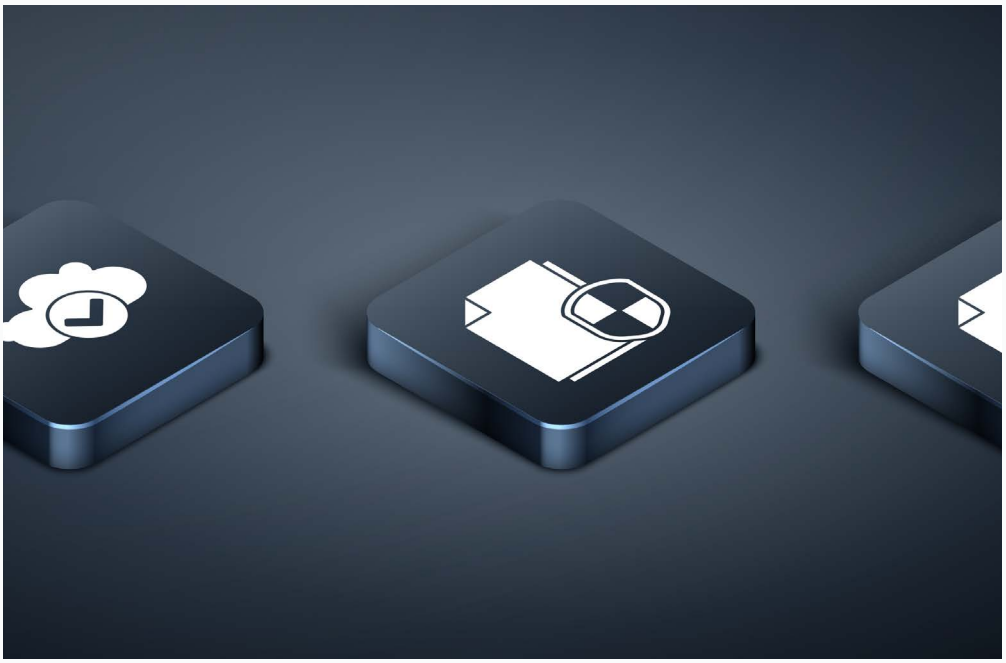
AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe März/April 2021 | Seite 1

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



INHALT

Datenschutzgerechte Personalaktenführung

Gesundheitseinrichtungen verarbeiten eine Vielzahl an sensiblen Patientendaten und unterliegen an dieser Stelle strengen Regeln. Darüber hinaus müssen sich Gesundheitseinrichtungen aber auch Gedanken machen, wenn es um die Frage geht, welche Personaldaten wie verarbeitet werden dürfen. Eine zentrale Rolle spielt dabei die Personalakte.

Sven Venzke-Caprarese

Allgemeine Regeln

Jede Gesundheitseinrichtung muss die Beschäftigten bei der erstmaligen Erhebung personenbezogener Daten nach Art. 13 DS-GVO darüber informieren, welche Daten zu welchen Zwecken wie lange verarbeitet werden. Spätestens im Rahmen der Einstellung sollten Beschäftigte daher darüber aufgeklärt werden, dass ihre Daten u.a. in einer Personalakte und in verschiedenen Fachverfahren gespeichert werden. An dieser Stelle ist es jedoch wenig sinnvoll, bereits im Rahmen der Einstellung eine Information zu erstellen, die alle künftige Eventualitäten umfasst. Sofern es z.B. möglich ist, dass Beschäftigte künftig einen Dienstwagen oder ein Poolfahrzeug nutzen und hierfür der Führerschein der Beschäftigten kontrolliert werden muss, ist es häufig sinnvoll, die entsprechende Art. 13-Information erst im Rahmen Fahrzeugüberlassung auszuhändigen. Es ist also in der Regel nicht mit der erstmaligen Information getan.

Personalakte

Ein zentraler Bestandteil der Personaldatenverarbeitung ist das Führen einer Personalakte. Was in eine Personalakte aufgenommen werden muss oder darf, ist gesetzlich nicht eindeutig geregelt. Sofern nicht spezielle Verordnungen oder Vorschriften erlassen wurden, besteht für die Gesundheitseinrichtung ein Gestaltungsspielraum. Die Grenzen setzt dabei § 26 BDSG. Demnach dürfen grundsätzlich nur die Personaldaten verarbeitet werden, die für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sind.

