Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

DR. SÖREN DEISTER

# DIE ELEKTRONISCHE PATIENTENAKTE – INNOVATION ODER GESETZGEBERISCHE FEHLKONSTRUKTION?

# „Modethema“ Digitalisierung?

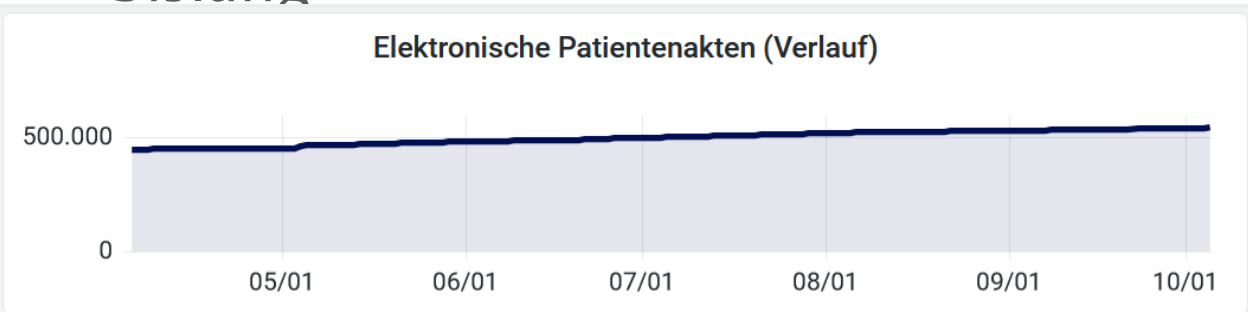
Ja, aber:

- Tatsächlich tiefgreifender Transformationsprozess hinsichtlich Produktivität, Wertschöpfung und Konzentration von ökonomischer und gesellschaftlicher Macht, auf den das Recht reagieren muss
  (vgl. Hoffmann-Riem, Recht im Sog der digitalen Transformation, 2022)
- Spezifisch für das Gesundheitswesen: „Daten teilen heißt besser heilen“ → großes Potential für bessere Versorgung
  (SVR-Gutachten 2021)
- Spezifisch für die elektronische Patientenakte (ePA):

- Bessere Behandlung v. Patient*innen durch bessere Information
- Vermeidung von Doppeluntersuchungen
- Kostensenkung

# Umsetzungsstand

- Seit 1.1.2021 besteht Anspruch der GKV-Versicherten auf Zurverfügungstellung einer ePA gegen ihre Krankenkasse
- Weniger als 1 Prozent der GKV-Versicherten nutzen diese bislang





- 52 Prozent der GKV-Versicherten geben an, nicht über Existenz der ePA durch Krankenkasse informiert worden zu sein
- 76 Prozent geben an, ePA grundsätzlich nutzen zu wollen

(jeweils Bitkom-Umfrage, Nov. 2021)

# Gegenstand des Vortrags

I. Das Regelungssystem im Überblick
II. Die datenschutzrechtlichen Streitpunkte
III. Defizite in der Umsetzung
IV. Lösungsvorschläge

Einschränkung:

Keine Expertise zu Datensicherheit, kein Schwerpunkt auf Datenschutzrecht

# I. Das Regelungssystem im Überblick

# Was die ePA (aktuell) nicht ist...

- ...Ersatz für lokale Behandlungsdokumentation der Leistungserbringer
- ...Kommunikationskanal zwischen Leistungserbringern

**Sondern:**

- Letztlich funktionell identisch mit einer Sammlung von Behandlungsdaten durch die Versicherten selbst in einer dafür eingerichteten Cloud
- Einstellbare Daten sind benannt in § 341 Abs. 2 SGB V, im Wesentlichen Behandlungsdaten der Leistungserbringer („Fach 1“) und eigene Daten der Versicherten („Fach 2“) mit stufenweisem Ausbau

# Charakteristika der gegenwärtigen ePA

- **Freiwillig**: Wird auf Antrag der Versicherten zur Verfügung gestellt („opt-in-Modell“) und von Krankenkasse eingerichtet
- **Einwilligungsbasiert**: Jeder Zugriff bedarf Einwilligung durch die Versicherten bezüglich der konkreten Person/Institution, die zugreifen soll
- **Versichertengeführt**: Die Steuerung (Verwaltung) der ePA erfolgt durch die Versicherten selbst

