AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Juni 2017 | Seite 1

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

INHALT

Verträge zur Auftragsverarbeitung – was muss im Hinblick auf die DS-GVO beachtet werden?

Bereits im letzten Newsletter hatten wir uns mit der Frage beschäftigt, welche Änderungen die ab dem 25. Mai 2018 geltende DS-GVO in Bezug auf das Verzeichnis der Verarbeitungstätigkeiten mit sich bringt. In diesem Beitrag betrachten wir, welche Änderungen bei bestehenden und künftigen Verträgen zur Auftragsverarbeitung zu beachten sind.

Sven Venzke-Caprarese

Neue Regelung auch für alte Verträge

Ab dem 25. Mai 2018 werden die Inhalte, die ein Vertrag zur Auftragsverarbeitung aufweisen muss, durch Art. 28 DS-GVO vorgegeben. Es ist davon auszugehen, dass diese Vorgaben sowohl für neue als auch für bestehende Auftragsverhältnisse gelten. Gesundheitseinrichtungen sollten daher bereits jetzt überprüfen, ob die bisherigen Inhalte der Verträge zur Auftragsverarbeitung den Regelungen des Art. 28 DS-GVO entsprechen.

Muss ein Vertrag, der § 11 BDSG bzw. den Landesdatenschutzgesetzen entspricht, angepasst werden?

Sofern Gesundheitseinrichtungen derzeit Verträge verwenden, die inhaltlich den Anforderungen des §11 BDSG entsprechen, werden sich zwar keine grundlegenden Änderungen ergeben. Allerdings treffen die Regelungen der DS-GVO in Teilbereichen speziellere Vorgaben als das BDSG. Hieraus

kann sich durchaus ein Regelungsdelta ergeben, was dazu führen kann, dass die bestehenden Verträge angepasst werden müssen.

Insbesondere im Hinblick auf die Landesdatenschutzgesetze wird sich in der Zukunft ein nicht unerheblicher Anpassungsbedarf ergeben. Denn viele Landesdatenschutzgesetze regeln die Anforderungen an die Inhalte eines Vertrags zur Auftragsverarbeitung noch wesentlich undifferenzierter als § 11 BDSG. So haben z. B. viele Landesdatenschutzgesetze im Hinblick auf die Auftragsverarbeitung noch einen Stand, der vor der Novellierung des BDSG aus dem Jahr 2009 liegt. Das Regelungsdelta wird daher bei den Landesdatenschutzgesetzen regelmäßig noch um einiges höher ausfallen.

Normenvergleich zeigt Delta auf

Um bestehende Verträge besser prüfen zu können, bietet sich ein Vergleich der bestehenden Rechtsnormen an. Vergleicht man § 11 BDSG mit Art. 28 DS-GVO, zeigen sich insbesondere folgende Abweichungen, die zu einem Anpassungsbedarf führen können:

1. Einsatz von Subunternehmern

Der Einsatz von Subunternehmern ist in Art. 28 DS-GVO spezieller geregelt als in § 11 BDSG.

Gem. Art. 28 Abs. 2, Abs. 3 lit. d DS-GVO muss vertraglich festgelegt werden, dass der Auftragsverarbeiter einen weiteren Auftragsverarbeiter nicht ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nehmen darf. Im Fall einer allgemeinen schriftlichen Genehmigung hat der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter zu informieren, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Bestehende Verträge nach § 11 BDSG enthalten zwar oftmals eine Klausel, nach welcher die Einschaltung von Subunternehmern der vorherigen Genehmigung durch den Auftraggeber bedarf. Gelegentlich finden sich aber auch Verträge, welche die Einschaltung von Subunternehmern erlauben, wenn der Auftraggeber über deren Einschaltung informiert wird und ansonsten die Vorgaben des Vertrags auch auf den Subunternehmer erstreckt werden. Eine ausdrückliche Regelung eines Einspruchsrechts fehlt an dieser Stelle dann aber häufig.

