AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Juli/August 2019 | Seite 1

www.aok-verlag.info/ds-im-blick

INHALT

Ein kleiner Sicherheitscheck

In der Praxis können viele Dinge passieren. Einige Risiken sind jedoch für fast jede Gesundheitseinrichtung relevant. In diesem Beitrag beleuchten wir fünf häufige Risiken und geben Tipps, mit welchen Maßnahmen man sich davor schützen kann.

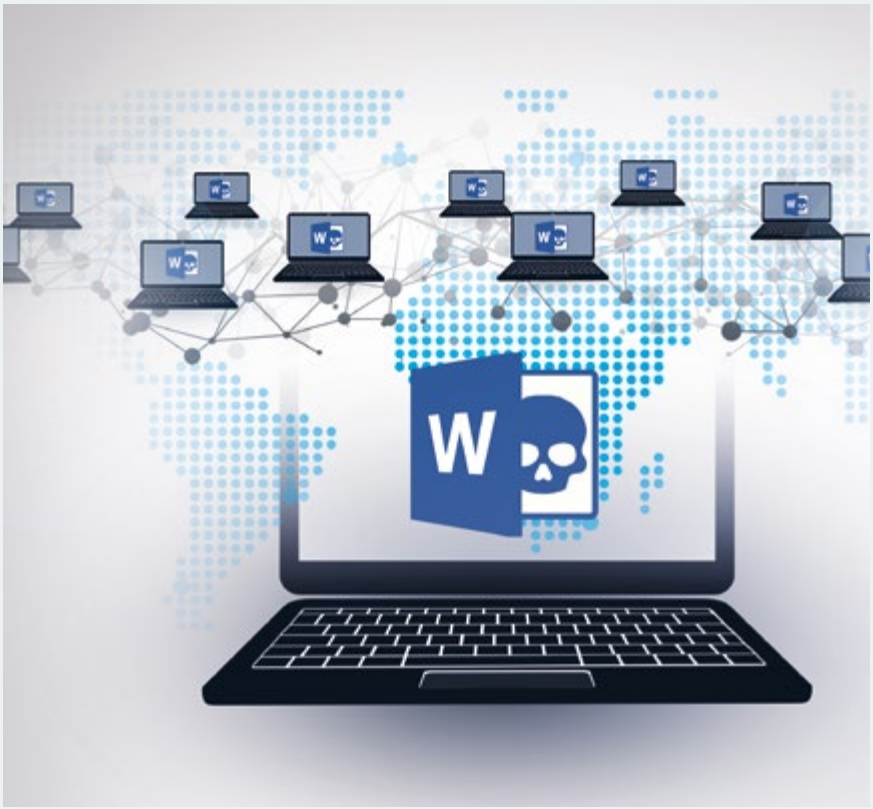
Sven Venzke-Caprarese

Emotet und Microsoft Office-Einstellungen

Seit gut einem halben Jahr wütet Emotet. Hierbei handelt es sich um eine besonders dreiste Variante von Schadsoftware. Ist eine Stelle erst einmal infiziert, greift Emotet in das Mailsystem des Opfers ein und versendet Antworten auf bestehende Mailverläufe. Selbst sensibilisierte Mitarbeiter können solche Mails dann oftmals nicht von einer echten Mail unterscheiden. Denn der Absender ist auf den ersten Blick bekannt. Zudem handelt es sich bei der Mail augenscheinlich um eine Antwort auf eine zuvor versendete E-Mail.

Die Gefahr: Im Anhang befindet sich meist ein .doc Worddokument, welches die Schadsoftware verteilt. Sogar viele Virenscanner sind an dieser Stelle machtlos. Die Schadsoftware kann sich allerdings nur dann erfolgreich verbreiten, wenn der Nutzer das Word-Dokument öffnet und auf Nachfrage des Programms die Makrofunktionen aktiviert. An dieser Stelle kommt es also auf das richtige Verhalten der einzelnen Mitarbeiter an. Wissen wirklich alle, dass Makros grundsätzlich nicht aktiviert werden sollten? Kann man wirklich sichergehen, dass sich jeder Mitarbeiter daran hält?

Die Antwort auf die Fragen lautet häufig „nein“. Es sollten daher neben weiteren Mitarbeitersensibilisierungen für das Thema Schadsoftware vor allem auch technische Maßnahmen getroffen werden.