# Nutzungsrechte der Versicherten

1) Auslesen, Übermitteln, Löschen und z.T. auch Verarbeiten im Sinne des Änderns von Daten in der ePA, § 337 Abs. 1, Abs. 2 SGB V
2) Erteilung von Zugriffsberechtigungen für Leistungserbringer §§ 337, 339, 352, 353 SGB V
3) Einstellen bzw. Einstellen lassen von Daten in die ePA, §§ 346-348 SGB V
4) Einsichtnahme in Protokolldaten über Zugriffe, 309 SGB V
5) Anlasslose Löschung der gesamten ePA, § 344 Abs. 3 SGB V

# Technische Steuerung (Verwaltung)

**Drei Wege:**

1) Über App auf Smartphone/Tablet („Frontend-User“)
2) Seit 1.1.2022 auch als Desktop-Version
3) Bei den Leistungserbringern mittels eGK und PIN-Eingabe

**Einstellung von Daten**:

Im Wesentlichen durch Leistungserbringer (Ärzt*innen) als Kopie aus dem PVS mit **Einwilligung** und **auf Verlangen der Versicherten**; z.T. auch durch Versicherte selbst (2-Fächer-Prinzip); beschränkt auf „aktuellen Behandlungskontext“

# Konkret: Das technische Zugriffsmanagement

**1) Bei Nutzung über App/Desktopversion („Frontend-User“)**

- **Umsetzungsstufe 1** ab 1.1.2021: „grobgranulares Zugriffsmanagement“ (§ 342 Abs. 2 Nr. 1 SGB V) → beschränkbar auf alle Daten der Behandler oder alle selbst eingestellten Daten oder alle Daten
- **Umsetzungsstufe 2** ab 1.1.2022: „feingranulares Zugriffsmanagement“ → jedes einzelne Dokument kann frei gegeben/gesperrt werden

**2) Ohne App/Desktopversion:**

- **Umsetzungsstufe 1:** wie oben beim Leistungserbringer via eGK
- **Umsetzungsstufe 2:** „Mittelgranulares Zugriffsmanagement“ = Zugriffsberechtigung auf „Kategorien von Dokumenten“ beschränkbar
- Im Übrigen **Vertretung** möglich, § 342 Abs. 2 Nr. 2 lit. b), lit. e)

# Wer darf in welchem Umfang zugreifen?

- Voraussetzung ist stets Einwilligung mittels „eindeutiger bestätigender Handlung durch technische Zugriffsfreigabe“ (§ 353 SGB V)
- Umfang des erlaubten Zugriffs ferner durch § 352 SGB V gesetzlich beschränkt
- Jeder Zugriff setzt ferner Authentifizierung voraus mittels elektronischen Heilberufsausweis (eHBA) sowie Security Module Card Typ B (SMC-B = „Praxisausweis“) als Komponente zur Authentifizierung von Leistungserbringerinstitutionen (§ 339 Abs. 3, 4, 5 SGB V)

# Wer darf in welchem Umfang zugreifen?

| Gruppe der Zugriffsberechtigten | Gesetzliche Vorgaben („Verarbeitungstatbestände“) |
|---|---|
| **Stufe 1**: Ärzt*innen, Psychotherapeut*innen, „Hilfspersonal“ | Umfassendes Verarbeitungsrecht, sofern „**für die Versorgung erforderlich**“ (§ 352 Nr. 1-4, 7, 8 SGB V) |
| **Stufe 2:** Nichtärztliche Leistungserbringer (Apotheker, Pflegepersonal, Hebammen, Heilmittelerbringer) | Auslesen, Speichern und Verwenden fast aller Daten; **Verarbeitung nur spezifischer Daten**, jeweils „soweit für die Versorgung erforderlich“ (§ 352 Nr. 5, 6, 9-15 SGB V) |
| **Stufe 3:** Öffentlicher Gesundheitsdienst, Betriebsärzt*innen | **Versorgungsunabhängig**; ÖGD: Umfassendes Verarbeitungsrecht, sofern erforderlich für Aufgabenerfüllung; Betriebsärzte: unbeschränktes „Auslesen, Verwenden, Speichern“ und Verarbeiten von Impfdaten (§ 352 Nr. 16-18 SGB V) |
| **Stufe 4:** Krankenkassen, Heilpraktiker*innen | Kein Zugriff möglich, Ausnahme für KKen nach § 345 SGB V. |

