AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Dez. 2018 | Seite 1

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

INHALT

Mythen der DSGVO

Die neuen Gesetze (DSGVO, KDG, DSG-EKD) sind seit ein paar Monaten anzuwenden. Diese Anwendung treibt unterschiedliche Blüten. Am Anfang noch als Kuriosum belächelt, schlägt die Stimmung langsam um. Beschäftigte der Gesundheitseinrichtungen, Patienten und Dienstleister sind zunehmend genervt. Aber liegt das tatsächlich am Datenschutzrecht? Wir versuchen Licht ins Dunkel zu bringen, um dabei einigen Mythen und zum Teil absurden Prozessen die Daseinsberechtigung zu nehmen.

Dr. Sebastian Ertel

Alles nur noch mit Einwilligung?

In vielen Gesundheitseinrichtungen muss im Rahmen der Anmeldung nicht nur die Krankenversichertenkarte vorgelegt, sondern auch eine Datenschutzerklärung unterzeichnet werden.

Bei letzterer handelt es sich allerdings regelmäßig nicht um eine Erklärung, die unter dem Aspekt der Transparenz der Datenverarbeitung umfassend aufklären soll. Vielmehr soll diese Erklärung die Grundlage der weiteren Datenverarbeitung sein. Ohne Unterschrift, so die Annahme, „darf“ die Krankenversichertenkarte nicht eingelesen, der Patient nicht im System angelegt und die Behandlung nicht begonnen werden.

Mit der Inanspruchnahme der Dienstleistung einer Gesundheitseinrichtung wird ein Behandlungsvertrag geschlossen. Dieser bildet die Grundlage für die Verarbeitung der Daten, die für die Behandlung erforderlich sind. Daneben bestehen eine Vielzahl an gesetzlichen Regelungen, die zur Datenverarbeitung legitimieren bzw. sogar verpflichten (z.B. Infektionsschutzgesetz, Sozialgesetzbuch V, Personenstandsgesetz, Bundesmeldegesetz). Nur wenn sich

aus diesen Konstellationen (weitere ergeben sich aus Art. 6 DSGVO) keine Datenverarbeitungsgrundlagen ergeben, kann bzw. muss auf eine Einwilligung zurückgegriffen werden. Das wird allerdings nur in den seltensten Fällen der Fall sein (www.lda.bayern.de/media/FAQ_Rechtsgrundlage_der_Verarbeitung.pdf).

Mythos! Für die Datenverarbeitung bedarf es nur ausnahmsweise einer Einwilligungserklärung.

Name oder Nummer?

Auch immer wieder zu erleben ist die Situation, dass Patienten nur noch mit Namen aufgerufen werden, wenn sie hierin eingewilligt haben. Andernfalls erfolgt der Aufruf mittels Nummer, in der Regel mit der Patientennummer, unter der der Patient im System geführt wird.

Das Aufrufen des Namens gilt als sozial- und grundrechtsadäquate Praxis. Dagegen birgt die Nutzung einer Nummer ein erhebliches Risiko. Wird wie in dem meisten Fällen die Patientennummer genutzt, führt dies zu einer Entwertung dieses Pseudonyms. Häufig werden Dokumente oder Proben nur mit der Patientennummer versehen, wenn diese an externe Stellen, beispielsweise Labore, weitergegeben werden sollen. Dieser Identitätsschutz wäre aufgehoben, da eine Zuordnung bei entsprechender Aufmerksamkeit im Wartezimmer beim Aufrufen des Patienten möglich wäre. Darüber hinaus können sich massive Probleme ergeben, wenn ein Patient bei der falschen Nummer reagiert, etwa weil er die Ziffern zwei und drei akustisch falsch verstanden hat. Erfolgt kein Identitätsabgleich im Behandlungszimmer, wäre eine falsche medizinische Behandlung die Folge.

Mythos! Der Name des Patienten darf weiterhin aufgerufen werden.

Einbindung Dritter ist immer eine Auftragsverarbeitung?

