Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

„Das Patientendaten-Schutzgesetz und die elektronische Patientenakte“

Gemeinsame Veranstaltung von vier
psychotherapeutischen Berufsverbänden Nordrhein

virtuell

18 Februar 2022

Es gilt das gesprochene Wort

Sehr geehrter Herr Dr. Bergmann,

sehr geehrte Damen und Herren,

I. Einleitung

ich freue mich, Ihnen auch meine Sicht auf das sogenannte Patientendaten-Schutzgesetz und die sogenannte elektronische Patientenakte darstellen zu können. Die Begriffe sind im Bundesgesundheitsministerium entstanden und ich kann Ihnen verraten, die Bindestriche im Wort „Patientendaten-Schutz-Gesetz“ sind während der Gesetzberatungen ein paarmal neu gesetzt worden.

Was auf jeden Fall nicht stimmt ist, dass es ein „Patientendatenschutzgesetz“ ist, wie es sich phonetisch anhört: es ist weder ein Patientendatengesetz und erst Recht kein Datenschutzgesetz. Geregelt werden nämlich nicht Patientendaten, sondern – da die gesetzlichen Krankenkassen durch dieses Gesetz verpflichtet werden, ihren Versicherten eine elektronische Akte anzubieten – Versichertendaten. Diese Versichertendaten werden – wie ich gleich ausführen werde und wie die Anweisungsbescheide des Bundesdatenschutzbeauftragten an Krankenkassen zeigt – im Sinne des Datenschutzes auch nicht gut behandelt: ein Datenschutzgesetz ist es also auch nicht.

Dementsprechend ist auch die „elektronische Patientenakte“ **keine Patientenakte**, sondern sie heißt aufgrund des Gesetzes nur so.

Patientenakten werden dort geführt, wo der Mensch Patient ist – dies ist er beim Arzt oder beim Zahnarzt, beim Therapeuten oder im Krankenhaus. Überall werden Patientenakten geführt, auch elektronisch.

Nahezu alle Ärztinnen und Ärzte haben ein Praxisverwaltungssystem. In den Krankenhäusern gibt es Krankenhausinformationssysteme, die selbstverständlich weitergeführt werden müssen. Bei der sogenannten elektronischen Patientenakte handelt es sich eigentlich um eine „elektronische Gesundheitsakte“, denn **die Versicherten** der Krankenkasse haben mit ihr die Möglichkeit, digital ihre Gesundheitsdaten an einem einigermaßen sicheren Ort zu speichern.

Von „einigermaßen sicher“ spreche ich aber nur, weil alles, was von Menschenhand gemacht ist, nie zu einhundert Prozent sicher ist. Aber der Speicherort ist schon sehr sicher. Analoge Speicherung, d.h. Papierakten, sind zudem keineswegs sicherer: Zu häufig lagen Patienten- und auch Versichertenakten aus Papier auf meinem Schreibtisch, die wir etwa in Abfallbehältern gefunden haben.

II. Das Patientenschutzgesetz

Es ist ein sogenanntes Artikelgesetz, in dem u.a. das Apothekengesetz, das Krankenhausentgeltgesetz, das Krankenhausfinanzierunggesetz, das Transplantationsgesetz, das Elfte Buch Sozialgesetzbuch, in dem die gesetzliche Pflegeversicherung geregelt ist usw., geändert wurden. Die bei weitem wichtigste Änderung betraf allerdings das Fünfte Buch Sozialgesetzbuch, in dem die gesetzliche Krankenversicherung geregelt ist.

Hier wurde ein 11. Kapitel mit der Überschrift „Telematikinfrastruktur“ und das 12. Kapitel mit der Überschrift „Interoperabilitätsverzeichnis“ mit insgesamt 88 neuen Paragraphen eingefügt. Das Fünfte Buch Sozialgesetzbuch ist mittlerweile so kompliziert wie die Steuergesetze. Vieles hätte daher dafür gesprochen, die Telematikinfrastruktur und die elektronischen Patientenakte in einem besonderen Einzelgesetz zu regeln. So wurde das Gesetz über die gesetzliche Krankenversicherung noch umfangreicher, noch komplizierter und noch unüberschaubarer.