Viele Einrichtungen entscheiden sich an dieser Stelle, die entsprechende Makro-Funktion aller MS-Office Programme (also nicht nur Word, sondern auch Excel, PowerPoint etc.) mittels übergreifender Softwarerichtlinie zu deaktivieren. Insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu erst kürzlich umfangreiche Handlungshilfen online gestellt und gibt konkrete Tipps und Vorschläge, wie MS-Office Programme auch vor dem Hintergrund von Emotet angemessen sicher betrieben werden können.

Es kann zudem sinnvoll sein, den eigenen Mailserver so einzustellen, dass dieser gar keine betroffenen Dateiformate (also z. B. .doc, .xls, .ppt) mehr annimmt. Was sich im ersten Moment danach anhört, die Arbeitsfähigkeit stark einzuschränken, ist bei genauerer Betrachtung gar nicht so schlimm. Denn die betroffenen Dateiformate sind eigentlich schon seit gut 10 Jahren gar nicht mehr aktuell. Vielmehr stehen modernere Nachfolger (z. B. .docx, .xlsx, .pptx) zur Verfügung. Diese verringern das Risiko, Opfer von Schadsoftware zu werden, erheblich. Und im Zusammenspiel mit den Empfehlungen des BSI dürften Gesundheitseinrichtungen gut gerüstet sein.

TLS und HTTPS

Keine Website ohne HTTPS! Diese Regel ist mittlerweile eigentlich bei allen Gesundheitseinrichtungen angekommen und kann in der Praxis durch einen Blick auf die Website schnell geklärt werden.

Was für Internetseiten gilt, gilt erst recht für E-Mail: Keine E-Mail ohne TLS! An dieser Stelle ist die Überprüfung der Regel aber nicht ganz so einfach. Denn oftmals kann die Frage, ob alle E-Mails bevorzugt per TLS empfangen und versendet werden, nur vom Administrator der Mailserver beantwortet werden. Allerdings kann gelegentlich auch ein kurzer Selbsttest schon Aufschluss geben: Unter der Adresse www.checktls.com/TestReceiver können Mailserver eingetragen und entsprechend getestet werden.

Festplatte voll verschlüsseln

In den meisten Fällen können Gesundheitseinrichtungen nicht ausschließen, dass personenbezogene Daten lokal auf Arbeitsplatzrechnern oder Laptops gespeichert werden.

Insbesondere die Festplatten von Laptops, die das Haus verlassen, sollten daher immer mit einer echten Pre-Boot-Vollverschlüsselung geschützt sein (also einer Verschlüsselung des gesamten Datenträgers). Dies gilt selbst dann, wenn eigentlich die Anweisung besteht, dass keine Dateien lokal auf den Festplatten der Rechner gespeichert werden dürfen. Denn ein näherer Blick enthüllt in der Praxis häufig ein anderes Bild und sei es nur deshalb, weil sich auf den Rechnern temporäre Dateien mit personenbezogenen Daten befinden, die ohne Wissen der Nutzer von den üblichen Office- oder Mailprogrammen angelegt wurden.

Doch was ist mit den Laptops, die das Haus nicht verlassen oder mit den Desktop-Rechnern der Mitarbeiter? Auch hier kann es sinnvoll sein, die Festplatten mit einem entsprechenden Schutz zu versehen. Denn bei einem Einbruch in die Räumlichkeiten sind auch diese gefährdet. Insbesondere bei Außenstandorten mit schlechten Zutrittskontrollmaßnahmen stellt eine solche Verschlüsselung der Desktop-Rechner nicht selten eine gute Maßnahme dar, um die Daten auf den Festplatten vor unbefugten Dritten zu schützen.

Eine gute Vollverschlüsselung zeichnet sich übrigens u. a. dadurch aus, dass Nutzer vor dem Bootvorgang ein Passwort eingeben müssen, damit der Rechner weiter hochfährt und sich entschlüsselt. Zwar gibt es in der Praxis häufig auch den Ansatz, diese manuelle Eingabe des Passwortes durch einen internen Selbstcheck des Clients zu ersetzen (Stichwort Trusted Plattform Module oder kurz TPM). Hierbei prüft der Rech-

ner, ob alle Komponenten bekannt und unverändert sind und entschlüsselt nur in diesem Fall die Festplatte – ohne ein Passwort zu verlangen (sog. TPM-only). Diese Variante hat jedoch ihre Tücken und bietet grundsätzlich weniger Schutz als eine manuelle Passworteingabe. Das BSI verweist auf Schwächen bei der Verwendung von TPM-only.