Häufige Inhalte

Bestandteil der Personalakte sind häufig:

- ein Personalbogen mit Stammdaten sowie Informationen zu etwaigen Änderungen (z.B. Umzüge, Namensänderungen),
- Bewerbung und Lebenslauf,
- Arbeitsverträge und Änderungen inkl. Gehaltsentwicklung,
- Korrespondenz mit Bezug zum Beschäftigungsverhältnis,
- Unterlagen zu Lohnsteuer und Sozialversicherung,
- Nachweise über Vor- und Ausbildung, Prüfungszeugnisse und andere Befähigungsnachweise,
- Fort- und Weiterbildungsmaßnahmen,
- Nachweis der Schwerbehinderteneigenschaft oder der Gleichstellung,
- Beurteilungen,
- Abmahnungen, Kündigungen, Unterlagen zu Rechtsstreitigkeiten, Informationen über Pfändungen (sofern der Arbeitgeber Drittschuldner ist),
- versicherungsrelevante Informationen, etwa über Zusatzversorgungen.

Keine doppelte Personalaktenführung – aber ggf. Nebenakten

Im Grundsatz gilt, dass eine doppelte Personalaktenführung unzulässig ist.

Gleichwohl ist es möglich, auch Nebenakten zu führen. In diesem Fall muss die Personalakte ein vollständiges Verzeichnis aller Nebenakten enthalten, z.B. damit Beschäftigte bei einer etwaigen Einsichtnahme in ihre Personalakte wissen, dass noch weitere Daten an anderer Stelle verarbeitet werden.

Ein gutes Beispiel für eine zulässige und oftmals sogar gebotene Nebenaktenführung ist die Dokumentation eines durchgeführten Betrieblichen Eingliederungsmanagements (BEM). Ein solches ist nach § 167 Abs. 2 SGB IX anzubieten, sofern Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig waren. Die Teilnahme am BEM-Verfahren ist für die Beschäftigten freiwillig. In der Personalakte selbst dürfen im Umfeld des BEM-Verfahrens zwar einige Daten gespeichert werden, etwa die Einladung zum BEM-Gespräch, die Annahme oder Ablehnung des Gesprächs und nach Durchführung des BEM-Verfahrens die Maßnahmen, die der Arbeitgeber erfüllen muss (z.B. die Beschaffung eines höhenverstellbaren Tisches oder eines anderen Bildschirms). Auf keinen Fall dürfen in der Personalakte aber ohne Weiteres die gesundheitsbezogenen Inhalte von Gesprächen gespeichert werden, die im Rahmen des BEM-Verfahrens geführt wurden. So hat etwa das Bundesarbeitsgericht mit Urteil vom 12.09.2006 (Az. 9 AZR 271/06) entschieden, dass sensible Gesundheitsdaten in besonderer Weise aufzubewahren sind. Sofern sensible Gesundheitsdaten zur Personalakte genommenen werden, sind diese vor unbefugter Kenntnisnahme durch Einschränkung des Kreises der Informationsberechtigten zu schützen. Im Ergebnis werden Unterlagen zu BEM-Gesprächen daher in der Praxis oftmals nur in verschlossenen Umschlägen zur Akte genommen. Häufig werden in Bezug auf die BEM-Unterlagen aber auch eigene und besonders geschützte Nebenakten angelegt, was als durchaus sinnvoll ist. In diesem Fall muss die Hauptakte einen Hinweis darauf enthalten, dass eine solche Nebenakte existiert.

Auch im Hinblick auf Arbeitsunfälle kann es sinnvoll sein, eine eigene Nebenakte anzulegen. So sind bei Arbeitsunfällen eine Dokumentation und Meldung vorgeschrieben. Häufig enthalten die Unfallmeldungen selbst sensible Gesundheitsdaten. Zudem kann es im Rahmen des Unfalls zu weiterer Korrespondenz kommen, die sensible Inhalte enthält. Die (Haupt)Personalakte ist hierfür also nicht immer der geeignetste Ort. Hier besteht aber eine gewisse Gestaltungsfreiheit.