In vielen Fällen wird die Heilbehandlung nicht nur durch das medizinische Personal der Gesundheitseinrichtung erbracht. In verschiedenen Konstellationen werden Externe mit eingebunden. Um auf Nummer sicher zu gehen, schließen viele Einrichtungen mit ihren Dienstleistern Auftragsverarbeitungsverträge ab bzw. die Dienstleister drängen auf den Abschluss eines solchen Vertrages. Tatsächlich ist der Abschuss einer entsprechenden Vereinbarung nicht in jedem Fall erforderlich. Gerade aus Sicht der Gesundheitseinrichtung ist es regelmäßig zweckmäßig, zu überprüfen, ob eine Auftragsverarbeitungssituation tatsächlich vorliegt. Denn in einer solchen bleibt die Einrichtung für die zu verarbeitenden Daten verantwortlich und muss den Dienstleister regelmäßig auf Einhaltung der gesetzlichen und vertraglichen Anforderungen überprüfen. Im Falle einer Datenpanne steht die Einrichtung in der Pflicht. Demgegenüber geht die Verantwortung bei einer Übermittlung (dem Gegenstück zur Auftragsverarbeitung) auf den Externen über. Dieser muss sich dann im Falle einer Datenpanne verantworten. Maßgebliches Abgrenzungskriterium ist, ob der Externe ein Eigeninteresse an den konkreten Daten hat bzw. ob die Datenverarbeitung nach Weisung erfolgt. Fehlt ein Eigeninteresse und erfolgt die Datenverarbeitung weisungsgebunden, liegt in der Regel eine Auftragsverarbeitung vor und ein entsprechender Vertrag muss abgeschlossen werden. Nach diesen Kriterien ist eine Auftragsverarbeitung grundsätzlich anzunehmen bei: externer Aktenvernichtung und -archivierung, Auslagerung der EDV und Softwaresupport durch den Hersteller mittels Fernzugriff.

Teilweise Mythos! Nur in bestimmten Fällen stellt die Einbindung Dritter eine Auftragsverarbeitung dar.

Externes Labor: Einwilligung des Patienten erforderlich?

Werden für die Untersuchung von Proben externe Laboratorien eingebunden, stellt sich regelmäßig die Frage nach den hierzu zu berücksichtigenden Anforderungen. Wichtig ist zunächst, dass die Inanspruchnahme von Dienstleistungen eines externen Labors keine Auftragsverarbeitung darstellt.

Eine Einwilligung ist nicht erforderlich, wenn das Labor von einem Berufsgeheimnisträger geführt wird. In diesem Fall wird zwischen dem Laborarzt und dem Patienten ein entsprechender Vertrag geschlossen. Wird das Labor nicht durch einen Berufsgeheimnisträger geführt, ist eine (mutmaßliche) Einwilligung des Patienten in die Datenweitergabe zwingend erforderlich (https://www.lda.bayern.de/media/FAQ_Auftragsverarbeitung_Arzt.pdf).

Teilweise Mythos! Nur bei Laboren, die nicht durch einen Berufsgeheimnisträger geführt werden, bedarf es einer Einwilligungserklärung.

Keine Datenweitergabe an weiter- oder mitbehandelnde Ärzte ohne Einwilligung?

Sind Ärzte verschiedener Einrichtungen an der Mit-/Weiterbehandlung eines Patienten beteiligt, liegt gegebenenfalls sogar ein Überweisungsschein vor, so sind nach § 9 Abs. 4 Berufsordnung-Ärzte alle beteiligten Ärzte von der ärztlichen Schweige-

pflicht befreit. Voraussetzung hierfür ist, dass das Einverständnis des Patienten vorliegt oder zumindest anzunehmen ist (mutmaßliches Einverständnis) und der Patient explizit über die Datenübermittlung informiert wurde. Liegt keine Überweisung vor, gilt § 73 Abs. 1b SGB V, d. h. die Datenübermittlung ist nur mit schriftlicher Einwilligung des Patienten möglich. Häufig findet sich die Situation, dass ein (weiter)behandelnder Arzt nach einem langen Zeitraum vorstellig wird und verschiedene Patientenunterlagen anfordert. Kann auf Grund der längeren Zeitspanne nicht mehr von einem Zusammenhang zur ursprünglichen Behandlung ausgegangen werden, bedarf es zwingend einer Schweigepflichtentbindung.