# Die ePA im Kontext der Telematikinfrastruktur

- TI = „Datenautobahn des Gesundheitswesen“ = „Informations-Kommunikations- und Sicherheitsinfrastruktur“ (§ 306 Abs. 1 SGB V)
- Schaffung, Aufbau und Zulassung von einzelnen Diensten obliegt der gematik GmbH (§ 310 SGB V)
- TI besteht aus zentraler Infrastruktur, insbes. gesichertem Netz (§ 306 Abs. 2 Nr. 1 SGB V), dezentraler Infrastruktur, insb. Komponenten zur Authentifizierung (§ 306 Abs. 2 Nr. 1 SGB V, z.B. eGK) sowie Anwendungsinfrastruktur (§ 306 Abs. 2 Nr. 3 SGB V z.B. ePA Dienste)
- Das gesicherte (zentrale) Netz wird im Wege einer von der gematik vergebenen öffentlichen Auftrags durch Arvato (Bertelsmann) betrieben (vgl. § 307 Abs. 3 S. 1, 323 Abs. 2 SGB V)
- Komponenten/Dienste, die von Anbietern betrieben und entwickelt werden, lässt die gematik durch Verwaltungsakt nach § 325 SGB V zu; Sicherheitszertifizierung nach § 325 Abs. 3 SGB V durch BSI

# Rechte und Pflichten im Überblick

## I. Versicherte

- Beantragen ePA und registrieren sich
- Verwalten („führen“) die ePA
- Erteilen Zugriffsberechtigungen für Leistungserbringer

## II. Krankenkassen

- Müssen ePA einrichten und Nutzung ggf. unter Einbeziehung (priv.) Unternehmen ermöglichen
- Müssen Versicherte umfassend informieren (§ 343 SGB V)
- Sind datenschutzrechtlich verantwortlich (§ 341 Abs. 4 SGB V)
- Dürfen nicht auf Daten zugreifen (Ausnahme: § 345 SGB V)
- Finanzieren ePA und gematik insgesamt (ganz überwiegend)

# Rechte und Pflichten im Überblick

## III. Leistungserbringer (insbes. Ärzt*innen)

- Dürfen (müssen?) nach Einwilligung zugreifen/bearbeiten, soweit erforderlich (§ 352 SGB V)
- Befüllen „auf Verlangen“ epA mit Daten aus „aktuellem Behandlungskontext“ und unterstützen „bei erstmaliger Befüllung“; Erstbefüllung wird gesondert vergütet (§§ 346-348 SGB V)
- Haben keine darüber hinausgehenden (sozialrechtlichen) Informationspflichten

## IV. gematik

- Vergibt öffentliche Aufträge, z.B. zum Betrieb des zentralen TI-Netzes
- Lässt Komponenten/Dienste (priv. Anbieter) nach Prüfung durch VA zu

# II. Die datenschutzrechtlichen Streitpunkte

# Die datenschutzrechtlichen Streitpunkte

- Datenschutzrechtlich verantwortlich für Verarbeitung der Daten zum Zwecke der ePA-Nutzung sind die Krankenkassen als Anbieter der ePA., § 341 Abs. 4, § 307 Abs. 4 SGB V
  Kritisch dazu J. Eichenhofer, NVwZ, 2021, 1090, 1092
- BfDI übt datenschutzrechtliche Aufsicht über bundesunmittelbare Krankenkassen aus, § 9 Abs. 1, Abs. 2 BDSG, § 90 SGB IV
- Erließ zunächst Warnung nach Art. 58 Abs. 2a DSGVO und schließlich im August 2021 einen anweisenden VA nach Art. 58 Abs. 2d DSGVO
- Bundesamt für Soziale Sicherheit teilt Auffassung nicht und empfiehlt Krankenkassen Klage gegen Anweisung, dies ist auch geschehen,§ 81a SGB X

# Inhaltliche Kritikpunkte des BfDI

**1. Feingranulare Dokumentenfreigabe nicht für alle ePA-Nutzer möglich**

- Bis 1.1.2022 nur „Alles-oder-Nichts-Prinzip“ bezogen auf ein Fach: Entweder alle Daten der Leistungserbringer für Berechtige sichtbar oder keine
- Seit 1.1.2022 auch dokumentenspezifisch; für „nicht-Frontend-User“ aber nur kategorienspezifisch

**2. Eingeschränkte Nutzungsmöglichkeit für nicht-Frontend-Nutzer**

- Insbesondere keine Möglichkeit, ePA-Daten/erteilte Berechtigungen/Zugriffe einzusehen
- Vertretung nur unter Offenlegung aller Daten an Vertretungsperson möglich

