DataAgenda-Arbeitspapier 35, 2/2022

DataAgenda - das Informationsportal zum Datenschutzrecht

Präsentiert von DATAKONTEXT

www.DataAgenda.de

@dataagenda

Elektronische Patientenakte

Seit dem 1. Januar 2021 stehen gesetzliche Krankenkassen in der Pflicht, ihren Versicherten die elektronische Patientenakte (ePA) zur Verfügung zu stellen. Der Zweck der ePA besteht darin, dass die Versicherten selbst ihre medizinischen Daten während einer Behandlung dem Arzt oder der Ärztin zur Verfügung zu stellen können.

Wichtig ist es, dass die ePA von den Versicherten verwaltet wird, die stets die „Souveränität über ihre Daten" behalten sowie deren Erstellung, Nutzung und Löschung nach eigenem Ermessen vornehmen können. Die ePA ersetzt weder die Dokumentationspflicht des behandelnden Arztes (§ 630f BGB), noch ersetzt sie die bisherige ärztliche Kommunikation. Das Gesetz im SGB V sieht nach der aktuellen Ausbaustufe (1. Januar 2022) eine weitere Ausbaustufe der ePA zum 1. Januar 2023 vor.

I. Verantwortlichkeit

Verantwortlicher ist gemäß Art. 4 Abs. 7 DS-GVO eine natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet oder aufgrund von EU-Recht oder dem Recht des jeweiligen Mitgliedsstaates dazu bestimmt ist. Dabei nutzt der Gesetzgeber bei der ePA die Öffnungsklausel, die in § 307 SGB V geregelt ist. Es gibt dabei drei Unterstrukturen: zentrale Zone, dezentrale Zone und Anwendungsinfrastruktur (§ 306 Abs. 2 SGB V).

Die Verzeichnisdienste zur Speicherung der ePA und anderen zentralen Diensten (z. B. VPN-Zugangsdienste für sichere Verbindungen zu dezentralen Zonen oder für PKI-Dienste oder zur Zuordnung von Teilnehmern) befinden sich im zentralen Bereich. Bei der dezentralen Zone wird die Telematik-Infrastruktur über leistungsstarke und sichere Router mit den Praxisverwaltungssystemen oder den Krankenhausinformationssystemen verbunden. Durch die Anwendungsinfrastruktur werden die Anwendungen wie die ePA-App oder das eRezept den Patienten zur Verfügung gestellt. Wenn es zum Download oder Upload der jeweiligen Daten kommt, wird eine Kopie der Daten erstellt.

1. Leistungsträger als Verantwortliche

Verantwortlicher ist der jeweilige Leistungsträger, also hauptsächlich die gesetzliche Krankenkasse, trotz der fehlenden Zugriffsmöglichkeiten auf die Daten. Das heißt der Leistungsträger ist für alle Datenverarbeitungen der ePA verantwortlich. Ausgenommen davon ist die Verantwortlichkeit für das Hoch- und Runterladen durch die Leistungserbringer.

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

2. Leistungserbringer als Verantwortliche

Der Leistungserbringer ist für den dezentralen Bereich verantwortlich. Aus Sicht des Leistungserbringers nimmt die Datenverarbeitung im Zusammenhang mit ePA zwei Formen an: einerseits das Hochladen von Dateien von PVS/HIS zu ePA als „Übertragung“ von Daten und andererseits von ePA zu PVS/HIS als „Erfassung“ von Daten“. Im Rahmen des ePA gelten die datenschutzrechtlichen Verantwortlichkeiten nur für diese beiden Verarbeitungsformen und nur in dezentralen Bereich. Gemäß dem Beschluss der Datenschutzkonferenz (DSK) vom 12.09.2019 ist der dezentrale Bereich gemeinsam mit der Gesellschaft für Telematik (Gematik) gem. Art. 26 DS-GVO verantwortlich.