Auch der Umgang mit Nachweisen zu Krankmeldungen sollte geregelt sein. Krankmeldungen können zwar auch in der regulären Personalakte gespeichert werden. Allerdings macht die Auslagerung in eine Nebenakte Sinn – u.a. weil hier individuelle Löschfristen gelten. In jedem Fall muss darauf geachtet werden, dass Krankmeldungen nur als „Bescheinigung für den Arbeitgeber“ vorliegen. Reichen Mitarbeiter versehentlich die „Bescheinigung für den Arbeitnehmer“ ein, ist diese zurückzugeben und die Bescheinigung für den Arbeitgeber anzufordern.

Geregelt werden muss auch der Umgang mit Protokollen zu Mitarbeitergesprächen. Solche Protokolle – etwa Zielvereinbarungen – sollten niemals heimlich erstellt, sondern immer den Beschäftigten gegenüber transparent gemacht werden. Empfehlenswert ist die Unterschrift aller Gesprächsteilnehmer, dass die Inhalte des Protokolls zur Kenntnis genommen wurden. Im Falle der Verweigerung der Unterschrift sollte ein entsprechender Vermerk vorgenommen und dem Beschäftigten Gelegenheit zur Gegenstellungnahme gegeben werden. Geregelt werden sollten bei Protokollen zu Mitarbeitergesprächen auch die Aufbewahrungsdauer und der Aufbewahrungsort (z.B. in der Personalakte oder alternativ die Aufbewahrung durch den Vorgesetzten ohne weiteren Einblick für Dritte).

Sofern im Arbeitsverhältnis Besonderheiten auftreten, etwa weil ein Mitarbeiter sich dem Arbeitgeber anvertraut und persönliche, familiäre oder gesundheitliche Probleme von sich aus offenbart, dürfen diese nicht einfach aufgeschrieben werden. Solche Dinge gehören grundsätzlich nicht in eine Personalakte. Vertraut sich ein Beschäftigter seinen Vorgesetzten an, und offenbart z.B. eigene Diagnosen, das Gesundheitsleiden des Ehepartners oder eine Krise im familiären Umfeld, so darf dies zwar im Rahmen eines Fürsorgegesprächs thematisiert, aber grundsätzlich nicht dokumentiert werden.

Sofern im Einzelfall aufgrund von am Arbeitsplatz erlangten Informationen allerdings weitere Maßnahmen erforderlich sind (etwa im Falle von offensichtlichen Suchterkrankungen, die zu einer Beeinträchtigung der arbeitsvertraglichen Pflichten führen) ist Vorsicht geboten. Hier sollte ein fester Prozess existieren, welche Informationen wann, wo und wie lange dokumentiert werden dürfen. Am wichtigsten ist an dieser Stelle Transparenz und die Befolgung des Erforderlichkeitsprinzips sowie der Datenminimierung. Im Rahmen des hier genannten Beispiels (Suchterkrankung) bietet die Deutsche Hauptstelle für Suchtfragen e.V. eine gute Praxishilfe.

Eine weitere Besonderheit stellen in der Praxis gelegentlich verteilte Standorte dar, die lokal relativ autonom arbeiten, jedoch durch eine zentrale Personalabteilung betreut werden. Hier kann es erforderlich sein, dass Vorgesetzte einen Teil der Personaldaten auch am Standort vorhalten müssen, etwa Informationen zum Arbeitszeitmodell, bestehende Qualifikationen und Nachweise etc. Eine doppelte Aktenführung muss an dieser Stelle vermieden werden. Lässt sich eine lokale Datenverarbeitung nicht verhindern, sollte von der Gesundheitseinrichtung im Detail vorgegeben werden, was zu welchem Zweck wie lange lokal verarbeitet werden darf. Die Personalakte sollte auch hierzu einen Verweis enthalten.

