Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung[1]

Landesbeirat für
Menschen mit Behinderungen

SenASGIVA, Oranienstraße 106, 10969 Berlin

Versand per E-Mail

Geschäftszeichen LfB LB
Geschäftsstelle des Landesbeirats
Zimmer: E.009
Tel. +49 30 9028 2838
E-Mail: LfB-Beirat@senasgiva.berlin.de
Oranienstr. 106, 10969 Berlin
Datum 27. Mai 2026

Stellungnahme zum Referentenentwurf eines Gesetzes für Daten und digitale Innovation im Gesundheitswesen – GeDIG

Sehr geehrte Damen und Herren,

Aus dem „Gesetz für Daten und digitale Innovation im Gesundheitswesen“ muss ein „Gesetz für Datenschutz und digitale Innovation im Gesundheitswesen“ werden.

Schwerpunkt: Datenschutz, Privatsphäre und Schutz vulnerabler Gruppen, insbesondere behinderter und psychisch kranker Menschen.

1. Vorbemerkung

Der Referentenentwurf eines Gesetzes für Daten und digitale Innovation im Gesundheitswesen verfolgt das Ziel, digitale Anwendungen, die elektronische Patientenakte, die Sekundärnutzung von Gesundheitsdaten, datenbasierte Versorgungsprozesse und die europäische Anschlussfähigkeit des deutschen Gesundheitswesens weiterzuentwickeln.

Diese Zielsetzung ist grundsätzlich nachvollziehbar. Digitale Innovation kann Versorgung verbessern, Behandlungsprozesse erleichtern, Patientensicherheit erhöhen, Forschung ermöglichen und Versorgungslücken sichtbar machen. Gerade Menschen mit chronischen Erkrankungen, Behinderungen, psychischen Erkrankungen, Pflegebedarf oder komplexen Behandlungsverläufen können von gut gestalteten digitalen Strukturen profitieren.

Der vorliegende Entwurf greift jedoch zu kurz. Er versteht digitale Innovation vor allem als Ausweitung der Nutzung, Verfügbarkeit und Verknüpfung von Gesundheitsdaten. Was fehlt, ist eine gleichrangige Stärkung des Datenschutzes, der informationellen Selbstbestimmung, der Vertraulichkeit und der praktischen Kontrollmöglichkeiten der Patientinnen und Patienten.

Das GeDIG darf nicht nur ein Gesetz zur erweiterten Datennutzung werden. Es muss zugleich die bestehenden Datenschutzprobleme der elektronischen Patientenakte beheben. Die ePA ist bereits heute mit erheblichen Schutzdefiziten verbunden: zu pauschale Zugriffsrechte, unzureichende feingranulare Steuerung, mangelnde digitale Teilhabe, unklare Schutzmechanismen für besonders sensible Daten, unzureichender Schutz vor Zweckverschiebung und erhebliche praktische Hürden bei Widerspruch, Kontrolle und Korrektur.

Deshalb muss die Zielrichtung des Gesetzes korrigiert werden:

Aus dem „Gesetz für Daten und digitale Innovation im Gesundheitswesen" muss ein „Gesetz für Datenschutz und digitale Innovation im Gesundheitswesen" werden.

Digitale Innovation im Gesundheitswesen ist nur dann akzeptabel, wenn sie Vertrauen stärkt, nicht schwächt. Sie muss Datenschutz nicht als Hindernis, sondern als Voraussetzung guter Versorgung begreifen.

2. Zusammenfassende Bewertung

Der Entwurf enthält wichtige Ansätze für bessere digitale Versorgung. Gleichzeitig verschiebt er das Verhältnis zwischen Datennutzung und Datenschutz deutlich zulasten der Patientinnen und Patienten.

Besonders kritisch sind die geplante erweiterte Nutzung von ePA-Daten durch Kranken- und Pflegekassen, die Möglichkeit zusätzlicher Datenerhebung durch Krankenkassen bei Versicherten und anderen Stellen, Reallabore der Krankenkassen zur Erprobung innovativer Datenverarbeitung, die Einführung einer Forschungskennziffer zur Verknüpfung von Gesundheitsdaten, die Ausweitung digitaler Bedarfseinschätzung und digitaler Versorgungspfade sowie die weiterhin unzureichende feingranulare Steuerung der ePA.