3. Gematik als Verantwortliche

Die Gematik ist gemäß Art. 26 DS-GVO gemeinsam mit den Leistungserbringern in dezentralen Bereich verantwortlich. Sie legt die „Mittel“ der Verarbeitung fest. Die Gematik macht den Leistungserbringern Vorgaben zu den technischen Anforderungen und der Konfiguration von Konnektoren, VPN-Zugangsdiensten und Kartenterminals. Im Dezentralen hat sie die sog. „Auffangverantwortlichkeit“. Das bedeutet, dass sie für die Datenverarbeitung verantwortlich ist, wenn keine andere Verantwortlichkeit greift.

II. Auftragsverarbeiter

Der Einsatz eines Auftragsverarbeiters ist nach Art. 28 DS-GVO möglich. Die GKV beauftragt beispielsweise IT-Dienstleister als Auftragsverarbeiter von ePA-Systemen. Auf Dienstleisterebene kommen auch IT-Dienstleister als Auftragsverarbeiter in Frage, z.B. für die PVS, Konnektoren und Kartenterminals. Es gibt zahlreiche Anforderungen an die möglichen Auftragsverarbeiter. Handelt es sich bei dem Auftragsverarbeiter um einen „Betriebsdienstleister“ der TI, wie z. B. einen Anbieter von ePA-Dateisystemen und zugehörigen Komponenten und Diensten, muss dieser zunächst von der Gematik zugelassen werden (§§ 324, 325 SGB V). Zusätzlich zu den allgemeinen Anforderungen müssen alle Auftragsverarbeiter im Zusammenhang mit der ePA die technischen Anforderungen der Gematik-Spezifikation zu Schnittstellen, Komponenten und Diensten erfüllen und diese auch regelmäßig erneuern. Auftragsverarbeiter, die nicht innerhalb der EU ansässig sind, dürfen ausschließlich mit einem Angemessenheitsbeschluss beauftragt werden.

III. Rechtmäßigkeit

Die Zulässigkeit einer Verarbeitung personenbezogener Daten bestimmt sich in Abhängigkeit vom Verhältnis zwischen Versicherten, Leistungserbringer und Leistungsträger. Unterschieden wird bei der Verarbeitung zwischen zwei Phasen: Erstens die Einrichtung und zweitens die Nutzung der ePA. Im Verhältnis zwischen dem Versicherten und der GKV erfolgt die Datenverarbeitung zur Erstellung der ePA auf Grundlage der Einwilligung des Versicherten. Die Erstellung und Nutzung der ePA unterliegt daher der Voraussetzung der Freiwilligkeit. Das heißt, dass diese Datenverarbeitung nur auf Verlangen des Versicherten erfolgt (§ 341 Abs. 1 SGB V). Weiter kann der Versicherte jederzeit dessen Löschung verlangen (§ 344 Abs. 3 SGB V). Aus Sicht der GKV hat der Verzicht auf die ePA keine Nachteile. Während der Nutzungsphase darf die GKV nur aufgrund einer gesetzlichen Richtlinie auf die ePA zugreifen.

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Im Verhältnis zwischen dem Versicherten und dem Leistungserbringer ist der Zugriff nur nach freiwilliger Einwilligung des Versicherten möglich (vgl. § 353 SGB V). Als weitere Voraussetzung für die Rechtmäßigkeit der Datenverarbeitung muss der Zugriff in einer bestimmten Verarbeitungsform erfolgen (vgl. § 352 Abs. 1 SGB V). Daher ist die Einwilligung des Patienten für die Rechtmäßigkeit der Datenverarbeitung erforderlich, aber allein nicht ausreichend. Unklar ist das Verhältnis der beiden hier angesprochenen Rechtsgrundlagen (Einwilligung und Erfüllung des Behandlungsvertrages).

