B

Grundrechte- und Datenschutz - Information und Erklärung zur „eingeschränkten Nutzung“ einer „elektronischen Patientenakte“ (ePA) mit zentraler Datenspeicherung

Das Recht auf Schutz Ihrer personenbezogenen Daten ist in Artikel 8 der EU-Grundrechtecharta festgeschrieben. Zu der „elektronischen Patientenakte“(ePA) mit einer zentralen Datenspeicherung und in Bezug auf Ihre persönlichen, sensiblen medizinischen Daten haben Datenschützer, Juristen sowie auch wir Ärztinnen und Ärzte der Familienpraxis Karlstein auf verschiedenen Ebenen erhebliche Sicherheitsbedenken.
Einige mögliche Risiken beim Anlegen einer elektronischen Patientenakte sind umseitig aufgeführt.

Einfacher und sicherer Weg: Keine ePA nutzen
Sie können dem Anlegen einer ePA bei Ihrer gesetzlichen Krankenkasse widersprechen - oder eine bereits angelegte ePA auch wieder löschen lassen. Danach müssen Sie sich nicht weiter um eine ePA kümmern.
Ein Nachteil darf Ihnen daraus nicht entstehen - das ist gesetzlich verankert.
Der Widerspruch gegen Ihre ePA ist aus Sicht der Ärztinnen und Ärzte der Familienpraxis Karlstein die einfachste und zuverlässigste Methode - und wir empfehlen Ihnen dies ausdrücklich.

Nach einem wirksamen Widerspruch ist das vorliegende „Formular B“ für Sie nicht erforderlich.
Bitte füllen Sie dann nur das in unserer Praxis erhältliche, sehr vereinfachte „Formular A“ aus.

Sollten Sie dennoch eine ePA führen wollen, können Sie mit der nachfolgenden Erklärung unsere Praxis davon ausschließen. Dann können wir Sie auch in Zukunft unkompliziert ohne ePA-Nutzung behandeln.
Vor Abgabe der Erklärung empfehlen wir Ihnen, sich über mögliche Rechtsfolgen beraten zu lassen. Dies kann z.B. durch einen sachkundigen Rechtsanwalt erfolgen.

Erklärung für

Name, Vorname: ……..…… Geb.Datum: ……..……..

Adresse: ……...……..

Krankenkasse: …… Versicherten-Nummer: ……..……..

Ich habe alle obenstehenden Hinweise und die umseitigen Informationen zu möglichen Risiken einer elektronischen Patientenakte (ePA) gelesen und verstanden. Ich gebe gegenüber der Familienpraxis in 63791 Karlstein, Dres. Zimmer-Miller-Bergmann-Überreiter, freiwillig die nachfolgende Erklärung ab. Eine Änderung meines diesbezüglichen Willens werde ich unverzüglich textlich mitteilen:

*„Hiermit **untersage ich**, dass alle Ärztinnen und Ärzte und/oder nichtärztliche Mitarbeiter-/innen der Familienpraxis Karlstein eine elektronische Patientenakte für meine Person anlegen, einsehen oder auf irgendeine andere Art und Weise nutzen oder bearbeiten. Dies gilt auch für den Fall, dass für mich eine elektronische Patientenakte angelegt wurde und auch dann, wenn diese von mir oder von Dritten an anderer Stelle genutzt wird. Ich haben zur Kenntnis genommen, dass eine angelegte ePA in meiner Verantwortung „patientengeführt“ werden muss. Ich habe dazu Informationen von meiner gesetzlichen Krankenkasse erhalten und gelesen.*
Ich versichere, dass ich alle Einstellungen in meiner elektronische Patientenakte so vornehme, dass die Familienpraxis Karlstein keine Zugriffsrechte erlangt. Ich werde dafür Sorge tragen, dass alle Dokumente und Unterlagen, die für meine Behandlung in der Familienpraxis Karlstein erforderlich oder zweckdienlich sind, dort so wie bislang auch ohne ePA-Einsichtnahme, z.B. als Papierausdruck oder als Telematik-Arztbrief, zeitgerecht zur Verfügung stehen.Ich übernehme die Haftung für alle materiellen und immateriellen Schäden, die der Familienpraxis Karlstein und/oder Dritten durch meine ePA entstehen. Meine Haftung gilt auch für ePA- bedingte Daten-Kompromittierungen sowie auch in Bezug auf Honorarregresse oder Sanktionen durch Kassenärztliche Vereinigungen und/oder Kostenträger gegen die Familienpraxis Karlstein bei fehlerhaften oder nicht dieser Erklärung gemäß konfigurierten ePA-Einstellungen.“

……..
Nur falls von oben abweichend: Name, Vorname und Adresse des gesetzlichen Vertreters oder der/des Sorgeberechtigten (Eltern)