Ein Grund dafür, das alles doch im Fünften Buch Sozialgesetzbuch zu regeln, ist, dass man in § 307 SGB V den gesetzlichen Krankenkassen der Verantwortung für die Telematikinfrastruktur und die sogenannte elektronische Patientenakte auferlegt hat. Daher war ich gehalten, die Anweisungsbescheide, auf die ich gleich noch näher eingehe, gegen gesetzliche Krankenkassen zu richten.

III. Die elektronische „Patientenakte“

Zunächst möchte ich Ihnen eine Einführung in die Zielsetzung und grobe Funktionsweise der elektronischen Patientenakte als Bestandteil der Telematikinfrastruktur der elektronischen Gesundheitskarte (elektronische Gesundheitskarte) geben und dabei auch auf ihre Chancen eingehen.

Um es deutlich zu sagen: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit befürwortet eine gutgemachte Digitalisierung im Gesundheitswesen und auch eine gutgemachte elektronische Gesundheitsakte, im Terminus des Bundesgesundheitsministeriums:

elektronische Patientenakte. Neben direkten Vorteilen für die Versorgung kann sie auch Patientenrechte stärken. Wenn Versicherte einen sicheren Datenspeicher für ihre Dokumente erstellen können, kann das ein großer Vorteil gegenüber aktuellen Lösungen wie E-Mails oder Papierausdrucken sein: Aus Versorgungs- und aus Datenschutzsicht!

Die elektronische Patientenakte ist explizit als eine von den gesetzlichen Krankenkassen ihren Versicherten anzubietende versichertengeführte Akte benannt. Völlig zu Recht hat die Bundesregierung in der Begründung zum Patientendaten-Schutz-Gesetz die Wahrung der Patientensouveränität als eine der wichtigsten Vorgaben betont.

Die elektronische Patientenakte soll dabei nicht die Behandlungs-dokumentation oder andere Akten von Ärzten, Krankenhäusern oder anderen Leistungserbringern ersetzen. Auch die direkte Kommunikation zwischen Leistungserbringerinnen und Leistungserbringern ist nicht Zweck der elektronischen Patientenakte. Da die elektronische Patientenakte versichertengeführt ist, entscheiden die Versicherten selbst, welche Daten sie in diese einstellen und welche nicht. Das können und müssen sie nicht ausschließlich anhand von medizinischen Gesichtspunkten tun. Daher kann die elektronische Patientenakte auch nicht als vollständige Fallakte gelten, wie sie Ärztinnen und Ärzte führen.

Wie bisher wird sich wohl in der direkten Kommunikation zwischen Arzt und Patient bei der Behandlung herausstellen, welche Dokumente benötigt werden.

Die elektronische Patientenakte kann dann über die Telematik-infrastruktur ein sicherer Weg sein, um diese Dokumente zu übergeben. In der analogen Welt entspricht die sogenannte elektronische Patientenakte einem Ordner, in dem alle medizinischen Befunde, Arztberichte, etc. vom Versicherten gesammelt werden und den er zu seinen Arztbesuchen mitnimmt.

Die Regelungen des Patientendaten-Schutz-Gesetzes widersprechen leider seiner eigenen Prämisse der Patientensouveränität. Ich habe deshalb gegenüber den gesetzlichen Krankenkassen drei wesentliche Punkte der elektronischen Patientenakte benannt, die gegen die Datenschutz-Grundverordnung verstoßen, wenn keine zusätzlichen Maßnahmen ergriffen werden.