Mobile Geräte managen

Smartphones und Tablets sind aus dem Alltag vieler Gesundheitseinrichtungen nicht mehr wegzudenken. Gleichwohl sehen sich viele Einrichtungen nach wie vor mit ungeklärten Fragen im Hinblick auf die Absicherung der Mobilgeräte konfrontiert.

Die Fragen beginnen schon mit der Anschaffung der Geräte. Ein Hauptkriterium bei der Anschaffung: Wie lange werden Updates und Sicherheitspatches vom Hersteller bereitgestellt?

Die Fragen gehen dann noch weiter. Dürfen Mitarbeiter das Dienst-Smartphone auch privat nutzen? Oder wird das private mitgebracht und kann als (auch) dienstliches verwendet werden? In beiden Fällen käme es zu einer Vermischung von privaten und dienstlichen Daten. Dies birgt viele Risiken. Denn was ist, wenn die privat genutzte Facebook-App das dienstliche Telefonbuch ausliest und durch einen falschen Klick plötzlich Patienten und Ansprechpartner eine „Freunde"-Einladung erhalten? Abhilfe schafft hier meist nur ein gutes Mobile Device Management-System (MDM) mit echter Containerlösung. Eine solche Lösung trennt private und dienstliche Daten, indem die dienstlichen Daten in einen eigens geschützten „Container", also einen besonders geschützten Speicherbereich, auf dem Mobilgerät verschoben werden. Ein Zugriff von außerhalb des Containers – also z. B. auch von der erwähnten App – kann dann ausgeschlossen werden.

Ein gutes MDM verfügt zudem über eine Anzeige, welche Geräte welchen Patch- und Updatestand aufweisen und lässt verschiedene Einstellungsvorgaben zu – z. B., dass die Passworteingabe am Gerät immer aktiviert sein muss und vom Nutzer selbst nicht ausgeschaltet werden kann. Auch eine Fernlöschung ist häufig möglich, sollte das Gerät als gestohlen gemeldet werden.

Übrigens: Das BSI gibt auch hier gute Tipps, worauf bei der Auswahl eines MDM zu achten ist und definiert Mindeststandards.

Mitarbeiter sensibilisieren

Oftmals birgt nicht nur die Technik Risiken. Häufig kommt es darauf an, Risiken dadurch zu vermeiden, dass Nutzer entsprechend sensibilisiert und geschult sind. Die „Awareness" muss stimmen. Denn noch so viele und gute technische Maßnahmen funktionieren nicht ohne den Faktor Mensch.

Mitarbeiter sollten daher regelmäßig auch im Hinblick auf Security-Awareness geschult werden.

Hierbei können ganz verschiedene Ansätze gewählt werden, z. B.:

- punktuelle Sensibilisierungen per E-Mail und mittels Merkblättern
- E-Learning Kurse, die sich speziell mit dem Thema beschäftigen
- Präsenzschulungen der Mitarbeiter

Es stehen aber auch noch weitere Möglichkeiten zur Verfügung. So können auch Poster, Flyer und Türhängeschilder mit thematischem Bezug die Awareness steigern. Denkbar ist es auch, die Awareness in der Einrichtung zu testen, etwa durch Phishing-Simulationen, bei denen im Auftrag der Einrichtung Mails an Mitarbeiter versendet werden, die Phishing-Mails simulieren. Am Ende einer solchen Simulation stehen meist eine anonyme Auswertung sowie breit aufgestellte Schulungsmaßnahmen, die auf die Simulation Bezug nehmen. In jedem Fall sollten vor einem solchen Vorhaben aber ein etwaiger Betriebs- oder Personalrat sowie der Datenschutzbeauftragte der Einrichtung beteiligt werden.

Vertiefungshinweis im Buch

Mehr Informationen finden Sie in der Loseblattsammlung „Datenschutz im Gesundheitswesen" (AOK-Verlag GmbH), Kapitel M (Mit dem Administrator auf Augenhöhe).