Beispiel: Ein Patient wurde in einer Gesundheitseinrichtung behandelt und in diesem Zusammenhang zur Weiterbehandlung an einen Kardiologen überwiesen. In unmittelbarem Zusammenhang mit der Überweisung dürfen die Patientenakte bzw. die relevanten Aktenteile, wenn der informierte Patient nicht widersprochen hat, dem Kardiologen zur Verfügung gestellt werden. Fragt der Kardiologe hingegen nach zwei Jahren Daten des Patienten ab, fehlt es an dem unmittelbaren Zusammenhang. Der Kardiologe muss eine Schweigepflichtentbindung vorlegen.

Kein Mythos! Im Rahmen der unmittelbaren Mit-/Weiterbehandlung kann von der Einwilligung ausgegangen werden, wenn der informierte Patient nicht widerspricht. Besteht eine erhebliche zeitliche Zäsur, muss eine ausdrückliche Einwilligungserklärung vorliegen.

Einwilligung erforderlich für die Abholung von Rezepten durch Dritte?

In bestimmten Situationen kann der Patient ein beispielsweise telefonisch angefordertes Rezept nicht persönlich abholen. Damit dieses an einen Dritten ausgehändigt werden darf, bedarf es einer Einwilligung. Ausreichend ist hier ein entsprechender Vermerk in der (digitalen) Patientenakte oder im Patientenverwaltungssystem. Dieser sollte das Datum der Einwilligung sowie den Namen der bevollmächtigten Person beinhalten. Zudem empfiehlt es sich, die Erklärung regelmäßig zu erneuern. Hierzu gibt es keinen festen Zyklus, als Richtwert sollten zwei Jahre angenommen werden.

Kein Mythos! In die Abholung durch Dritte muss der Betroffene einwilligen.

Der NEUE Datenschutz im Gesundheitswesen

Broschüre HIER bestellen

Europäische Datenschutz-Grundverordnung, ein ganz neues BDSG und unzählige novellierte Datenschutzvorschriften auf Bundes- und Landesebene – seit Mai 2018 ist die datenschutzrechtliche Landschaft in Europa und hierzulande eine grundlegend andere.

Die Broschüre soll Datenschutzverantwortlichen in Gesundheitseinrichtungen eine Hilfestellung an die Hand geben, sich in das neue Recht einzuarbeiten und die Datenverarbeitung in Gesundheitseinrichtungen auch künftig rechtskonform zu gestalten. Das Fachbuch vermittelt die neuen gesetzlichen Grundlagen, führt praxisnah in die Datenschutzorganisation einer Gesundheitseinrichtung ein und erläutert am Beispiel des Krankenhauses die zentralen rechtlichen Herausforderungen für Datenschutzverantwortliche.

Neben dem Datenschutz wird dabei auch das neue und zunehmend wichtigere Recht der IT-Sicherheit beleuchtet.

Broschüre DIN A5, ca. 380 Seiten
Preis: 89,90 € pro Stück inkl. MwSt. und versandkostenfreier Zusendung im Inland
Art. Nr.: 43100 | **ISBN: 978-3-553-43100-2**

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

Versand sensibler Daten per E-Mail

E-Mail-Kommunikation gehört mittlerweile zum Alltag. Täglich werden unzählige Nachrichten mit sensiblen Gesundheitsdaten zwischen den verschiedensten Einrichtungen versandt. Teilweise machen sich die Beteiligten dabei keine Gedanken über die im Hintergrund ablaufenden Prozesse und die Datensicherheit. Viel häufiger sind sich die Beteiligten des Problems allerdings bewusst, jedoch fehlt eine praxisgerechte Lösung.

Sven Venzke-Caprarese

Das Problem: Unverschlüsselte E-Mails haben grundsätzlich Postkartencharakter

Unverschlüsselte E-Mails verfügen grundsätzlich über keine Schutzvorrichtungen. Daher wird deren Sicherheit häufig mit einer Postkarte verglichen. Jede Person, die die Postkarte in den Händen hält, könne ohne weiteres deren Inhalte lesen.