Karlstein, den ……..
Datum

……..……
Unterschrift Patient/-in
bzw. des Fürsorgeberechtigten / gesetzl. Vertreters

B

Infos zu Risiken einer Elektronischen Patientenakte (ePA) mit zentraler Datenspeicherung (nicht abschließende Auflistung)

Risiko: Unsichere Anonymisierung und Pseudonymisierung
Ihre in der ePA zentral gespeicherten Gesundheits-Daten sollen vor einer Weiterverwendung zwar anonymisiert oder pseudonymisiert werden. Dies erscheint aber kaum vollständig und sicher machbar. Der Aufwand ist im Konzept der ePA nicht plausibel bedacht. Doch selbst dann, wenn eine Anonymisierung oder Pseudonymisierung mit großem Aufwand durchgeführt wird, besteht danach die Gefahr der „Zurückrechnung“. Dies bedeutet, dass durch die Kombination verschiedener „Daten-Merkmale“ (z.B. Alter - Geschlecht - Postleitzahl - Beruf) wieder Rückschlüsse auf einzelne Menschen gezogen werden können. Daten, die heute für fragwürdige „Forschungszwecke“ an Dritte abfließen, können so zu "digitalen Zeitbomben" mit unvorhersehbarem Schädigungspotential in der Zukunft werden.

Risiko: Hacker-Angriffe / Krimineller Datenmissbrauch
Die Daten der ePA liegen nicht bei den gesetzlichen Krankenkassen und auch nicht auf den elektronischen Gesundheitskarten, sondern zentral auf Servern in einem sogenannten „ePA-Aktensystem“. Diese Daten-Sammelstellen werden von der „Gematik GmbH“ betrieben, die in Zukunft zu einer staatsnahen „Digitalagentur“ umgebaut werden soll. Die Sammlung zentral gespeicherter, persönlicher Daten ist prädestiniert, die Aufmerksamkeit von kriminellen Hackern aus dem In- und Ausland auf sich zu ziehen. Es besteht die Gefahr, dass Kriminelle versuchen werden, sich Zugang zu den gespeicherten Daten zu verschaffen um dann damit Lösegelder oder andere Forderungen zu erpressen. Viele Hacker-Angriffe und Datenpannen im In- und Ausland zeigen, dass dies oft auch in gut geschützt geglaubten Umgebungen, z.B. im Gesundheitswesen, tatsächlich passiert. Weitere Gefahren ergeben sich an vielen Schnittstellen bei Dateneingabe und -nutzung, z.B. auf den Smartphones der Patienten.

Risiko: Datenschäden durch Schadsoftware
Dateien, die in die Zentraldaten-ePA einfließen, können aus verschiedensten Quellen stammen und haben zudem auch viele verschiedene Dateiformate. Es ist zu erwarten, dass nicht alle Datenquellen wie z.B. Smartwaches / „Wearables“ von kommerziellen Anbietern, stets die aktuellsten Sicherheitsstandards gewährleisten. Deshalb ist ein Einschleppen von Schadcode über ePA-Dateien grundsätzlich vorstellbar. Sich unbemerkt ausbreitender Schadcode kann neben Datenverlust zu massiven materiellen und immateriellen Sekundärschäden führen. Dagegen erscheinen die vorgesehenen Schutzkonzepte eher intransparent und wenig vertrauenerweckend.

Risiko: Datenmissbrauch durch "Innentäter"
„Innentäter“ sind beschäftigte Personen, die sich nicht an Regelungen und Vorgaben wie z.B. Datenschutzrichtlinien oder Informationssicherheitsvorgaben halten. Im deutschen Gesundheitswesen könnten ca. 2 Millionen im Gesundheitswesen Tätige eine Zugangsberechtigung zur ePA erhalten. Auch wenn der Patient diese „Zugänge“ theoretisch kontrollieren und steuern könnte: Dies wäre ein sehr zeitaufwändiges „Hobby“ - und für die meisten Patienten im Alltag auf Dauer nicht sicher leistbar. Letztlich sind Gesundheitsdaten vor Gelegenheits-Innentätern, die aus Neugier oder aus anderen Eigeninteressen unberechtigt Einsicht in ePA´s nehmen, kaum zuverlässig zu schützen.