Kritik

Aus Sicht des Datenschutzes bei der elektronischen Patientenakte gibt es **drei gravierende Schwachstellen**:

1. Das Berechtigungsmanagement wegen des „Alles oder nichts Prinzips“,

2. Frontend-Nicht-Nutzer, d.h. diejenigen, die kein Smartphone oder ein Tablet haben, werden benachteiligt,

3. die Umsetzung des alternativen Authentisierungsverfahrens muss verbessert werden.

1. Berechtigungsmanagement

Beginnen möchte ich mit dem defizitären Berechtigungsmanagement, das auch Inhalt einer „Anweisung“ war, die ich gegenüber in meine aufsichtsbehördliche Zuständigkeit fallenden bundesunmittelbaren gesetzlichen Krankenkassen als datenschutzrechtlich Verantwortliche ausgesprochen habe. Worum geht es?

Dokumente werden nach einem festgelegten Schema in der elektronischen Patientenakte abgelegt. In der ersten Phase 2021 gab es nur zwei Fächer. Dokumente aller Leistungserbringer, d.h. aller Ärzte, Ärztinnen, Zahnärzte, Zahnärztinnen, Therapeutinnen und Therapeuten sowie aller Krankenhäuser und Kliniken kommen gesammelt in ein Fach. Dokumente, die Versicherte selbst einstellen, in ein zweites Fach.

Die Dokumente im Leistungserbringerfach sind besonders wichtig. Sie stammen von Leistungserbringern, also z.B. vom Hausarzt, der Hausärztin, vom Kardiologen oder vom Krankenhaus oder der Reha-Klinik. Diese sind als Einsteller auch nachweisbar. Für jedes Dokument kann daher nachgewiesen werden, dass es nicht verändert wurde und von welchem Leistungserbringer es stammt.

Dokumente im Versichertenfach haben diese Eigenschaft nicht. Zwar können Versicherte natürlich auch ärztliche Dokumente einscannen und in der elektronische Patientenakte digitalisieren. Es ist aber nicht mehr nachweisbar, ob sie unverändert wurden oder überhaupt vom Leistungserbringer stammen.

Wo sah nun der Bundesdatenschutzbeauftragte den Missstand beim Berechtigungsmanagement?

Als Versicherter konnte ich jedem Arzt in 2021 nur eine Berechtigung für ein ganzes Fach erteilen. Ich konnte meinem Arzt nicht nur einzelne Dokumente zuweisen. Ich konnte auch nicht einzelne Dokumente ausschließen. Die Zugrifferlaubnis erstreckte sich immer auf das komplette Fach. Das heiß, jeder zugelassene Arzt oder Therapeut sah alles. Um es deutlich zu machen: Der Physiotherapeut hatte dann auch Zugang etwa zu den Dokumenten, die vom Gynäkologen oder vom Zahnarzt stammen. Brauchte der Physiotherapeut dies? Das kritisierte ich unter dem Schlagwort „Alles-oder-nichts-Prinzip“.

Weder aus Sicht der Versicherten noch der Leistungserbringer ist so eine ausschließliche Pauschalfreigabe fachlich sinnvoll. Natürlich ist es in vielen Situationen – z.B. gegenüber einem Hausarzt – sinnvoll, möglichst viele Informationen zur Verfügung zu stellen. Es gibt aber auch Situationen, in denen eine dokumentengenaue Steuerung nötig ist. Versicherte wollen vielleicht eine psychiatrische Behandlung ihrem Zahnarzt nicht bekannt machen.

Verstärkend kommt hinzu, dass Berechtigungen für bis zu 18 Monate gültig sind und somit das Tor zum gesamten Dokumentenbestand lange offen steht. Allerdings dürfen die Leistungserbringer legal nicht jederzeit auf alle Daten zugreifen: Das Gesetz formuliert explizit den schon in der Datenschutz-Grundverordnung verankerten Grundsatz der Zweckbindung:

Der Zugriff ist mit Einwilligung der Versicherten nur zulässig, soweit er für die Versorgung erforderlich ist. Der Versicherte kann nur nicht überprüfen, ob sich der Arzt, Therapeut oder das Krankenhaus daran hält.