Sicherheit der Personalakte

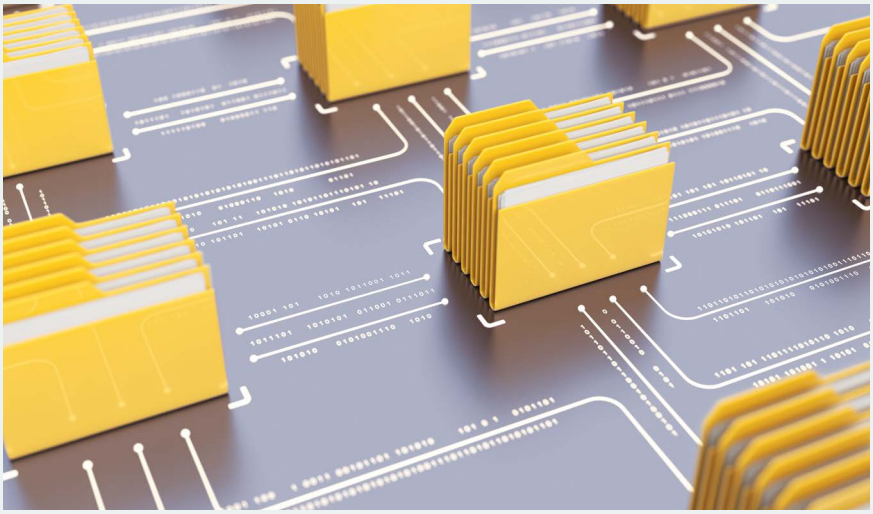
Die Sicherheit der Personalakte ist ein weiteres Thema, das berücksichtigt werden muss. Zum einen muss gewährleistet werden, dass keine Unbefugten auf die Personalakten zugreifen können. Sofern die Personalakten noch in Papierform geführt werden, muss sich die Gesundheitseinrichtung auch Gedanken um die Verfügbarkeit der Personalakten machen, insbesondere im Hinblick auf den Schutz vor Wasser und Feuer.

Löschung von Daten

Ein überaus komplexes Thema ist die Frage, wann welche Daten aus der Personalakte gelöscht werden müssen. An dieser Stelle findet man in der Praxis häufig den allgemeinen Ansatz, die Personalakte 10 Jahre nach Beendigung der Beschäftigung zu vernichten. Ins Feld geführt werden hier oftmals pauschale Verweise auf §§ 257 HGB, 147 AO, 28f SGB IV und 39b EstG.

Tatsächlich greift dieser Ansatz zu kurz. Denn manche Daten müssen bereits im Beschäftigungsverhältnis gelöscht werden, andere zum Zeitpunkt der Beendigung und wiederum andere nach Beendigung des Beschäftigungsverhältnisses. Um nur einige Beispiele zu nennen:

- Abmahnungen leichterer Art, die wegen eines einmaligen Fehlverhaltens ausgesprochen werden, können bereits nach drei Jahren gelöscht werden. Schwerere oder regelmäßige Verfehlungen dürfen hingegen bis zur Beendigung des Beschäftigungsverhältnisses gespeichert werden, jedoch nicht darüber hinaus. Sofern klar ist, dass das Beschäftigungsverhältnis beendet wurde und auch kein Prozess vor dem Arbeitsgericht mehr droht, müssen Abmahnungen daher gelöscht werden.



- In Bezug auf Unfallmeldungen gelten besondere gesetzliche Vorschriften sowie Vorgaben der Berufsgenossenschaften. Eine Aufbewahrung ist hiernach für die Dauer von fünf Jahren vorgeschrieben. Sofern keine Besonderheiten vorliegen, können die Unfallmeldungen danach vernichtet werden.
- Krankmeldungen können vier Jahre ab Kalenderjahrende der Entstehung eines Entgeltanspruchs gelöscht werden; § 6 Abs. 1 AAG.
- Lohnkonten können für sechs Jahre aufbewahrt werden.
- DEÜV-Bescheinigungen über Datenübermittlungen können nach § 25 Abs. 2 Datenerfassungs- und Übermittlungsverordnung bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres aufbewahrt werden.
- Die Aufbewahrung von BEM-Unterlagen sollte mit den betroffenen Beschäftigten abgestimmt und im Rahmen der Einwilligung zur Teilnahme thematisiert werden. In der Regel wird von einer Aufbewahrungsdauer von drei bis fünf Jahren ausgegangen.
- Mitarbeitergesprächsprotokolle sollten, sofern es sich um regelmäßige Jahresgespräche handelt, nicht länger als zwei bis drei Jahre gespeichert werden. Sofern bei aktuellen Gesprächen noch Inhalte aus alten Protokollen relevant sind, sollten diese in das aktuelle Protokoll aufgenommen und erneut thematisiert werden.