Risiko: Nutzungseinschränkungen und Exklusion
Eine Zentraldaten-ePA ist abhängig von stabilen, technischen Infrastrukturen. Systemausfälle, technische Fehler oder eine langsame Internetverbindung können den Zugang unmöglich machen oder erschweren. Menschen ohne Smartphone, Tablet oder Computer müssen mit starken Einschränkungen leben und können die ePA im Regelfall nur „passiv nutzen“. Ein eigenständiges Einsehen, Hochladen oder Verwalten von Daten wäre nicht ohne weiteres möglich und Widersprüche müssten aufwändig über sogenannte „Ombudsstellen“ der verschiedenen Krankenkassen erklärt werden. Zudem sind nicht alle Patienten und Patientinnen hinreichend technisch versiert. Sie können bei ePA-Nutzung und bei der Einhaltung von Sicherheitsstandards auf große Schwierigkeiten stoßen. Die Risiken lägen dann beim Patienten, der verantwortlich für die „Führung der ePA“ ist.

Risiko: Forschungsziele kommerziell statt am Gemeinwohl orientiert
Nach zentraler Speicherung sollen Befunde und Daten dann in Zukunft nicht nur für Ihre medizinische Behandlung, sondern in großem Umfang auch für verschiedene „Forschungszwecke“ im In- und Ausland genutzt werden. Nutzer könnten dann auch Pharmafirmen, große Konzerne und Digitalfirmen werden, die damit z.B. auch "künstliche Intelligenz"-Modelle anlernen. Ob die Ergebnisse später jemals den versprochenen medizinisch-wissenschaftlichen Nutzen für die Patientenversorgung und für das Gesundheitswesen haben, ist offen. Es steht aber zu befürchten, dass neue Kontroll- und Kostensparmodelle etabliert und vor allem die Interessen von Digital- und Pharmafirmen, Kostenträgern und Versicherungen gestützt würden.

Risiko: Zugriff von Behörden, Vorratsdaten und politischer Wandel
Zentral gespeicherte Gesundheitsdaten können als „Vorratsdatenspeicherung“ betrachtet werden. Ohne schützende politische und rechtliche Rahmenbedingungen könnten diese sehr tiefen und umfassenden Daten in Zukunft zu verschiedenen Kontroll-, Überwachungs- oder Fahndungszwecken herangezogen werden. Es kann nicht ausgeschlossen werden, dass Strafverfolgungsbehörden in Zukunft gezielte Zugriffe auf elektronische Patientenakten begehren, inclusive aller darin dokumentierten Gesundheits- und Behandlungsdaten. In Zeiten von Gefahrenlagen wie Pandemien oder nach politischen Umbrüchen wären auch noch viel weiterreichende Szenarien denkbar: Mit dem Argument einer „Gefahrenabwehr“ könnten breit angelegte Zugriffe auf die Gesundheitsdaten der Bürger legalisiert werden, um z.B. Rasterfahndungen oder Infektionsschutzmaßnahmen durchzuführen.

Risiko: Patientenversorgung wird beeinträchtig
Die Gesundheitsversorgung in Deutschland ist zurzeit in vielen Bereichen am Limit. Das massenhafte Anlegen, Befüllen und Pflegen von ePA‘ s verursacht einen sehr großen Verwaltungs- und Arbeitsaufwand, der zu großen Teilen von medizinischem Fachpersonal geleistet werden soll. Für die Datenverarbeitung ist dabei große Sorgfalt gefragt, denn jeder Dokumentenupload führt zu Sicherheits- und Haftungsrisiken. Durch diese zusätzlichen Belastungen kann sich die medizinische Versorgung sogar verschlechtert. Wartezeiten auf Arzttermine könnten noch länger als bisher werden.

Risiko: Beeinträchtigung der informationellen Selbstbestimmung für Kinder und für betreute Personen
Ein sorgfältiger und gewissenhafter Umgang mit den digitalen Daten von Kindern und betreuten Personen ist sehr wichtig. Wir bauen heute das ethische, gesellschaftliche und rechtliche Fundament für die digitale Welt, in der diese in Zukunft leben müssen. Jede Nutzung der digitalen Daten dieser besonders schützenswerten Personengruppe durch Dritte muss daher sorgfältig abgewogen werden. Dies gilt ganz besonders für sensible Gesundheitsdaten. Kinder sollten später die Freiheit haben, selbstbestimmt zu entscheiden, was mit ihren Daten geschieht und wer diese nutzen darf. Kinder dürfen erst ab einem Alter von 15 Jahren ihre Selbstbestimmungsrechte in Bezug auf ihre Gesundheitsdaten wahrnehmen. Wenn Eltern nicht zuvor für sie im "Opt-Out"-Verfahren widersprechen, werden ePA´s auch für gesetzlich krankenversicherte minderjährige Kinder angelegt. Bis zur Möglichkeit einer eigenen Entscheidung würden dann viele Daten zentral gespeichert und von Dritten genutzt – und damit den beschriebenen Risiken ausgesetzt. Im Falle eines Datenmissbrauchs könnten dann später im Erwachsenalter gravierenden Nachteile entstehen, z. B. bei dem Versuch, eine Lebens- oder Berufsunfähigkeitsversicherung abzuschließen.