Das „Alles-oder-nichts-Prinzip“ war auch schlicht nicht zeitgemäß. Wir wissen alle, dass eine dokumentengenaue Zugriffsfreigabe am Markt Standard und damit technisch auch leicht möglich ist. Da fallen mir viele Alltagsbeispiele ein, vom Betriebssystem über Cloudspeicher bis zum Teilen von Fotos in sozialen Netzwerken. Aber auch Hersteller medizinischer Software haben in der Debatte, dass ihre Software feingranulare Berechtigungen zulässt.

Das „Alles oder nichts Prinzip“ widerspricht der Datenschutz-Grundverordnung. Die Datenschutz-Grundverordnung definiert in Artikel 5 die Grundsätze, die eingehalten werden müssen, wenn Daten verarbeitet werden. Nach Artikel 25 Datenschutz-Grundverordnung müssen Verantwortliche – also hier die Krankenkassen – geeignete Maßnahmen ergreifen, um diese Grundsätze auch umzusetzen. Ein feingranulares, dokumentengenaues Berechtigungsmanagement ist eine solche Maßnahme. Es sorgt dafür, dass nur die notwendigen Dokumente „geteilt“ werden und alle anderen eben verborgen bleiben. Das entspricht den Grundsätzen der Rechtmäßigkeit, der Datenminimierung, der Erforderlichkeit und Zweckbindung sowie der Vertraulichkeit. Nach aktuellem Stand der Technik ist so ein dokumentenspezifisches, feingranulares Berechtigungsmanagement sehr wohl möglich. Das zeigt eine Vielzahl von Anwendungen auf dem Markt.

Damit verstößt das „Alles oder nichts Prinzip“ also gegen die Vorgaben in Artikel 25 sowie Artikel 5 Absatz 1 Datenschutz-Grundverordnung.

Erst seit dem 1. Januar diesen Jahres gibt es die Möglichkeit, dokumentengenaue Berechtigungen zu vergeben.

Allerdings haben diese Möglichkeit nur die Nutzer der elektronische Patientenakte-App auf einem Smartphone oder einem Tablet. Fast alle anderen können das nicht (erste Ausnahmen KNAPPSCHAFT + weitere KK). Das bringt mich zu meinem zweiten großen Kritikpunkt:

2. Benachteiligungen für Frontend-Nichtnutzer, d.h. für Menschen, die kein Smartphone oder Tablet haben

Die elektronische Patientenakte als Akte existiert ganz ohne eine „App“. Sie ist zunächst lediglich das Aktensystem „in der Telematikinfrastruktur-Cloud“. Versicherte können sie bei ihrer Krankenkasse beantragen und sie z.B. bei ihrem Hausarzt ersteinrichten lassen. Der ist auch verpflichtet, auf Wunsch des Versicherten medizinische Daten aus der Behandlung in die elektronische Patientenakte zu kopieren. Bei einem weiteren Arztbesuch können diese Daten dann aus der elektronische Patientenakte freigegeben werden. Dazu stecken die Versicherten ihre elektronische Gesundheitskarte in das Kartenlesegerät und bestätigen die Freigabe mit ihrer PIN.

Zusätzlich stellen die Krankenkassen den Versicherten eine elektronische Patientenakte-App zur Verfügung. Versicherte, die die App nicht nutzen wollen oder können, werden als Frontend-Nichtnutzer bezeichnet. Eine ganze Reihe von Funktionen dieser App bilden elementare Einsicht- und Kontrollrechte bzgl. der elektronischen Patientenakte ab. Zunächst ist das Berechtigungsmanagement zu sehen, über das ich schon vorher berichtet habe. Ohne App können Versicherte vor Ort in Praxis oder Krankenhaus am Kartenterminal ab 2022 lediglich „mittelgranular“ freigeben. Dazu werden Kategorien von Dokumenten gebildet. Auf diese Kategorien beziehen sich dann die Berechtigungen. Eine dokumentengenaue Steuerung ist vor Ort in der Praxis nicht möglich. Ein konkreter Zeitpunkt für die Einführung von feingranularem Berechtigungsmanagement vor Ort in der Praxis wurde im Gesetzgebungsverfahren aus dem Entwurf gestrichen.