2. Verschwiegenheitsverpflichtung

Nach Art. 28 Abs. 3 lit. b DS-GVO ist zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Ein solch ausdrücklicher Regelungsbedarf bestand in der Vergangenheit nicht. Zwar verweist § 11 Abs. 2 S. 2 Nr. 5 BDSG darauf, dass auch Auftragsverarbeiter ihre Mitarbeiter nach § 5 BDSG auf das Datengeheimnis verpflichten müssen, wenn für sie das BDSG gilt. Viele Verträge zur Auftragsdatenverarbeitung regeln eine entsprechende Verpflichtung allerdings nicht ausdrücklich, da § 11 Abs. 2 S. 2 Nr. 5 BDSG insofern nur eine ohnehin

bestehende gesetzliche Pflicht des Auftragsverarbeiters wiedergibt.

Da die DS-GVO keine ausdrückliche Verpflichtung auf das Datengeheimnis mehr kennt, muss sich die Verpflichtung des Auftragsverarbeiters zur Vertraulichkeitsverpflichtung seiner Mitarbeiter jetzt direkt aus dem Vertrag ergeben.

3. Weisungsdokumentation

Art. 28 Abs. 3 lit. a DS-GVO legt fest, dass die Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen hin erfolgen darf. Eine solche ausdrückliche Pflicht zur Dokumentation kennt das BDSG nicht. Auch an dieser Stelle kann sich daher ein Anpassungsbedarf bestehender Verträge ergeben.

An dieser Stelle ist zudem eine Besonderheit zu beachten. Selbst wenn bisherige Verträge regeln, dass Weisungen nur schriftlich erteilt werden dürfen, reicht dies nicht unbedingt aus. Denn Regelungsziel von Art. 28 Abs. 3 lit. a DS-GVO ist die Dokumentation der Weisungen.

4. Technische und organisatorische Maßnahmen

Art. 28 Abs. 3 lit. c DS-GVO regelt, dass der Auftragsverarbeiter verpflichtet werden muss, alle gemäß Art. 32 erforderlichen Maßnahmen zu ergreifen.

Zwar waren Auftragsverarbeiter auch nach dem BDSG dazu zu verpflichten, die angemessenen technischen und organisatorischen Maßnahmen nach § 9 BDSG nebst Anlage zu treffen. Zudem wird sich argumentieren lassen, dass die Maßnahmen nach BDSG und die Maßnahmen nach DS-GVO an sich grundsätzlich deckungsgleich sind. Allerdings fordert Art. 32 Abs. 1 lit. d DS-GVO ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Ein solches Verfahren ist nach dem BDSG bislang nicht ausdrücklich vorgeschrieben. Auch dies kann zu einem Anpassungsbedarf der Verträge führen, etwa indem Dienstleister verpflichtet werden, regelmäßige Penetrationstests oder die Ergebnisse von internen Audits vorzulegen.

5. Unterstützung

Ein Auftragsverarbeiter nach DS-GVO muss den Verantwortlichen zudem stärker als bisher in verschiedenen Belangen unterstützen. Dies gilt z. B. für

- die Unterstützung im Rahmen der Meldung von Datenpannen, der Benachrichtigung der Betroffenen, der Datenschutzfolgeabschätzung und der vorherigen Konsultation (Art. 28 Abs. 3 lit. f DS-GVO).
- die Unterstützung durch geeignete technische und organisatorische Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte – inkl. dem Recht auf Datenübertragbarkeit (Art. 28 Abs. 3 lit. e DS-GVO).
- die Zurverfügungstellung der Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten (Art. 28 Abs. 3 lit. h DS-GVO).

Fazit

Auch wenn sich die Regelungen der DS-GVO zu den Inhalten der Verträge zur Auftragsverarbeitung auf den ersten Blick nur marginal von den Regelungen des BDSG unterscheiden, wird doch in vielen Fällen eine Anpassung der Verträge erforderlich sein.

Da auch bestehende Verträge betroffen sind und Vertragsanpassungen in der Praxis regelmäßig viel Aufwand und Zeit kosten, sollten Gesundheitseinrichtungen diese Aufgabe bereits jetzt angehen.