Die Frage, ob E-Mails wirklich immer Postkartencharakter haben, muss dabei etwas differenziert betrachtet werden:

Interne E-Mails

Werden E-Mails innerhalb einer Einrichtung versendet und verlassen sie das interne Netz nicht, besteht zwar weiterhin Postkartencharakter. In vielen Fällen verlässt die Nachricht dann allerdings noch nicht einmal den Mailserver und durch technische und organisatorische Maßnahmen wird sichergestellt sein, dass grundsätzlich nur die befugten Mitarbeiter der Einrichtung Zugriff auf die E-Mail bzw. die E-Mail-Server haben.

In der Praxis hilft dies jedoch wenig, da Mitarbeiter in den seltensten Fällen von außen einschätzen können, ob interne E-Mails wirklich nur intern und angemessen sicher verarbeitet werden. Besteht hier kein ausdrückliches Konzept der Einrichtung, müssen auch intern versandte Mails wie Postkarten betrachtet werden, die von unbestimmten Überbringern zugestellt werden.

Transportverschlüsselung

Viele Mailserver unterstützen heutzutage eine Transportverschlüsselung bei der Übertragung von E-Mails und erzwingen diese teilweise sogar.

So können Betreiber von Mailservern z.B. bestimmen, ob E-Mails mit oder ohne Transportverschlüsselung versendet und abgerufen werden sollen. Der transportverschlüsselte Versand kann über TLS (Transport Layer Security) realisiert werden. Das Problem in der Praxis ist jedoch, dass nicht jeder der beteiligten Mailserver (Absender und Empfänger) entsprechend konfiguriert ist. Unterstützt ein Mailserver keine transportverschlüsselte Übertragung, ist es eine Frage der Einstellung des Mailservers, ob die E-Mail dann trotzdem unverschlüsselt übertragen wird oder nicht. In der Praxis finden sich häufig Einstellungen, bei denen die Mailserver auf unverschlüsselte Übertragungsprotokolle zurückfallen, wenn einer der Mailserver eine verschlüsselte Übertragung nicht unterstützt. Dies ist allerdings Einstellungssache.

Insbesondere für Gesundheitseinrichtungen wäre es daher überlegenswert, die eigenen Mailserver so zu konfigurieren, dass ausschließlich transportverschlüsselte Protokolle zum Einsatz

kommen und die E-Mail nicht versendet, sondern eine Fehlermeldung ausgegeben wird, wenn die Gegenseite diese sicheren Protokolle nicht unterstützt. In der Praxis kann dieser Weg allerdings zu Mehraufwand führen, sollte aber gleichwohl geprüft werden. Liegt eine wirksame Transportverschlüsselung vor, ist zumindest der Weg von Mailserver zu Mailserver abgesichert - die Postkarte insofern also mit einem verschlossenen Brief vergleichbar. Allerdings liegt die E-Mail auf den Mailservern dann wieder unverschlüsselt vor, was in vielen Fällen aber kein Problem darstellen dürfte.

Inhaltsverschlüsselung

Besonders heikel wird es, wenn von Einrichtungen Gesundheitsdaten oder sonstige besondere Arten personenbezogener Daten nach Art. 9 DSGVO mittles E-Mail übertragen werden sollen und bislang keine besonderen Schutzmaßnahmen auf der Ebene des Transports getroffen wurden oder bekannt sind. In diesen Fällen hilft oftmals nur eine Inhaltsverschlüsselung.

Public-Key Verfahren

Häufig wird eine Inhaltsverschlüsselung von E-Mails mittels sog. Public-Key Verfahren realisiert. In der Praxis sind hier insbesondere PGP und S/MIME zu nennen. Beide Verfahren sind relativ einfach anzuwenden, sofern sie erst einmal eingerichtet sind.