Die nächste wichtige Funktion, die ohne App nicht genutzt werden kann, ist die Protokolleinsicht. Die elektronische Patientenakte protokolliert alle Zugriffe und Zugriffsversuche. Um Missbrauch aufzudecken ist es wichtig, dass ich selbst nachvollziehen kann, wer auf meine Akte zugegriffen hat. Berechtigungen werden an die ganze Institution (etwa eine Gemeinschaftspraxis oder eine Praxisgemeinschaft[1] oder das Krankenhaus) vergeben und sind ab 2022 auch in ihrer Dauer nicht begrenzt.

[1] Im Unterschied zu einer Praxisgemeinschaft, die sich nur die gemeinsamen Praxisräume und ggf Personal teilt (Kostengemeinschaft), aber ansonsten eigenständig sind und getrennt abrechnen, ist eine Gemeinschaftspraxis (heute Berufsausübungsgemeinschaft) in der Regel als Gesellschaft bürgerlichen Rechts (GbR) oder als Medizinisches Versorgungszentrum (MVZ) organisiert und bildet eine Abrechnungsgemeinschaft.

Vielleicht habe ich ja einige Berechtigungen vergessen, die ich vor längerer Zeit vergeben habe? Auch eine Übersicht über die vergebenen Berechtigungen erhalte ich nur mit der App.

Selbst die fundamentale Funktion, Einsicht in die eigene Akte zu nehmen, setzt die Nutzung der App voraus. Als Frontend-Nichtnutzer weiß ich also nicht mal, welche Dokumente in meiner elektronische Patientenakte liegen. An der Stelle kann man sich fragen, ob Versicherte nicht einfach von ihrem Auskunftsrecht nach Datenschutz-Grundverordnung Gebrauch machen könnten. Die Krankenkassen können und dürfen die Verschlüsselung der Daten aber nicht aufbrechen – auch nicht im Rahmen einer Auskunft. Und diese Designentscheidung ist richtig. Diese starke Verschlüsselung befürworte ich. Sie soll auch zu Auskunftswecken nicht aufgeweicht werden.

Das heißt zusammengefasst, dass Nutzenden ohne Frontend, d.h. ohne Smartphone oder Tablet, bisher elementare Funktionen zur Wahrnehmung ihrer Kontrollrechte nach der Datenschutz-Grundverordnung nicht zur Verfügung stehen. Neben Menschen, die kein aktuelles Smartphone besitzen, gibt es auch Menschen, die mit gutem Recht ablehnen, ihre Gesundheitsdaten auf ihrem Smartphone zu verarbeiten.

Nun kann man einwerfen, dass das dann wohl nicht zusammenpasst: Vorteile der Digitalisierung nutzen und gleichzeitig Ablehnung der Smartphone-Nutzung für Gesundheitsdaten.

Tatsächlich gab es aber schon eine Lösung, die zumindest die gröbste Ungleichbehandlung hätte mindern können. Der Gesetzesentwurf sah eigentlich ein Frontend für spezielle gehärtete Tablets vor, das nahezu alle Funktionalitäten der elektronische Patientenakte-App geboten hätte. Dort hätten Versicherte – z.B. in den Geschäftsstellen der Krankenkassen – innerhalb einer gesicherten Umgebung Einblick in elektronische Patientenakte und Protokoll nehmen können. Übrigens wäre dort auch das dokumentengenaue Berechtigungsmanagement möglich gewesen.