Einsicht in die Behandlungsakte bei mehreren Patienten

Tagtäglich werden Ärztinnen und Ärzte sowie das Klinikpersonal mit Anfragen Dritter konfrontiert, bei denen es vielfach auch um die Einsichtnahme in eine Behandlungsakte geht. Soweit sich das Einsichtsbegehren auf nur eine Patientenakte beschränkt, die für einen bestimmten Patienten vorgehalten wird, bereitet dieser Fall grundsätzlich keine weiteren Schwierigkeiten. Wesentlich komplizierter gestaltet sich hingegen die Situation, wenn zwei oder mehrere Patienten in einer Akte gleichzeitig geführt werden. Wenngleich diese Konstellation in der Praxis nicht häufig vorkommen mag, so wirft sie dennoch eine Vielzahl an Fragen auf, die es im Rahmen dieses Beitrages aufzuzeigen gilt.

Dr. Sebastian Ertel/Patrick Alexander Lis

Der Fall

Ein ehemaliger, mittlerweile volljähriger Patient, kam in einem Krankenhaus zur Welt und wurde kurz nach seiner Geburt zur Adoption freigegeben. Nunmehr bittet er um Einsicht in die Geburtsunterlagen, die Aktenteile zu seiner Person, zu seiner leiblichen Mutter, aber auch gemeinsame Dokumente umfasst.

Unterlagen des Kindes

Soweit es um Unterlagen geht, die ausschließlich das Kind betreffen, ist die Rechtslage eindeutig. Hier besteht nach § 630g BGB, § 10 Abs. 2 MBO-Ä, § 15 DS-GVO ein umfassendes Einsichts- und Auskunftsrecht der betroffenen Person – hier des Patienten selbst.

Unterlagen der Mutter

Deutlich komplexer gestaltet sich die Beantwortung der Frage nach einer rechtskonformen Bearbeitung des Auskunftsbegehrens hinsichtlich der in der Akte befindlichen Unterlagen, die der leiblichen Mutter zuzuordnen sind.

Grundsätzlich steht dem Auskunftsanspruch des Kindes die Schweigepflicht

der behandelnden Ärzte des Krankenhauses zugunsten der Mutter entgegen.

Die Regelungen des § 630g Abs. 3 BGB können zu Lebzeiten der Mutter nicht angewandt werden. Danach haben Erben bzw. die nächsten Angehörigen ein Einsichtsrecht in die Akte des verstorbenen Patienten.

Maßgeblich ist zudem, aus welcher Motivation die Einsicht in die Patientenakte begehrt wird.

Es macht aus rechtlicher Sicht einen Unterschied, ob der Auskunftsanspruch auf Angaben über die eigene Abstammung abzielt (bspw. wer ist die leibliche/genetische Mutter) oder ob dieser seinen Schwerpunkt tatsächlich hinsichtlich der Gesundheitsdaten der Mutter hat.

Wo liegt der Unterschied?

Nach höchstrichterlicher Rechtsprechung hat ein Adoptivkind ein sogenanntes Recht auf Kenntnis der Abstammung. Dieses Recht wird aus der Menschenwürdegarantie und dem allgemeinen Persönlichkeitsrecht abgeleitet und ist im Bürgerlichen Gesetzbuch sowie anderen Normen des Zivilrechts (Personenstandsgesetz, Adoptionsgesetz etc.) verankert. Wenngleich Adressat dieses Rechts in der Regel der Staat (das Standesamt oder die zuständige Abteilung der Gemeinde/Stadt) ist, kann auch ein Krankenhaus oder eine Klinik mit dieser Anfrage konfrontiert werden. Zu beachten ist, dass dieses Recht lediglich die Auskunft über die Identität der genetischen Eltern erfasst. Neben dem Vor- und Nachnamen, sowie dem Geburtsdatum ist hiervon ggfs. noch die Anschrift umfasst. Diese Daten sind abschließend, das bedeutet, dass Informationen über Gesundheitsdaten nicht erteilt werden. Wie bereits oben angemerkt, bedarf es bei Fragen zu Gesundheitsdaten der Mutter deren Entbindung von der ärztlichen Schweigepflicht.