Die folgende Gegenüberstellung soll die dabei zu beachtenden Punkte noch einmal verdeutlichen, wobei die Punkte, die Anpassungsbedarf auslösen können, orange hinterlegt sind.

§ 11 Abs. 2 S. 2 BDSG		Art. 28 DS-GVO	
	Schriftlicher Auftrag	**Abs. 3, Abs. 9**	Vertrag oder anderes Rechtsinstrument, schriftlich abzufassen, was auch in einem **elektronischen** Format erfolgen kann
		Abs. 3	Pflichten und Rechte des Verantwortlichen sind festzulegen.
Nr. 1	Gegenstand des Auftrags	**Abs. 3**	Gegenstand der Verarbeitung
Nr. 1	Dauer des Auftrags	**Abs. 3**	Dauer der Verarbeitung
Nr. 2	Umfang, Art und Zweck der Verarbeitung	**Abs. 3**	Art und Zweck der Verarbeitung
Nr. 2	Art der Daten	**Abs. 3**	Art der personenbezogenen Daten
Nr. 2	Kreis der Betroffenen	**Abs. 3**	Kategorien betroffener Personen
Nr. 3	Technische und organisatorische Maßnahmen	**Abs. 3 lit. c**	Alle gemäß **Artikel 32** erforderlichen Maßnahmen
Nr. 4	Berichtigung, Löschung, Sperrung		
Nr. 5	Die nach Abs. 4 bestehenden Pflichten des Auftragnehmers [hierzu gehört auch die Verpflichtung auf das Datengeheimnis nach § 5 BDSG]	**Abs. 3 lit. b**	gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen
Nr. 6	Etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen	**Abs. 2, Abs. 3 lit. d**	Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
Nr. 7	Kontrollrechte des Auftraggebers sowie Duldungs- und Mitwirkungspflichten des Auftragnehmers	**Abs. 3 lit. h**	Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

§ 11 Abs. 2 S. 2 BDSG		Art. 28 DS-GVO	
Nr. 8	mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen	**Abs. 3 lit. f**	unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
Nr. 9	Umfang der Weisungsbefugnisse des Auftraggebers	**Abs. 3 lit. a**	Verarbeitung nur auf **dokumentierte** Weisung des Verantwortlichen
Nr. 10	Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags	**Abs. 3 lit. g**	nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht
		Abs. 3 lit. f	Unterstützung bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten
		Abs. 3 lit. e	angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen
		Abs. 3 lit. h	dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt

Ersetzendes Scannen

Zunehmender Dokumentationsbedarf und lange Aufbewahrungsfristen und -pflichten stellen zunehmend ein Problem für Gesundheitseinrichtungen dar. Steigender Platzbedarf und Verwaltungsaufwand führen zu einem Umdenken und zur Suche nach ressourcensparenden Alternativen. Eine solche ist die Digitalisierung der Unterlagen durch Einscannen.

Dr. Sebastian Ertel

Aufbewahrungsfristen

Nach § 10 MBO-Ärzte bzw. 630f BGB sind Patientenakten für mindestens 10 Jahre aufzubewahren. Da zivilrechtliche Haftungsansprüche eines Patienten gemäß § 199 Abs. 2 BGB letztlich erst nach 30 Jahren verjähren, wird häufig eine entsprechend lange Aufbewahrung der Patientenunterlagen empfohlen. Auch aus anderen spezialgesetzlichen Regelungen, beispielsweise dem Transfusionsgesetz, ergeben sich Aufbewahrungsfristen von bis zu 30 Jahren.

Einfach scannen und gut?

Es ist indes nicht ausreichend, wenn ein Mitarbeiter der Einrichtung abgestellt wird, Patientenunterlagen einzuscannen und so eine digitale Patientenakte zu erstellen.