Diese Lösung mithilfe von sogenannten „Terminals“ ist dann in letzter Minute aus dem Gesetzentwurf gestrichen worden. Stattdessen gibt es nun ab 2022 die Vertreterlösung, mit der ein Versicherter einen mit Smartphone ausgestatteten Vertreter mit der Frontend-Nutzung seiner elektronischen Patientenakte beauftragt. Das ist sicherlich für viele Situationen eine sinnvolle Lösung. Allerdings muss trotzdem jede und jeder die Möglichkeit haben, seine Rechte wahrzunehmen, ohne einem Dritten den vollen Zugang zu seiner elektronische Patientenakte zu geben. Im Übrigen hilft diese Lösung Personen, die keine Gesundheitsdaten auf privaten Endgeräten verarbeiten wollen, nicht.

3. Authentisierungsverfahren ohne elektronische Gesundheitskarte

Mein dritter Kritikpunkt ist die Umsetzung des alternativen Authentifizierungsverfahrens. Der Gesetzgeber wollte zusätzlich neben der elektronischen Gesundheitskarte ein anderes Authentisierungsmittel zulassen.

Schon mit dem Terminservice- und Versorgungsgesetz (TSVG) aus dem Mai 2019 wurde die rechtliche Grundlage für einen Zugang zur elektronischen Patientenakte ohne elektronische Gesundheitskarte geschaffen. Diese rechtliche Grundlage wurde mit dem Patientendaten-Schutz-Gesetz im Fünften Buch Sozialgesetzbuch konkretisiert.

Das Gesetz gibt als Voraussetzung für den Zugriff ohne Einsatz der elektronischen Gesundheitskarte an, dass sich der Versicherte „jeweils durch ein geeignetes technisches Verfahren, das einen hohen Sicherheitsstandard gewährleistet, authentifiziert hat“.

Ich habe diese Regelung als zu unspezifisch kritisiert. Der eigentliche Mangel liegt allerdings nicht im Gesetz, sondern in der konkreten Ausgestaltung des Verfahrens. Im Unterschied zu den zwei vorherigen Punkten ist dieser Missstand nicht unmittelbare Folge des Gesetzes-textes.

Die gematik beschreibt ein Verfahren, das sie „Alternative Versichertenidentität“ (kurz: Al.VI) nennt. Hier wird für die Versicherten eine zweite kryptografische Identität erzeugt. Diese existiert zusätzlich zur kryptografischen Identität auf der elektronischen Gesundheitskarte. Dieses Verfahren entspricht einer Fernsignatur, das kryptografische Identitätsmaterial wandert aus der Hardware des Nutzers zum entfernten Dienst. Dann fallen wichtige Sicherheitsleistungen, die sonst in der elektronischen Gesundheitskarte gekapselt sind, nun in die Verantwortung der Frontendhersteller.

Bereits im Mai 2019 nach der ersten Vorstellung des Verfahrens habe ich zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI) formuliert, dass dieses Verfahren nur für eine Übergangszeit geduldet werden kann. Das BSI hat Anforderungen entwickelt, die Identifizierungsverfahren für den Zugang zur Telematikinfrastruktur erfüllen müssen. Die gematik muss ein anderes Verfahren entwickeln, das allen diesen Anforderungen entspricht. Bis dahin müssen die Versicherten genau über die Unterschiede der Authentisierung mit elektronische Gesundheitskarte oder mit Al.VI informiert werden.

Zusammenfassung

Ich hoffe, ich konnte

- Ihnen die durch das Gesetz definierte Zwecke elektronische Patientenakte näher bringen

- und erklären, was meine drei großen Kritikpunkten an der elektronische Patientenakte sind:
  - Das Berechtigungsmanagement mit dem „Alles oder nichts Prinzip“,
  - Frontend-Nicht-Nutzer werden benachteiligt,
  - Die Umsetzung des alternativen Authentisierungsverfahrens muss verbessert werden.

Ich danke Ihnen für Ihre Aufmerksamkeit.