Gemeinsame Unterlagen

Nicht weniger komplex ist die Frage nach dem Umgang mit Unterlagen, auf denen sich Daten beider Personen befinden, beispielsweise bei der Kardiotokographie (Wehentätigkeit der Mutter). Während die den Erfragenden

betreffenden Informationen weitergegeben werden dürfen, müssen die in derselben Akte befindlichen Informationen über die Wehentätigkeit der Mutter unkenntlich gemacht bzw. geschwärzt werden, soweit keine Schweigepflichtentbindung vorliegt.

Wie ist in solchen Fällen zu verfahren?

In der Praxis ist darauf zu achten, dass der Anfragende die Hintergründe seines Begehrens offenlegt. Soweit dies nicht bereits im ersten Schreiben mitgeteilt wurde, sollte dies vor Beginn der Bearbeitung unbedingt angefragt werden.

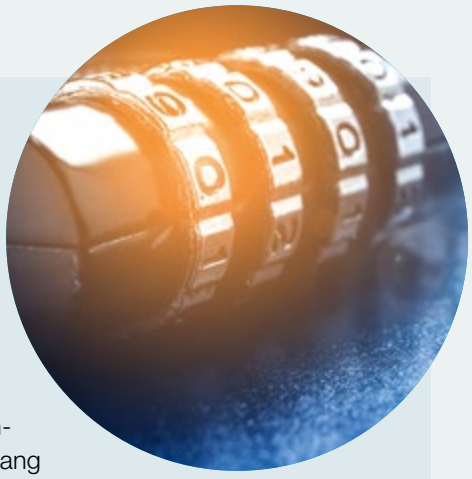
Hieraus lassen sich wichtige Rückschlüsse auf die dann zu ergreifenden Maßnahmen ziehen: Geht es dem Anfragenden lediglich um die Auskunft der Gesundheitsdaten (bspw. um Hinweise auf vererbbare Krankheiten zu erhalten) oder (auch) um die Identität der Mutter?

In jedem Fall ist bereits im frühen Stadium der Bearbeitung ein Identitätsnachweis zu fordern. Liegt, wie im beschriebenen Fall, die Behandlung schon mehrere Jahre oder gar Jahrzehnte zurück, sollten sich die zu ergreifenden Maßnahmen hieran orientieren: Zur Identitätsfeststellung sollte mindestens die Vorlage des Personalausweises, besser noch, die Vorlage einer Geburtsurkunde erfolgen.

Vertiefungshinweis im Buch

Weitere Informationen finden Sie in Kapitel B/ 9.1 des Fachbuchs „Datenschutz im Gesundheitswesen“, AOK-Verlag GmbH, Remagen, ISBN 978-3-553-43110-1.

Kurznotiz:



Passwörter alle 90 Tage wechseln? Eine Empfehlung aus der Vergangenheit!

Die aktuellen Tätigkeitsberichte der Datenschutzbeauftragten der Länder enthalten einige Überraschungen. Eine positive Überraschung findet sich im 34. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2018. Auf Seite 55 findet sich nämlich die Abkehr von einer alten Regelung, die in der Praxis weder Administratoren noch Nutzern Freude bereitet hat. So heißt es im Tätigkeitsbericht:

„Früher wurde empfohlen, Passwörter in regelmäßigen Abständen zu ändern. Diese Empfehlung gilt heutzutage als überholt, da sie nicht zu mehr Sicherheit führt – sondern nur dazu, dass Nutzer sich diese im Klartext notieren, einfache Passwörter wählen, eine Zahl hochzählen oder ähnliches. Daher sollten Administratoren die Nutzer nicht mehr zwingen, Passwörter in regelmäßigen Abständen zu ändern.“

Zusätzlich findet sich ein Hinweis auf “aktualisierte Hinweise zum Umgang mit Passwörtern“. Betrachtet man diese genauer, so wird auch hier die deutliche Aussage getroffen:

„Eine erzwungene regelmäßige Änderung von Passwörtern ist überholt. Administratoren sollten daher ihre Nutzer nicht regelmäßig auffordern oder zwingen, die Passwörter zu ändern. Stattdessen sollten die Nutzer für sichere Passwörter sensibilisiert werden.“

An dieser Stelle hat man also die Möglichkeit, als Datenschutzbeauftragter eine Änderung vorzuschlagen, über die sich vor allem die Nutzer freuen dürften.

© AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215 | Mail fachinfo@aok-verlag.de | Web http://www.aok-verlag.info Herausgeber: AOK-Verlag GmbH, Remagen | Geschäftsführer: Frank Schmidt | Redaktion: Prof. Dr. Benedikt Buchner, Dr. Sebastian Ertel, Sven Venzke-Caprarese | Der Inhalt des vorliegenden Newsletters ist mit größter Sorgfalt zusammengestellt worden. Eine Haftung für die Angaben übernimmt der Verlag jedoch nicht. | Bildnachweise: iStock

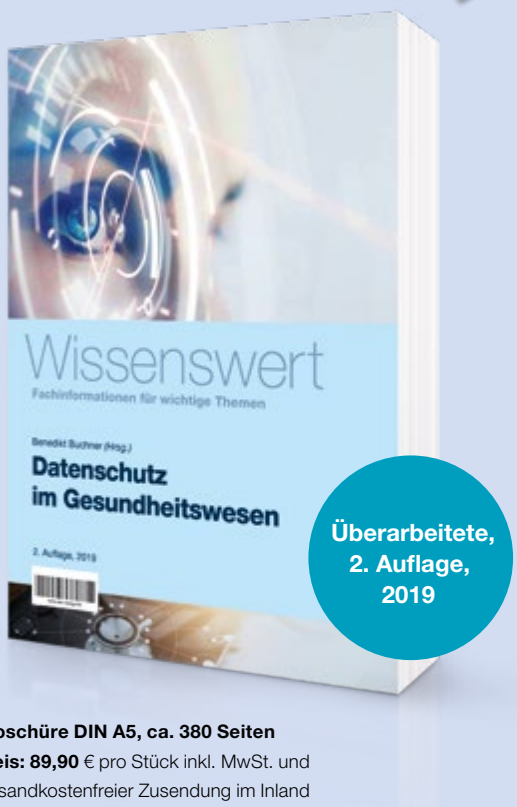
Datenschutz im Gesundheitswesen

Mit Geltung der Europäischen Datenschutz-Grundverordnung und der damit verbundenen umfassenden Anpassung der nationalen Datenschutzvorschriften haben sich die datenschutzrechtlichen Rahmenbedingungen auch für Gesundheitseinrichtungen seit Mai 2018 grundlegend geändert.

Die Broschüre soll Datenschutzverantwortlichen dabei helfen, die Datenverarbeitung in Gesundheitseinrichtungen auch künftig rechtskonform zu gestalten. Das Handbuch vermittelt die neuen gesetzlichen Grundlagen, führt praxisnah in die Datenschutzorganisation ein und erläutert am Beispiel des Krankenhauses die zentralen datenschutzrechtlichen Herausforderungen.

Neben dem Datenschutz wird dabei auch das neue für Gesundheitseinrichtungen zunehmend wichtigere Feld der IT-Sicherheit beleuchtet.

Broschüre HIER bestellen



Broschüre DIN A5, ca. 380 Seiten
Preis: 89,90 € pro Stück inkl. MwSt. und versandkostenfreier Zusendung im Inland
Art. Nr.: 43110 | **ISBN: 978-3-553-43110-1**

Aus dem Inhalt (Auszug):

- **A – Rechtliche Grundlagen**
  DS-GVO, neues BDSG und Auswirkungen für den Gesundheitsdatenschutz
- **B – Datenschutzorganisation**
  Praktische Umsetzung der DS-GVO in Gesundheitseinrichtungen durch den Datenschutzbeauftragten
- **C – Datenschutz im Krankenhaus**
  Patientendatenschutz im Betriebsgeschehen sicherstellen
- **D – Der Internetauftritt**
  Internetauftritt und Social Media-Plattformen rechtssicher ausgestalten
- **E – Datensicherheit**
  Rahmenvorschriften zur IT-Sicherheit und bereichsspezifische Vorgaben für den Gesundheits- und Medizinbereich

AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215 | Mail fachinfo@aok-verlag.de
Jetzt Broschüre bestellen unter: aok-verlag.info/de/der-neue-datenschutz-im-gesundheitswesen