AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Sept./Okt. 2019 | Seite 1

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

INHALT

Schriftform bei Schweigepflichtentbindungen

Für die Offenbarung von Daten, die der Schweigepflicht eines Berufsgeheimnisträgers unterliegen, bedarf es einer entsprechenden Legitimation. Diese kann aus einer gesetzlichen Regelung hergeleitet werden, die für einen konkreten Fall hinsichtlich bestimmter Daten die Übermittlung an einen Dritten erlaubt. Besteht eine solche gesetzliche Regelung nicht, bedarf es einer Schweigepflichtentbindung durch den Betroffenen. Diese Aspekte haben wir in vergangenen Newslettern umfassend thematisiert.

Dr. Sebastian Ertel

Was gibt es Neues?

§ 73 Abs. 1 b SGB V regelt den Datenfluss bezüglich Behandlungsdaten und Befunden zwischen Gesundheitseinrichtung und Hausarzt. Der Datenaustausch durfte bislang nur erfolgen, wenn durch den Patienten oder die Patientin eine entsprechende Einwilligung erteilt wurde. In der bis zum 10.5.2019 geltenden Fassung war diese Einwilligung zwingend schriftlich einzuholen. Zum 11.5.2019 trat das Terminservice- und Versorgungsgesetz (TSVG) in Kraft. Hierdurch erfuhr der § 73 Abs. 1 b SGB V eine massive Änderung.

Neben verschiedenen anderen Punkten ist wohl der wesentlichste, dass die Formulierung „mit schriftlicher Einwilligung“ durch „mit dessen Zustimmung“ ersetzt wurde.

Was bedeutet das?

Zumindest den Datenaustausch den Hausarzt betreffend kann nunmehr mit einer ausdrücklichen, mündlichen Einwilligung gearbeitet werden. Diese kann durch eine eindeutige Erklärung („Ja, ich will, dass Daten übermittelt werden“) oder eine entsprechende Geste (Kopfnicken auf eine entsprechende Frage) erfolgen.

Wird die Patientin oder der Patient im Rahmen der Aufnahme oder Entlassung nach dem nachbehandelnden Arzt zum Zwecke der Übermittlung des Entlassungsberichtes gefragt und nennt diese/r hierbei einen Namen, wird hieraus teilweise eine ausdrückliche Einwilligung hergeleitet. Der Patientin oder dem Patienten muss lediglich bewusst sein, dass durch das Handeln eine Übermittlung von Patientendaten ausgelöst wird.

Diese Sichtweise ist jedoch kritisch. Einerseits wird die Patientin oder der Patient bei der Aufnahme oder Entlassung mit so vielen Informationen konfrontiert, dass die Einwilligungserklärung unter Umständen unbewusst abgegeben wird. Zudem bedeutet ein Krankenhausbesuch für einzelne Patienten immer auch eine überfordernde Stresssituation. Diese werden zu allem „Ja“ sagen, um dieser Situation schnellstmöglich zu entkommen.

Was ist der sicherste Weg?

Im Streitfall muss seitens des Krankenhauses bewiesen werden, dass die Patientin oder der Patient eine Einwilligung in die Übermittlung von Gesundheitsdaten tatsächlich erklärt hat. Kann dieser Beweis nicht geführt werden, liegt eine unbefugte Offenbarung von (Gesundheits-)geheimnissen vor. Diese ist nach § 203 StGB strafbewehrt und kann im schlimmsten Fall auch zum Entzug der Approbation führen. Daneben sind Schadensersatzzahlungen gegenüber der betroffenen Person möglich. Letztlich bedeutet ein solcher Vorfall auch einen Reputationsschaden für das Krankenhaus.

Bereits aus diesem Grund sollte grundsätzlich der Weg über eine schriftliche Schweigepflichtentbindung gegangen werden. Dies bedeutet zwar eine strengere Regelung als in der DSGVO vorgesehen. Gleichwohl ist diese zulässig, da hierdurch das gesetzlich definierte Datenschutzniveau nicht unterschritten wird.

