Impressum

ExperSite Ausgabe 01 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: shutterstock, Vasin Lee; S. 2: iStock, Yuri Arcurs; S. 3: shutterstock, Leonardo da; S. 3: Falko Wübbecke, Dortmund; S. 4/5: Falko Wübbecke, Dortmund; S. 6: shutterstock, Alexander Kirch; S. 6: T. Jäschke; S. 8/9: shutterstock, wavebreakmedia; S. 10: shutterstock, S L; S. 11: shutterstock, Leonardo da; S. 12: iStock, BraunS; S. 13: shutterstock, Matej Kastelic; S.14/15: Network Box Deutschland; S. 16: Kanzlei Przytulla & Kollegen, iStock, dra_schwartz; S.18: shutterstock, Stock-Asso; S. 19: shutterstock, Rashevskyi Viacheslav, John Smith Design; U4: hipaacartoons, R.J. Romero.

Einblicke & Ausblicke

"Go ahead - use unsecured texting to send patient orders. Everybody does it. What could go wrong?"

Wir bedanken uns für die inhaltlichen Beiträge bei:

Dariush Ansari (Network Box Deutschland GmbH)
Manfred Kindler (Krankenhaus-Kommunikations-Centrum)
Manfred Weitz (Update BDSG)
RA Fritz-Martin Przytulla LL.M. (Rechtsanwaltskanzlei Przytulla)

Die nächste Ausgabe erscheint im September 2016

Im Schwerpunkt: Behandlungsbilder und -videos: Die Nutzung für interne und externe Zwecke. So handeln Sie datenschutzkonform.