In diesem Zusammenhang muss sich vor Augen gehalten werden, dass ein eingescanntes Dokument lediglich eine Kopie des Originals darstellt. Es entfällt die Garantie, die dem Original anhaftet, dass die Kopie denselben Inhalt hat. Denn beim Scannen kann vieles schiefgehen. Durch Knicke oder Falze können Dokumenteninhalte auf der eingescannten Version fehlen. Denkbar ist auch, dass Buchstaben oder Zeichen nicht richtig reproduziert werden. Dies könnte insbesondere bei Untersuchungswerten gravierende Folgen haben. Ein weiterer Aspekt ist die bewusste Manipulation der Dokumente.

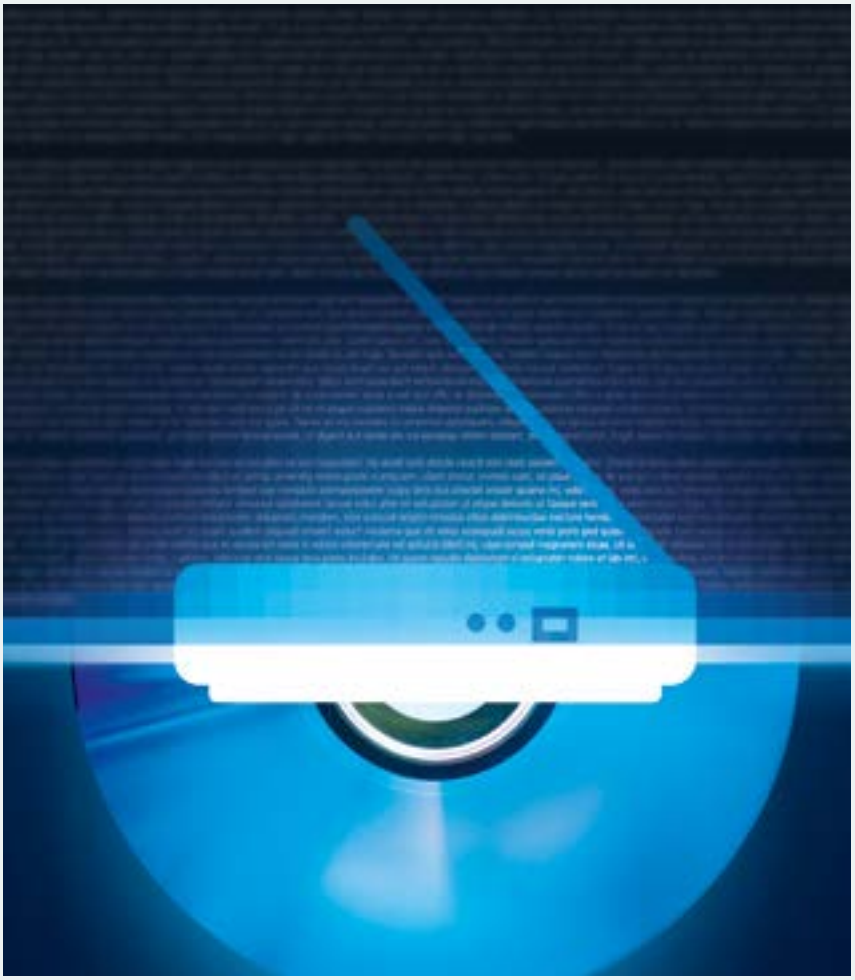
Aus diesem Grund verringert sich automatisch der Beweiswert einer (digitalen) Kopie, insbesondere dann, wenn das Original nicht mehr verfügbar ist, weil es unmittelbar nach dem Scanvorgang vernichtet wurde.

Ist ein elektronisches Dokument Gegenstand eines gerichtlichen Verfahrens, erfolgt die Beweisaufnahme durch die Inaugenscheinnahme und unterliegt der freien richterlichen Beweiswürdigung, gegebenenfalls unter Hinzuziehung eines Sachverständigen als gerichtlichen Gehilfen.

Spezifische Beweisregelungen kommen demgegenüber regelmäßig nicht zur Anwendung: Da eingescannte Dokumente keine Urkunden sind, ist eine Anwendung der Regelungen zum Urkundenbeweis nicht möglich.