Kann, aus welchen Gründen auch immer, eine schriftliche Einwilligung nicht eingeholt werden, sollte die Entgegennahme einer mündlichen Erklärung hinreichend dokumentiert werden. Im Idealfall ist die Einwilligung gegenüber zwei Beschäftigten der Einrichtung zu erklären und diese im Krankenhaus-Informations-System der Einrichtung bzw. in der Patientenakte hinreichend zu dokumentieren. Neben dem Inhalt der Erklärung sollten Datum und Uhrzeit sowie Namen der Erklärungsempfänger erfasst werden.

Identitätsfeststellung bei Betroffenenanfragen

Sowohl bei der Einsichtnahme in die Patientenakte nach § 630g BGB als auch bei der Geltendmachung von Betroffenenrechten nach den Art. 15 ff. DSGVO (Recht auf Auskunft, Berichtigung, Löschung und Datenübertragbarkeit) stellt sich für die betroffene Gesundheitseinrichtung häufig die Frage: Ist die anfragende Person wirklich die betroffene Person? Denn es könnte schwerwiegende Konsequenzen haben, wenn eine Gesundheitseinrichtung auf Grund der Anforderung einer unberechtigten Person Daten einer anderen Person löscht, verändert, herausgibt oder an andere Stellen übermittelt.

Gesundheitseinrichtungen benötigen daher einen Prozess, der bei der Erfüllung von Betroffenenrechten gewährleistet, dass die anfragende Person auch diejenige ist, die sie vorgibt zu sein.

Sven Venzke-Caprarese

Vor Ort anwesende Personen

Sofern Patienten ihre Rechte in der Gesundheitseinrichtung vor Ort ausüben, wird die Identitätsprüfung in der Regel kein Problem sein. Hier kann und sollte die Gesundheitseinrichtung auf die Vorlage eines Ausweisdokuments bestehen, um die betroffene Person sicher zu identifizieren. Über das Ergebnis der Identitätsprüfung sollte ein Vermerk geschrieben werden. Das jeweils geltend gemachte Betroffenenrecht kann dann, sofern keine sonstige Verweigerungsgründe vorliegen, gewährt werden.

Nicht vor Ort anwesende Personen

Schwieriger wird es, wenn Betroffene ihre Rechte geltend machen, jedoch nicht vor Ort anwesend sind. Denkbar ist hier insbesondere eine Betroffenenanfrage per E-Mail, Telefon, Fax oder Brief.

Hier stellt sich in einzelnen Fällen die Frage, ob eine Identitätsfeststellung überhaupt erforderlich ist. Meldet sich eine betroffene Person z. B. auf einem der o. g. Kommunikationswege und verlangt die Übersendung von Aktenkopien an eine bereits im System bekannte Postanschrift, die der betroffenen Person zugeordnet ist, kann die Gesundheitseinrichtung zu dem Schluss kommen, dass eine Identitätsfeststellung nicht erforderlich ist. In vielen Fällen wird die Situation jedoch anders sein.

Verlangt die betroffene Person z. B. eine Auskunft an eine bislang nicht bekannte Postanschrift oder verlangt sie die Löschung, Berichtigung oder Portierung der Daten, wird die Gesundheitseinrichtung regelmäßig die Identität der Person überprüfen müssen, um sicherzugehen, dass es sich wirklich um die betroffene Person handelt, deren Daten verarbeitet werden sollen. Doch wie genau kann die Identitätsfeststellung erfolgen?

Diese Frage beantwortete eine Klinik aus Hamburg im Jahr 2018 für sich auf ganz spezielle Weise. Ein Patient, der zur Klinik einen Anreiseweg von mehreren Stunden gehabt hätte, forderte per E-Mail eine schriftliche und kostenfreie Auskunft über die zu seiner Person gespeicherten Daten gemäß Art. 15 DSGVO. Wie sich dem aktuellen Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten in Kapitel IV Ziffer 5 entnehmen lässt, erklärte sich die Klinik zwar grundsätzlich zur Auskunft bereit, forderte jedoch die Vorlage des Personalausweises vor Ort am Standort der Klinik. Nachdem sich die betroffene Person an die Aufsichtsbehörde wandte, stellte diese fest, dass die Anforderung der Klinik unverhältnismäßig war.