Unklarheiten bestehen aktuell, „wann" Ärzte auf die Daten zugreifen können und es gibt Fragen dazu, „ob" sie darauf zugreifen müssen. Die Ermittlung und Bewertung von Informationen aus einer ePA kann haftungsrechtlich durchaus relevant werden. Grundsätzlich muss der Arzt die Informationen aus der ePA nur abrufen und ggf. speichern, sofern dies für eine konkrete Behandlungssituation erforderlich ist. Geschieht dies trotz Zugangsmöglichkeit dennoch nicht, kann dies als haftungsrechtlicher Fehler in der Krankenakte gewertet werden. Die ePA führt keine neuen zivilrechtlichen Haftungsregelungen ein. Daher folgt die Haftungsfrage den bekannten Regelungen im deutschen Bürgerlichen Gesetzbuch (BGB). Der Arzt muss dann im Rahmen der Anamnese gezielt nach Vorbehandlungen und dazugehörigen Unterlagen fragen, wenn er keinen Zugriff zur ePA vornimmt. Soweit es medizinisch geboten ist, müssen die erhaltenen Behandlungsunterlagen gelesen werden.

IV. ePA 2.0: Was ist neu?

Mit der ePA 2.0 traten zum 1. Januar 2022 einige relevante Änderungen ein. Es wurden sogenannte stationäre Clients eingeführt, d. h. die ePA kann jetzt sowohl über das Smartphones/Tablets wie auch über den PC genutzt werden. Darüber hinaus sind weitere Nutzergruppen hinzugekommen: hierzu zählen u.a. Pflegeberufe, Hebammen, Physiotherapeuten, öffentliche Gesundheitsdienste, Arbeitsmedizin und Rehakliniken. Besonders hervorzuheben ist die Einführung einer komplexen Berechtigungsvergabe. Die delegierte Geschäftsführung hat bereits im Gesetzgebungsverfahren des Patientendatenschutzgesetzes (PDSG), welche die gesetzlichen Regelungen zur ePA enthält, Kritik auf sich gezogen und nach dessen Inkrafttreten zu einer förmlichen Abmahnung durch den Bundesdatenschutzbeauftragten (BfDI) geführt. Versicherte können den Zugang derzeit nur grob nach dem „Alles-oder-Nichts"-Prinzip gewähren. Dies steht im Widerspruch zu der DS-GVO und der Patientensouveränität, da es nicht mit den Pflichten des Verantwortlichen gemäß Art. 25 DS-GVO vereinbar ist. Weder die Datenminimierung i.S.d. Art. 5 Abs. 1 lit. c DS-GVO noch ein robustes Zugriffsmanagement (vgl. Art. 32 DS-GVO) wurde eingebaut. Mit der ePA 2.0 ist dies nun behoben wurden.

V. Ausblick: ePA 3.0

Die ePA 3.0 fügt in Zukunft eine Reihe weiterer neuer Funktionen hinzu wie insbesondere die automatische Einrichtung von Daten aus digitalen Gesundheitsanwendungen (DiGA) sowie die Freigabe von Daten für Forschungszwecke. Die digitalen Gesundheits- oder Medizinanwendung sind digitale Anwendungen, die ein Arzt verschreiben oder eine versicherte Person direkt bei einer Krankenkasse beantragen kann. Solche Anwendungen müssen von der Gematik authentifiziert werden bevor sie sich mit der ePA verbinden. Darüber hinaus können Versicherte mit der Einführung von ePA 3.0 ihre Daten auf vielfältige Weise für Forschungszwecke nutzen. Dies basiert natürlich auf der rein freiwilligen Zustimmung des Patienten. Damit gibt es die Möglichkeit der Bereitstellung von ePA-Daten an Forschungsrechenzentren nach § 303d SGB V zur Verwendung in gesetzlich geregelten Forschungsvorhaben (§ 363 Abs. 1 bis 7 SGB V) oder an einzelne Forschungsvorhaben (§ 363 Abs. 8 SGB V).