Technische Richtlinie „Ersetzendes Scannen“ des BSI

Mit der Technischen Richtlinie „Ersetzendes Scannen“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurden Leitlinien geschaffen, die eine Digitalisierung von Papier-



dokumenten bei unmittelbarer Vernichtung der Originale ermöglichen und die Aspekte der Informations- und Rechtssicherheit gleichermaßen berücksichtigen. Besonderes Augenmerk liegt in diesem Zusammenhang auf der Simulationsstudie „Ersetzendes Scannen“, die 2013/14 durch das Forschungszentrum für Informationstechnik-Gestaltung der Universität Kassel durchgeführt wurde. In dieser wurde in je sieben simulierten Zivil- und Finanzgerichtsverfahren der Beweiswert von eingescannten Dokumenten erforscht. Zudem standen die Empfehlungen der TR RESISCAN auf dem Prüfstand.

Im Ergebnis kann durch verschiedene Maßnahmen der Beweiswert eines eingescannten Dokumentes signifikant gesteigert werden. Drei Aspekte sind hierbei hervorzuheben.

Zeitpunkt des Scannens:

Bestehen Zweifel an der Echtheit des (nicht mehr vorhandenen) Originals, ist die Frage zu klären, ob im Zeitpunkt des Scannens ein Manipulationsinteresse bezüglich des Dokuments bestand. Je früher der Scanprozess erfolgte, umso weniger ist ein Manipulationsinteresse anzunehmen. Von großer Bedeutung ist insoweit die Dokumentation des Zeitpunkts des Scannens. Dieser kann einerseits mittels qualifizierten Zeitstempels gemäß § 2 Nr. 14 SigG erfolgen. Alternativ kann ein Dokumentenmanagementsystem (DMS) genutzt werden, wenn

- die Systemzeit grundsätzlich unveränderbar ist;
- das DMS von einem Externen, der keine Manipulationsinteressen hat, betrieben wird;
- der Scan unmittelbar im DMS gespeichert wird, so dass zu keinem Zeitpunkt ein ungeschützter Zugriff besteht, und
- der Scan nicht ohne entsprechende Protokollierung aus dem DMS entfernt wird.

Der Scanprozess:

Zweifel am ordnungsgemäßen Scanprozess können durch standardisierte Prozesse der Verfahrensdokumentation im Sinne der TR RESISCAN ausgeräumt werden. Flankiert wird dieses durch eine differenzierte Qualitätskontrolle. Eine weitere Maßnahme, Zweifel am ordnungsgemäßen Scanprozess auszuräumen, besteht darin, diesen durch einen externen Dritten vornehmen zu lassen. Dieser hat vom Grundsatz her kein Manipulationsinteresse, so dass durch diesen vorgenommene Scans als beweiskräftiger angesehen werden. Auf die in diesem Zusammenhang bestehenden Probleme hinsichtlich der ärztlichen Schweigepflicht wird im Weiteren eingegangen.

Beweiswert des Scanproduktes:

Letztlich muss die Echtheit des erstellten Scans gewährleistet werden. Dies betrifft den Nachweis, dass der Scan von der im System bezeichneten Person stammt und keine nachträgliche Änderung erfuhr. Insofern müssen technische Mittel installiert werden, die Veränderungen am eingescannten Dokument erfassen und revisionssicher protokollieren bzw. eine Veränderung konsequent verhindern. Dieser Nachweis kann unmittelbar über ein DMS gewährleistet werden, wenn

- der Scan ohne Zwischenschritt unmittelbar in das DMS überführt wird,
- der Scan lediglich gelesen, nicht aber bearbeitet werden kann und

- jeder Umgang mit dem Scan protokolliert wird.

Alternativ kann auch hier wieder mit einer elektronischen Signatur, konkret einer qualifizierten elektronischen Signatur (§ 2 Nr. 3 SigG) gearbeitet werden. Diese stellt die Identität des Signierenden fest sowie die Integrität des Scanprodukts zum Zeitpunkt des Scannens sicher.