Längstens sechs Jahre nach Beendigung des Beschäftigungsverhältnisses sollte der Großteil der Daten dann gelöscht werden. Eine Ausnahme können noch Unterlagen darstellen, die im Rahmen der Rentenversicherung oder der Zusatzversorgung relevant sind.

Elektronische Personalakte

Aufgrund der Vielzahl an Anforderungen kann es durchaus erforderlich sein, die Personalakten elektronisch zu führen. Denn bei Einhaltung der erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen können die Personalakten wirksam vor Wasser und Feuer geschützt werden – zwei Gefahren, vor denen man Papierpersonalakten nur bedingt schützen kann.

Auch im Hinblick auf die unterschiedlichen Löschfristen kann das Führen einer elektronischen Personalakte große Vorteile bieten. Sofern die eingesetzte Software unterschiedliche Inhalte erkennt und unterschiedliche Aufbewahrungs- und Löschfristen definiert werden können, kann gewährleistet werden, dass Personaldaten tatsächlich angemessen gelöscht werden.

Ein weiterer Vorteil von elektronischen Personalakten ist die bessere Handhabbarkeit von Betroffenenanfragen nach Art. 15 DS-GVO (Recht auf Auskunft und kostenlose Kopie in elektronsicher Form).

Verbotene bzw. kritische Inhalte

Sofern Personalakten Führungszeugnisse enthalten, sollte die Zulässigkeit der Erhebung und Speicherung vom Datenschutzbeauftragten der Gesundheitseinichtung überprüft werden. Denn das Einholen von Führungszeugnissen ist bei privatwirtschaftlich oder kirchlich betriebenen Gesundheitseinrichtungen grundsätzlich nur in fest umrissenem Rahmen möglich bzw. vorgeschrieben – etwa nach § 75 Abs. 2 S. 4 SGB XII und § 124 Abs. 2 S. 4 SGB IX in Bezug auf Fach- und anderes Betreuungspersonal, das in der Wahrnehmung der Aufgaben Kontakt mit Menschen mit Behinderung hat.

Bonitätsauskünfte in Bezug auf Beschäftigte sind grundsätzlich unzulässig.

Personalausweiskopien, Führerschein kopien oder Mutterpasskopien dürfen nicht in der Personalakte enthalten sein. Sofern z.B. Führerscheine vorliegen müssen, reicht ein entsprechender Aktenvermerk, dass eine Prüfung erfolgte.

Informationen zu Diagnosen, zu familiären oder sozialen Problemen sowie ähnlich sensible und dem privaten Bereich zuzuordnende Informationen dürfen grundsätzlich nicht in der Personalakte gespeichert werden.

Fazit

Eine datenschutzgerechte Personalaktenführung ist in der Praxis alles andere als einfach. Tatsächlich kommt es darauf an, dass sich die Gesundheitseinrichtung über alle der hier behandelten Punkte Gedanken macht und entsprechende Prozesse in der Praxis umsetzt.

Gewährleistung der IT-Sicherheit im Gesundheitswesen

Zum Jahreswechsel 2020/21 ist das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (PDSG) in Kraft getreten. Dieses hält mit § 75c SGB V Verpflichtungen zur Gewährleistung der IT-Sicherheit bereit. Während bislang nur Betreiber Kritischer Infrastrukturen (Krankenhausbetreiber mit jährlich über 30.000 vollstationären Fällen) diese Anforderungen an die IT-Sicherheit erfüllen mussten, sieht die neue Regelung vor, dass ab dem 1.1.2022 alle Krankenhäuser diese Anforderungen zu erfüllen haben.