**3. Zugriffsverfahren der „alternativen Versichertenidentität“ nicht hinreichend sicher**

# Inhaltliche Kritikpunkte des BfDI

- Dies soll gegen Art. 25 DSGVO **„Datenschutz durch Technikgestaltung/Voreinstellung“** i.V.m. u.a. Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO verstoßen
- Kern der Argumentation: Es werden mehr Daten geteilt, als für den Behandlungszweck erforderlich sind und auch mehr als nach gesetzlichem Tatbestand verarbeitet werden dürfen; Einwilligung wird durch „alles oder nichts“ prekär (vgl. auch Bieresborn, jM 22, 113,119)
- Andererseits: umfassend informierte Einwilligung sowie gesetzliche Begrenzung der Zugriffsmöglichkeiten; Ausdifferenzierteste Lösung ist nicht immer die datenschutzrechtlich vorzugswürdige; Ungleichbehandlung aufgrund technischen Aufwands gerechtfertigt

# III. Defizite der bisherigen Umsetzung

# 1. Defizite im Rahmen der Einführung

- Datenschutzrechtliche Diskussion und Verunsicherung hätten durch Abwarten auf „feingranulare Steuerung“ vermieden werden können
- Einführung vor Schaffung eines umsetzbaren Angebots für nicht-Frontend-Nutzer
- Gesetzlich Vorgaben ebenfalls z.T. grob defizitär bis an Grenze der Auslegbarkeit (z.B. Sanktionsverfahren nach § 342 Abs. 5 SGB V), häufig redundant und unsystematisch
- Keine systematische Erprobungsphase unter Einbindung Akteure

# 2. Mangelnde Akzeptanz/Umsetzung in Selbstverwaltung

- Für Vertragsärzt*innen bedeutet ePA zunächst:
- Technischen Mehraufwand
- Mehraufwand für Befüllung, ggf. Unterstützung bei Verwaltung der ePA
- Potentielle Kontrolle durch Kolleg*innen
- Angst vor Haftungsrisiken

→ Mangelnde Akzeptanz, schleppende Umsetzung (40-60 %)

# 2. Mangelnde Akzeptanz/Umsetzung in Selbstverwaltung

- Krankenkassen kommen ihrer Informationspflicht (§ 343 SGB V) wohl eher widerwillig nach → mangelnde Kenntnis der Versicherten
- Keine wirksamen Mechanismen zur Durchsetzung der jeweiligen Pflichten

So sei es irrführend Deutschland mit skandinavischen Ländern wie Schweden oder Finnland zu vergleichen und sich diese als Vorbilder bei der Digitalisierung des Gesundheitswesens zu nehmen. Schließlich hätten Finnland und Schweden staatliche Systeme mit einer einzigen Krankenkasse und ohne freie Arztwahl. „Das macht es bedeutend einfacher, solche Gesundheitssysteme zu digitalisieren."

*Melanie Wendling*, Geschäftsführerin des Bundesverbands Gesundheits-IT (bvitg)

# 3. Technische Fehler und Defizite

- Gehäufte technische Ausfälle bei TI-Nutzung (z.B. Konnektoren)
  (vgl. Borchers, c´t 5/22, 14; Maus, c´t 4/22, 44)
- Anwendungsprobleme durch Vielzahl „mögliche[r] Kombinationen zwischen Betreibern, Karten, Konnektoren, Kartenterminals, Diensten“
  (vgl. Langguth, e-health.com, 26.1.22)
- Technisch umstrittener Austausch von Konnektoren für 300 Millionen Euro (vgl. Schönberg/Maus, c´t v. 15.7.22)

# 4. Schädliches Marktverhalten von Anbietern/Herstellern

- Anbieter und Hersteller versuchen ihre System „geschlossen“ zu halten, sog. „lock-in-Effekt“
- Das bedeutet: Primärsystemanbieter von Praxisverwaltungssystemen verhindern Nutzbarkeit mit Komponenten anderer Anbieter oder verlangen zusätzliche Gebühren
- Diesbezüglich neue Regelung in § 332a SGB V in Pflegeentlastungsgesetz geplant, die Anbieter von Primärsystemen zur kostenfreie Einbindung aller von der gematik zugelassenen Komponenten und Dienste verpflichtet
- Wechsel von Primärsystem zum Teil erschwert durch Verträge → Einführung von Kollektivverhandlungen durch KBV in § 332b SGB V geplant