Einbindung externer Dienstleister

Wie gesehen, können externe Dienstleister auf verschiedene Weise in den Prozess des ersetzenden Scannens eingebunden werden: als Betreiber eines entsprechenden DMS oder als Durchführende des Scanverfahrens. Erfolgt der Scanprozess zur Digitalisierung von Patientenakten, muss in diesem Zusammenhang zwingend die ärztliche Schweigepflicht berücksichtigt werden. Zumindest bei der Verwendung eines DMS kann dieses Problem dahingehend gelöst werden, dass dem Anbieter des Systems keine Zugriffsrechte auf die Daten eingeräumt werden und die Konfiguration ausschließlich im Beisein der unternehmensinternen IT erfolgt.

Problematischer ist demgegenüber die Durchführung des Scannens durch ein externes Unternehmen. Dessen Beschäftigte nehmen zwangsläufig Kenntnis von den Inhalten der Unterlagen – entweder bei der Vorbereitung des Scans, beispielsweise durch die Entfernung von Büroklammern oder Klarsichthüllen, oder auch nach dem erfolgten Scan im Rahmen der Qualitätskontrolle.

Ergibt sich aus dem für die Einrichtung einschlägigen Krankenhaus- oder Gesundheitsdatenschutzgesetz keine gesetzliche Offenbarungsbefugnis, kann einem strafbewehrten Verstoß gegen die ärztliche Schweigepflicht nur bei einer entsprechenden Entbindung durch den Patienten entgegengewirkt werden. Diese hilft aber auch nur in den Fällen, in denen der Patient noch erreichbar ist, etwa weil die Entbindungserklärung im Rahmen der Patientenaufnahme eingeholt wird. Keine Lösung bietet die Einwilligungserklärung in den Fällen, in denen bereits archivierte Patientenakten digitalisiert werden sollen. Der Patient ist nicht mehr vor Ort und müsste privat angeschrieben und um Abgabe der Erklärung gebeten werden. Wohnt der Patient nicht mehr unter der bekannten Adresse, ist vielleicht verstorben oder verweigert die Erklärung, bedeutet das neben dem erheblichen administrativen Aufwand auch die Schaffung von uneinheitlichen Zuständen (Papier- und Digitalakten).

Im Interesse einer Vereinheitlichung und Vereinfachung der Digitalisierung erfolgt häufig eine Abstellung eines Mitarbeiters der Gesundheitseinrichtung beim Dienstleister, der als Erfüllungsgehilfe des Berufsgeheimnisträgers die Digitalisierung der Patientenakten und die gegebenenfalls sich anschließende Vernichtung überwacht und einer gezielten Kenntnisnahme von den Inhalten der Unterlagen durch die Beschäftigten des externen Dienstleisters entgegenwirkt.