Dr. Sebastian Ertel

Je weiter die Digitalisierung im Gesundheitssektor voranschreitet, umso stärker muss der Fokus auf die IT-Sicherheit gelegt werden. Nicht zuletzt wegen der hohen Sensibilität der Daten, dem besonderen Vertrauensverhältnis zwischen Ärztinnen/Ärzten und Patientinnen/Patienten und dem erheblichen Schaden, der bei einem Verlust der Daten oder deren Kenntnisnahme durch Unbefugte entsteht.

Da die Thematik an sich nicht neu ist, aber jetzt auf alle Krankenhäuser ausgerollt wird, kann man auf bestehenden Grundsätzen und Standards aufbauen.

B3S-KH

Die Deutsche Krankenhausgesellschaft hat einen branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S-KH) erstellt und nach umfangreicher Überarbeitung Anfang 2019 dem

Bundesamt für Sicherheit in der Informationstechnik zur abschließenden Prüfung vorgelegt. Dieser wurde positiv beschieden. Er ist noch bis August 2021 gültig.

Die Anwendung des B3S-KH der Deutschen Krankenhausgesellschaft ist nicht verpflichtend, aber mangels vergleichbarer Ausarbeitungen alternativlos.

Innerhalb des B3S-KH sind sechs Schutzziele definiert:

- Verfügbarkeit
- Integrität
- Authentizität
- Vertraulichkeit
- Patientensicherheit
- Behandlungseffektivität

Für diese wurden 168 Maßnahmen definiert. Hinsichtlich der Umsetzung wird zwischen

- Muss-Maßnahmen,
- Soll-Maßnahmen und
- Kann-Maßnahmen

differenziert.

ISMS

Kern der Umsetzung des B3S-KH ist der Aufbau und Betrieb eines Informationssicherheits-Managementsystems (ISMS). Die entsprechend definierten Maßnahmen orientieren sich an den Vorgaben der ISO 27001 sowie der ISO 27799. In der Umsetzung bedeutet dies, dass die Erhebung und Dokumentation aller relevanter Strukturen, Prozesse und Abläufe erforderlich sind.

Umzusetzende Maßnahmen

Die 168 Maßnahmen des B3S-KH setzen sich aus 76 Maßnahmen zur technischen Informationssicherheit und 92 organisatorischen Maßnahmen zusammen.

Zu den organisatorischen Maßnahmen gehört insbesondere die Benennung

- eines Informationssicherheitsbeauftragten. Dessen Aufgabe besteht in der Überwachung und Kontrolle der getroffenen IT-Sicherheitsmaßnahmen und der Verfolgung der Entwicklung im Bereich der IT-Sicherheit. Hierdurch sollen potentielle Gefahren frühzeitig erkannt und daraus resultierende negative Auswirkungen für die Einrichtung verhindert werden.
- von Prozessverantwortlichen für jede Abteilung bzw. jeden Prozess (erfolgt keine Benennung, gilt die Geschäftsführung als prozessverantwortlich). Die Prozessverantwortlichen sollen die ihnen zugewiesenen Prozesse vollumfänglich kennen. Hierdurch sollen Abweichungen und damit verbundene Risiken schneller erkannt und entsprechende Gegenmaßnahmen eingeleitet werden können.

Weitere Ziele und Maßnahmen sind:

- die Sicherstellung der Aufrechterhaltung der kritischen Dienstleistungen im Störungs- oder Notfall.
- die Definition von Informationswerten/ Informationswertegruppen sowie der Umgang mit diesen Informationswerten, um die Ausfallwahrscheinlichkeiten von Hard- und Software prognostizieren zu können.
- der Schutz der relevanten IT-Systeme und Medizingeräte vor Ausfall externer Versorgungsdienste

Im Bereich der technischen Informationssicherheit sind beispielsweise folgende Maßnahmen zu betrachten:

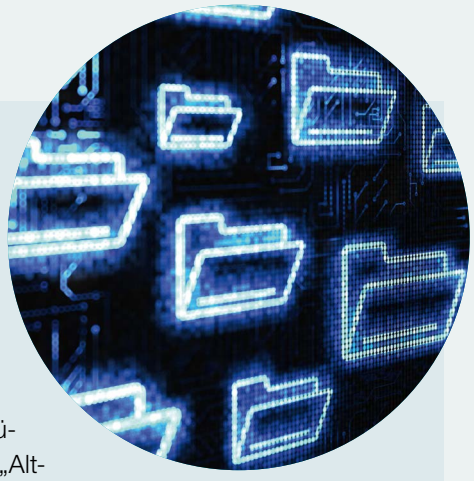
- Netz- und Systemmanagement; insbesondere durch die Segmentierung der Netzwerke soll eine Ausbreitung eines schädigenden Ereignisses in der gesamten Einrichtung verhindert werden.
- Absicherung der Fernzugriffe; es muss klar sein, welche Fernzugriffe bestehen und wie diese angestoßen bzw. abgesichert werden.
- Schutz vor Schadsoftware; hierzu gehören klare Regelungen und Vorgaben zum Umgang mit nicht autorisierter Software.
- Identitäts- und Rechtemanagement; über Rollen- und Berechtigungskonzepte muss definiert werden, welcher Benutzer entsprechend seiner Aufgaben auf bestimmte Daten zugreifen und diese verarbeiten kann. Neben klaren Vorgaben zur Vergabe, Änderung und Entziehung von Rechten, muss das Need-to-Know-Prinzip (Zugriff nur auf die tatsächlich benötigten Daten) umgesetzt werden.
- Sichere Authentisierung; der Zugang zu IT-Systemen und personenbezogenen Daten ist durch ein angemessenes Authentisierungsverfahren abzusichern (komplexe Passwörter, Änderungspflicht bei Initialpasswörtern).
- Absicherung der Nutzung von mobilen Geräten und Fernzugriffen innerhalb einer ungeschützten Umgebung
- Datensicherung, Datenwiederherstellung und Archivierung; die Verfügbarkeit der Daten muss durch ein Datensicherungskonzept gewährleistet sein, dessen Wirksamkeit regelmäßigen Überprüfungen unterzogen wird.
- Patch- und Änderungsmanagement
- Protokollierung
- Umgang mit Datenträgern; gerade bei mobilen Datenträgern besteht die latente Gefahr, dass diese verloren gehen oder in Vergessenheit geraten. Sofern diese regelmäßig

die Einrichtung verlassen, bestehen hier gesteigerte Risiken. Daher ist der Umgang klar zu regeln (Verschlüsselung, Aufbewahrung, Datenlöschung, Datenträgervernichtung).

- Softwaretests und Freigaben; Prüfung von Anwendungen und Weiterentwicklungen in einer abgesicherten und vom Produktivsystem getrennten Testumgebung grundsätzlich ohne den Einsatz von Echtdaten. Die Überführung von der Test- in die Produktivumgebung darf ausschließlich nach einem formalen Abnahme- und Freigabeprozess erfolgen.
- Datenschutz: „Die Krankenhausleitung MUSS eine Richtlinie zum Schutz personenbezogener Daten entwickeln, implementieren und kommunizieren." Leider führt der B3S-KH nicht aus, was im Detail in der Richtline geregelt werden muss.

Fazit

Viele der im B3S-KH geregelten Maßnahmen sollten in der Einrichtung seit Jahren gelebter Standard sein. Das soll aber keinesfalls darüber hinwegtäuschen, dass vor den Einrichtungen eine Menge Arbeit liegt. Ein Schwerpunkt wird in der Umsetzung der Dokumentationspflicht bestehen. Häufig ist diese nicht aktuell, wenn eine entsprechende Dokumentation denn überhaupt vorliegt. In vielen Fällen, so hat die Erfahrung gezeigt, besteht eine „Dokumentation ausschließlich in den Köpfen" der Mitarbeitenden der IT-Abteilung.



Kurznotiz:

Wann ist die Lagerung von Patientenakten keine Datenverarbeitung?

Die Überschrift der heutigen Kurznotiz wird bei Datenschützern vermutlich den Reflex auslösen, zu antworten, dass die Lagerung von Patientenakten immer auch eine Datenverarbeitung ist. Und diese Antwort ist richtig.