Das Problem ist jedoch, dass sowohl Absender als auch Empfänger die entsprechenden Verfahren einrichten müssen und vor der Kommunikation ein digitaler Schlüssel ausgetauscht werden muss. Insbesondere dann, wenn die Kommunikation mit vielen Kommunikationsteilnehmern erfolgen soll, die alle aus unterschiedlichen Infrastrukturen kommen, wird es in der Praxis schwer, sich auf ein Verfahren zu einigen und sicherzustellen, dass alle Kommunikationsteilnehmer dieses

eingerichtet haben. Zudem ist bei der Verwendung von Public-Key Verfahren ein Konzept der Einrichtung erforderlich, welches z.B. auf Vertretungssituationen und die Verfügbarkeit der E-Mails eingeht. Denn es wäre wenig gewonnen, wenn die E-Mails zwar vertraulich übermittelt werden, jedoch auf der Seite des Empfängers nicht mehr gelesen werden können, weil ungeregelte Vertretungssituationen entstehen, Mitarbeiter ausscheiden oder Schlüssel verloren gehen. Hier hilft jedoch ein gutes Konzept der Einrichtung.

Anhänge verschlüsseln

Eine in der Praxis häufig genutzte Möglichkeit, ist die Verschlüsselung der E-Mail-Anhänge. Beinahe alle gängigen Softwareverfahren, mit denen Dateien in ZIP-Formate gepackt werden können, unterstützen Funktionen der Dateiverschlüsselung. Allerdings müssen auch hier einige Besonderheiten beachtet werden:

- Die Dateien sollten mit mindestens AES 256 Bit verschlüsselt werden – dies muss in der Softwareanwendung eingestellt werden.
- Verschlüsselt werden lediglich die Anhänge, nicht die E-Mail an sich. Die Mail darf also keine personenbeziehbaren Daten enthalten.
- Auch die Dateinamen sollten verschlüsselt werden, sofern diese personenbeziehbare Daten enthalten. Eine entsprechende Einstellung ist meistens jedoch nicht vorkonfiguriert, sondern muss ausdrücklich angewählt werden.
- Der Absender der E-Mail muss ein angemessen komplexes Passwort wählen (mindestens acht Zeichen - besser zehn - darunter, mindestens ein großer und ein kleiner Buchstabe, eine Zahl und ein Sonderzeichen. Bei dem Passwort darf es sich nicht um ein Trivialpasswort handeln).

• Das Passwort muss auf anderem Wege als per E-Mail mitgeteilt werden (z. B. telefonisch). Besteht ein regelmäßiger Austausch zwischen zwei Kommunikationspartnern, kann im Vorfeld auch ein Standardpasswort gewählt werden, welches bis zu einem Widerruf oder einer Änderung immer wieder genutzt wird.

Fazit

Gesundheitseinrichtungen sollten sich mit der Frage einer angemessen sicheren E-Mail-Kommunikation beschäftigen. Es hilft hier wenig, Mitarbeitern mitzuteilen, dass keine (sensiblen) personenbezogenen Daten per unverschlüsselter E-Mail versendet werden dürfen, wenn keine angemessenen Alternativen zur Verfügung gestellt werden.

Kurznotiz:

Erstes Datenschutzbußgeld im Gesundheitsbereich

Die portugiesische Datenschutzbehörde hat gegen das Barreiro-Krankenhaus eine Geldstrafe in Höhe von 400.000 € verhängt. Hintergrund dieser Geldstrafe ist, dass die Zugangsrechte zu den klinischen Daten von Patenten nicht getrennt wurden.

Über das Krankenhaus-Informations-System der Einrichtung hätten mindestens neun Personen (nicht Mediziner, sondern Sozialarbeiter) Zugriff zu den klinischen Daten der Patienten. Zudem seien 985 Benutzer die Berechtigungsrolle „Arzt“ zugeordnet. Tatsächlich seinen nur 296 Ärzte im Krankenhaus beschäftigt.

Ferner habe die Einrichtung die eigenen Patientendaten nicht richtig von den archivierten Daten eines anderen Krankenhauses getrennt.

Diese Missstände wurden im Rahmen einer Inspektion, nach vorheriger Meldung der Ärztekammer, festgestellt. Die ersten beiden Verstöße wurden mit jeweils 150.000 €, der dritte mit 100.000 € geahndet. Dem Krankenhaus steht noch die Möglichkeit der gerichtlichen Überprüfung zur Verfügung.

© 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: iStock