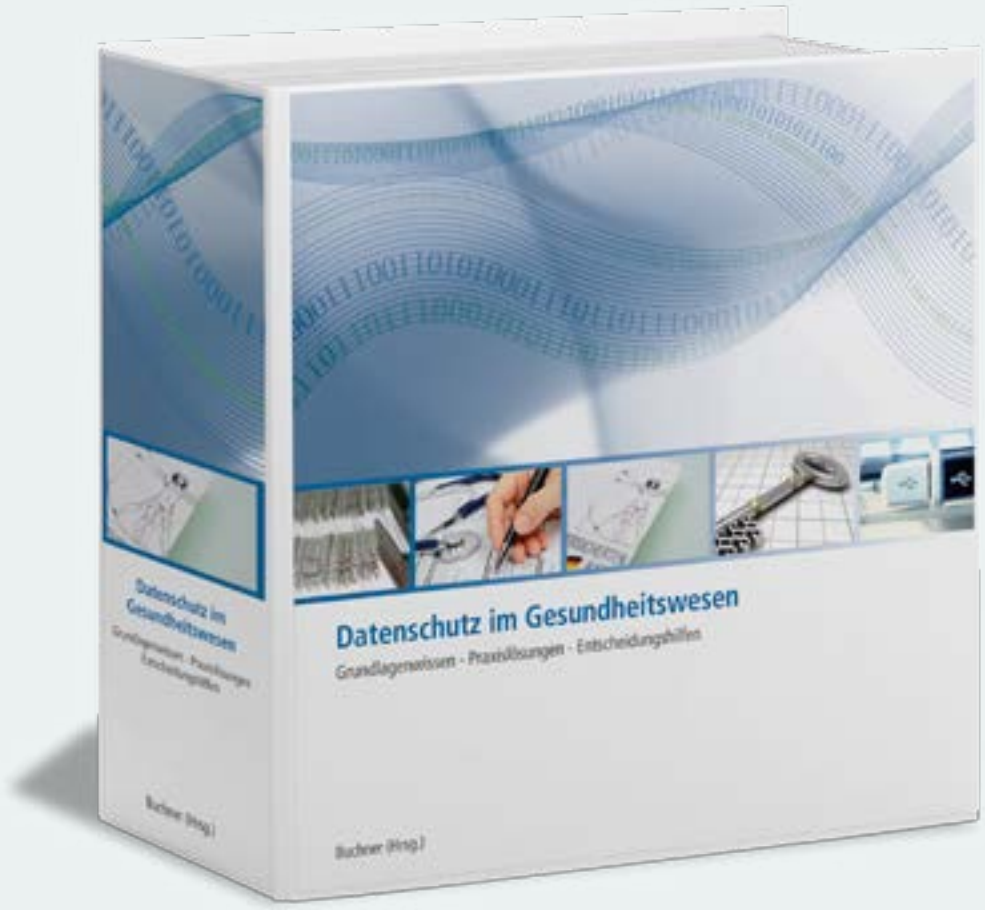
Kurznotiz:

Ransomware – erneute Angriffswellen (WannaCry)

Bereits vor gut einem Jahr hatten wir in unserem März-Newsletter über Bedrohungen durch Ransomware und Schutzmaßnahmen berichtet. War das Thema damals insbesondere durch die Ausbreitung der Ransomware „Locky“ aktuell, wütet derzeit die Ransomware „WannaCry“. Auch in diesem Jahr sind dabei Einrichtungen des Gesundheitswesens nicht verschont geblieben. Unsere Empfehlungen aus dem letzten Jahr gelten jedoch grundsätzlich fort. Zum Schutz vor Ransomware kommt es, wie im Newsletter aus März 2016 im Detail dargestellt, insbesondere auf folgende Punkte an:

- Patch- und Updatemanagement
- Virenscanner, Firewall, SMTP-Gateway
- Netzsegmentierung
- Einschränkung der Nutzerrechte
- Mitarbeitersensibilisierung
- Angemessenes Backup-Konzept
- Notfall- und Recovery-Management

Nicht mehr aktuelle Betriebssysteme, wie Windows XP, sollten nicht mehr verwendet werden. Sofern sich im Einzelfall ein Einsatz von unsicheren Betriebssystemen nicht vermeiden lässt (etwa weil das alte MRT-Gerät auch im Jahr 2017 noch zwingend mit dem Betriebssystem „Windows 95“ betrieben werden muss), sind besondere Schutzmaßnahmen gegen die damit einhergehenden Risiken erforderlich. Nähere Details haben wir in unserem Newsletter aus Juni 2016 im Kurzbeitrag „Sicherheit von Krankenhausnetzen und Medizingeräten in der Kritik“ dargestellt.



Datenschutz im Gesundheitswesen

Grundlagenwissen – Praxislösungen – Entscheidungshilfen

2 Ordner mit Register im Format DIN A5,
ca. 1.500 Seiten Inhalt
ISBN: 978-3-553-43000-5
Preis 179.- inkl. MwSt.

Uneingeschränkter Online-Zugriff auf alle Arbeitshilfen inkl. 3-4 kostenpflichtige Nachtragslieferungen pro Jahr zum Preis von jeweils 79,90 Euro inkl. MwSt. und versandkostenfreier Zusendung im Inland.

© 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 | Geschäftsführung: Otto Gmeiner | 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: www.istock.com