Allerdings schien es auf den ersten Blick so, dass ein Beschluss des Oberverwaltungsgerichts Hamburg vom 15.10.2020 (Az.: 5 Bs 152/20) dies anders sah. Nicht wenige Nachrichtenportale titelten in diesem Rahmen etwa mit Überschriften wie „Bloße Einlagerung von Patientenakten ist keine Datenverarbeitung i.S.d. DSGVO". Bei genauerer Betrachtung des Beschlusses zeigte sich aber, dass das Oberverwaltungsgericht Hamburg tatsächlich sehr nachvollziehbar (und anders) entschieden hatte. Denn in dem zugrundeliegenden Fall ging es darum, dass der Eigentümer eines Grundstücks dieses wieder nutzen konnte, da die bisherige Nutzerin – eine Krankenhausgesellschaft – aufgelöst wurde. Die bisherige Nutzerin hinterließ dem Eigentümer aber eine „Altlast" auf dem Grundstück, in Form eines prall mit Patientenakten gefüllten Archivs. Das Oberverwaltungsgericht Hamburg stellte insofern nur klar, dass das Auffinden eines solchen Archivs auf dem eigenen Eigentum keine Datenverarbeitung des Eigentümers darstellt und dieser insofern – zumindest datenschutzrechtlich – nicht in die Verantwortung genommen werden kann. Diese Entscheidung ist auch nachvollziehbar, denn das Auffinden von „herrenlosen" Akten allein stellt noch keine Lagerung dar.

Zu klären bleibt allerdings, wer zukünftig für die Akten verantwortlich sein wird?

© 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, 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: GettyImages, AOK-Verlag

Datenschutz in der Pflege

Der rechtskonforme Umgang mit sensiblen Daten ist unverzichtbare Voraussetzung für einen vertrauensvollen und selbstbestimmten Pflegeprozess. Jedoch sind gerade im Pflegebereich die rechtlichen Vorgaben zum Datenschutz seit jeher besonders vielgestaltig und mit Geltung der europäischen Datenschutz-Grundverordnung (DS-GVO) nochmals komplexer geworden. Dies gilt vor allem für das teils nur schwer durchschaubare Zusammenspiel der europäischen Verordnung mit dem nationalen Datenschutzrecht. Besonders zu berücksichtigen sind im Pflegebereich zudem auch sozialrechtliche Vorgaben, die ordnungsrechtlichen Regelungen der Landesheimgesetze und schließlich auch die Grundsätze der ärztlichen Schweigepflicht. So bedeutet es oftmals eine ganz erhebliche Herausforderung, all diese vielfältigen und mitunter sehr detaillierten rechtlichen Anforderungen im Pflegealltag rechtssicher und praktikabel umzusetzen.

Die Broschüre soll dabei helfen, diese Herausforderung erfolgreich zu meistern und die Anforderungen eines rechtssicheren Datenschutzes und verantwortungsvoller Pflege so gut wie möglich in Einklang zu bringen.

Als Arbeitshilfe im Alltag weist sie passgenau für den Pflegebereich den Weg durch das Dickicht des Datenschutzrechts und zeigt praxisnahe Lösungsansätze auf.

Broschüre HIER bestellen

Broschüre DIN A5, ca. 264 Seiten
Preis: 49,80 € pro Stück inkl. MwSt. und versandkostenfreier Zusendung im Inland
Art. Nr.: 43111 | **ISBN: 978-3-553-43111-8**

Aus dem Inhalt (Auszug):

- **A – Datenschutz in der Pflege: Die rechtlichen Grundlagen**
  Konkrete Vorgaben für die Datenverarbeitung in der Pflege
- **B – Datenschutzorganisation**
  Praktische Umsetzung der DS-GVO in Gesundheitseinrichtungen durch den Datenschutzbeauftragten
- **C – Der Internetauftritt**
  Internetauftritt und Social Media-Plattformen rechtssicher ausgestalten
- **D – IT-Sicherheit**
  Schutzziele der Datenverarbeitung
- **E – Corona-Update**
  Datenschutz in Pandemie-Zeiten

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/datenschutz-in-der-pflege