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

VI. COVID-19

Der Corona-Expertenbeirat der Bundesregierung äußerte sich erst kürzlich über die Dringlichkeit der schnellen Umsetzung der verbesserten ePA:

„Der ExpertInnenrat empfiehlt dabei die umgehende Umsetzung der Empfehlungen aus dem 2021 erstellten Gutachten des Sachverständigenrats zur Begutachtung der Entwicklung im Gesundheitswesen [...] Gesundheitsdaten sollten möglichst zeitnah einzelfallbasiert und vollständig in Form einer elektronischen Patientenakte vorliegen und neben dem Zweck der verbesserten Patientenversorgung auch für die anonymisierte wissenschaftliche Auswertung zugänglich sein.[1]"

Das die Bundesregierung beratende Gremium hält es demnach für besonders wichtig, dass auch ePA 3.0 so schnell wie möglich umgesetzt wird, um die Daten auch zu Forschungszwecken verwenden zu können.

VII. Fazit

Es zeigt sich, dass die ePA im aktuellen Entwicklungsstadium den Anforderungen der „Patientensouveränität" noch nicht vollständig und damit hinreichend gerecht wird. Gerade beim Berechtigungsmanagement ist es rätselhaft, warum man mit der Version 1.1 keine Zugriffsrechte auf Einzeldokumentebene gewähren kann. Zusätzlich zu den Vorteilen, welche die ePA ganz unstrittig bietet, sehen sich Leistungserbringer wie insbesondere die Ärzteschaft neuen rechtlichen Unsicherheiten und Risiken in Bezug auf ihre Patienten gegenüber. Zum Thema Haftungsrecht sollten Ärzte die ePA unbedingt in ihren Arbeitsablauf integrieren und als Informationsquelle im Rahmen der Krankenakte aktiv nutzen.

1 ExtpertInnenrat der Bundesregierung zu COVID-19, 2022, 4. Stellungnahme des ExpertInnenrates der Bundesregierung zu COVID-19: Dringende Maßnahmen für eine verbesserte Datenerhebung und Digitalisierung, S. 1 f.

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Seminartipp zum Arbeitspapier

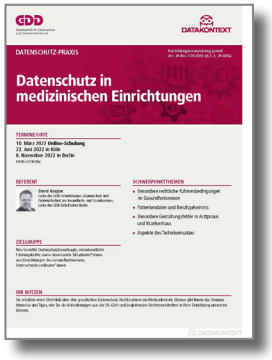
Datenschutz in medizinischen Einrichtungen

In den meisten Branchen muss hier und da auch mit besonders schützenswerten Daten umgegangen werden, was eine gesteigerte Sensibilität und Sorgfalt bei der Ausgestaltung der Datenverarbeitung erfordert. Im Gesundheitswesen dreht sich dagegen (fast) alles um solch besondere Daten. Die Herausforderung, Patientendaten stets gesetzeskonform zu verarbeiten und zu nutzen, scheint unüberwindlich – ist sie es auch?

Neben der Patientenbehandlung als solche stehen weitere Herausforderungen im Raum: die zunehmende Digitalisierung, neue Technologien und Versorgungsformen sowie ein enormer Kostendruck. Als wäre dies bisher nicht genug, kommen nun vielfältige Rechtsänderungen auch auf die Einrichtungen des Gesundheitswesens hinzu.

Dieses Seminar soll Ihnen neben einem Überblick über den spezifischen Datenschutz-Rechtsrahmen im Medizinbetrieb auch Hinweise zur Bewältigung einer Reihe damit zusammenhängender Probleme bieten.

Weitere Infos finden Sie hier.



DataAgenda
ist das Informationsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet Videos, News, Whitepaper und Seminartipps rund um den Datenschutz.

Datakontext
ist einer der führenden Fachinformationsdienstleister in den Bereichen Datenschutz und IT-Sicherheit und bietet Kompetenz aus einer Hand: Fachbücher, Fachzeitschriften und Seminare, Zertifizierung und Beratung.

Prof. Dr. Rolf Schwartmann
Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V (GDD), Leiter der Kölner Forschungsstelle für Medienrecht (TH Köln) und Mitglied der Datenethikkommission.

Dr. Tobias Jacquemain, LL.M. (GDD e.V.)
Promotion zum Schadensersatz für Datenschutzverstöße nach Art. 82 DS-GVO und Lehrbeauftragter an der Universität zu Köln, an der Technischen Hochschule (TH) Köln sowie an der TH Georg Agricola in Bochum.

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com