# 5. Hoher Aufwand der Nutzung für Versicherte

- Registrierungs- und Anmeldeprozess recht kompliziert und zeitaufwändig (Registrierung bei KK und Ident-Nachweis via Postident, Krankenkassenfiliale oder zukünftig Apotheke; auch über NFC-fähige eGK und PIN möglich), § 336 Abs. 6 SGB V
- Setzt Mindestmaß an Ausdauer und Technikaffinität voraus, aber letztlich nicht viel aufwändiger als Freischalten und Nutzen von Online-Banking
- Nutzen dieses zeitlichen Aufwands zunächst nicht unmittelbar ersichtlich
- Auch Apps selbst laut Stiftung Warentest (10/22) fehleranfällig und unübersichtlich

# 6. Abschreckung durch versorgungsfremde Berechtigungen

- Potentielle Auswirkungen auf Arbeitsverhältnis/Beamtenverhältnis und Verwendung für Aufgaben der Gefahrenabwehr nicht konsequent ausgeschlossen
- Beschlagnahmeschutz von in die ePA übertragenen Daten möglicherweise unzureichend → Daten befinden sich nicht in Gewahrsam einer nach § 97 StPO zeugnisverweigerungsberechtigten Person
  (strittig, siehe Dochow, MedR 2021, 13, 20; Solscheid, MedR 2021, 795 ff.)
- Dies begründet potentielle Vertrauensdefizite
- Außendarstellung z.T. irreführend, z.B. „entscheidend [für Zugriff] ist, dass diese Personen in die Behandlung der Versicherten eingebunden sind“ (gematik in SozSich 22, 96).

# Jedenfalls...

... ist die These, „die epA scheitert am strengen Datenschutz“ unterkomplex

...ist dennoch „Richtungsentscheidung“ wieviel Datensammlung für Versorgungsverbesserung hinzunehmen ist, nowendig

# IV. Lösungsvorschläge

# Systematisierung

**1) Versorgungssystembezogene Defizite**

→ Schwer reformierbar, „langer Atem“; dennoch notwendig

**2) TI-bezogene Defizite**

- Vielzahl an Anbietern/Komponenten vereinheitlichen
- Gematik weiter verstaatlichen, ggf. aus SGB V ganz herauslösen → Umwandlung gematik in staatsunmittelbare, steuerfinanzierte Bundesbehörde?

3) **Nutzungsbezogene Defizite**

- Kombination mit unmittelbar nützlichen Tools wie Terminbuchung etc.
- Registrierungsprozess beschleunigen

# Systematisierung

## 4) Potentielle Vertrauensdefizite/Missbrauchsrisiken

- Strenge Begrenzung auf versorgungsbezogene Nutzung
- Beschlagnahmeschutz klarstellen
- Gleichberechtigte Nutzungsmöglichkeit für nicht-Frontend-User schaffen
- Ggf. Psychotherapie heraus nehmen

## 5) Akzeptanzdefizite der Leistungserbringer

- Nachfrageorientiert umgestalten?
- ?

# Generallösung: „Opt-Out-Modell“?

- Im Koalitionsvertrag angekündigt
- ePA wird automatisch angelegt, Anlage kann widersprochen werden → Jedenfalls (P) der geringen Nutzungszahlen wohl behoben
- In anderen europäischen Ländern (Österreich, Spanien, Estland) bereits umgesetzt, wird grds. für DSGVO-konform gehalten (vgl. Gutachten Krönke/Aichstill, 2021, strittig)
- Rechtfertigung über einwilligungsunabhängige gesetzliche Verarbeitungstatbestände, insb. Art. 9 Abs. 2 lit. g, h DSGVO (Belange der öffentlichen/individuellen Gesundheit) möglich
- Varianten mit automatischer Befüllung und „Verschattungsmöglichkeit“ oder versichertengeführter Befüllung (wie aktuell) denkbar
- Versorgungspolitisch sinnvoll; einfache/transparente Steuerungsmöglichkeit für Ausblenden/Verschatten erforderlich
- Löst allerdings nur einen Teil der genannten Probleme, insbes. bei Beibehaltung versichertengeführter Akte

# Fazit

Innovation und gesetzgeberische Fehlkonstruktion (+)

Vielen Dank für die Aufmerksamkeit –
soeren.deister@uni-hamburg.de