Geholfen hätte der Klinik im vorliegenden Fall vermutlich der „Datenschutz-Knigge für Identitätsfeststellungen, der sich im aktuellen Tätigkeitsbericht des Thüringer Landesdatenschutzbeauftragten unter Ziffer 6.5 wiederfindet. Demnach dürfen Verantwortliche im Rahmen von

Betroffenenanfragen, die nicht vor Ort gestellt werden, auch die Übersendung einer Ausweiskopie zur Identitätsfeststellung verlangen. Daten, die nicht zur Identifizierung benötigt werden, können allerdings von der betroffenen Person auf der Kopie geschwärzt werden.

Geschwärzt werden dürfen also regelmäßig:

- Ausweisnummer,
- Lichtbild,
- persönliche Merkmale,
- Staatsangehörigkeit.

Folgende Informationen des Personalausweises darf die verantwortliche Gesundheitseinrichtung jedoch nutzen:

- Name,
- Anschrift,
- Geburtsdatum,
- Gültigkeitsdauer.

Auch die Unterschrift darf übrigens genutzt werden, sofern die Gesundheitseinrichtung über eine solche verfügt und diese im Einzelfall mit der Unterschrift auf dem Personalausweis abgleichen möchte.

Betroffene müssen bei der Anforderung der Personalausweiskopie ausdrücklich auf die Möglichkeit zur Schwärzung hingewiesen werden. Diese Informationspflicht lässt sich bereits aus Art. 13 Abs. 2 lit. e DSGVO herleiten. Einige Details benennt der „Datenschutz-Knigge“ leider nicht. Nach Prüfung der Identität ist auch hier eine Dokumentation des Prüfergebnisses ratsam. Die Gesundheitseinrichtung muss sich zudem Gedanken machen, wann die Personalausweiskopie wie vernichtet wird. In der Regel sollte die Antwort lauten: Die Personalausweiskopie wird direkt nach der Prüfung datenschutzkonform gem. DIN 66399, beispielsweise mit einem Schredder, der mindestens die Stufe P4 erfüllt, vernichtet.

Kurznotiz:

Wieder Bußgeld wegen unzureichendem Berechtigungskonzept

Im letzten Jahr verhängte die Portugiesische Datenschutzaufsichtsbehörde ein Bußgeld im sechsstelligen Bereich, weil das Berechtigungskonzept des eingesetzten Krankenhaus-Informations-Systems (KIS) unzureichend war. Nun ist die Niederländische Datenschutzaufsichtsbehörde aktiv geworden. Aufgrund einer Beschwerde überprüfte sie das KIS-Berechtigungskonzept eines Krankenhauses und stellte gravierende Mängel fest. Auslöser war eine Beschwerde eines niederländischen Prominenten, der sich in dem Krankenhaus behandeln ließ. Mehrfach wurde auf dessen Krankenakte von verschiedenen Beschäftigten der Einrichtung, die in die Behandlung oder nachgelagerte Abrechnung nicht involviert waren, zugegriffen. Auch hier wurde ein hohes sechsstelliges Bußgeld verhängt, welches sich noch erhöhen kann, wenn die Mängel nicht innerhalb der gesetzten Frist abgestellt werden. Zwar wurden seitens des Krankenhauses jährliche Stichproben durchgeführt. Diese waren jedoch nach Auffassung der Aufsichtsbehörde so grobmaschig, dass eine effektive Schwachstellenfeststellung faktisch unmöglich war. Wir werden das Thema in einem der nächsten Newsletter detailliert behandeln und konkrete Handlungsempfehlungen geben.

© 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: gettyimages

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