Der Entwurf erkennt besondere Patientengruppen zwar punktuell an. Er zieht daraus aber nicht die notwendigen Konsequenzen. Menschen mit Behinderungen, psychischen Erkrankungen, Suchterkrankungen, Traumafolgen, Pflegebedarf, kognitiven Einschränkungen oder seltenen Erkrankungen benötigen nicht nur Zugang zu digitalen Angeboten. Sie

benötigen besonderen Schutz vor Stigmatisierung, Fehlinterpretation, Profilbildung, Benachteiligung und faktischem Einwilligungsdruck.

Gesundheitsdaten sind keine bloße Ressource für Innovation. Sie sind Ausdruck persönlicher Lebensgeschichte, Verletzlichkeit, Krankheit, Krise, sozialer Lage und Hilfebedürftigkeit. Ihre Nutzung muss deshalb streng begrenzt, verständlich kontrollierbar und wirksam geschützt sein.

3. Datenschutz als Voraussetzung digitaler Innovation

Der Entwurf stellt Datennutzung, Forschung, Interoperabilität und digitale Versorgungssteuerung in den Vordergrund. Datenschutz erscheint dagegen überwiegend als nachgelagerte Absicherung. Diese Gewichtung ist falsch.

Gerade im Gesundheitswesen gilt: Ohne Vertrauen keine gute Versorgung. Wenn Patientinnen und Patienten befürchten müssen, dass sensible Angaben aus Arztgesprächen, Psychotherapie, Psychiatrie, Pflege, Reha oder Krisensituationen in andere Kontexte wandern, werden sie Informationen zurückhalten oder Versorgung meiden.

Das betrifft psychisch kranke Menschen in besonderer Weise. Angaben über Suizidgedanken, Psychosen, Sucht, Traumatisierung, Selbstverletzung, Zwangsmaßnahmen, Gewalt, familiäre Konflikte oder Psychopharmaka gehören zu den sensibelsten Gesundheitsdaten überhaupt. Werden solche Daten zu breit verfügbar oder zu schwer kontrollierbar, gefährdet dies nicht nur die Privatsphäre, sondern auch die Behandlung selbst.

Datenschutz ist daher kein Gegensatz zu Versorgung. Datenschutz ist Versorgungsschutz.

Ein modernes Digitalgesetz für das Gesundheitswesen muss deshalb drei Ziele gleichrangig verfolgen: bessere digitale Versorgung, sinnvolle und gemeinwohlorientierte Forschung sowie wirksamen Schutz der Vertraulichkeit, Selbstbestimmung und Privatheit. Der Entwurf erfüllt den dritten Punkt bislang nicht ausreichend.

4. Bestehende Datenschutzprobleme der ePA müssen behoben werden

Die ePA wird im Entwurf weiter ausgebaut und stärker in Versorgungs-, Forschungs- und Steuerungsprozesse eingebunden. Das wäre nur vertretbar, wenn zugleich die bestehenden Schutzdefizite der ePA konsequent behoben würden. Genau dies geschieht bislang nicht ausreichend.

Das zentrale Problem sind zu pauschale Zugriffsrechte. Die ePA darf nicht nach dem Prinzip „alles oder nichts“ funktionieren. Patientinnen und Patienten müssen selbst bestimmen können, welche Leistungserbringer welche Informationen sehen dürfen. Besonders problematisch sind pauschale Zugriffe ganzer Einrichtungen oder Berufsgruppen. Wer einer Praxis, Klinik, Apotheke oder sonstigen Stelle Zugriff gewährt, darf nicht automatisch riskieren, dass auch für die konkrete Behandlung irrelevante, aber hochsensible Daten sichtbar werden.

Erforderlich ist ein einfaches, barrierefreies und wirklich feingranulares Berechtigungsmanagement. Versicherte müssen sensible Informationen gezielt schützen können, insbesondere psychiatrische und psychotherapeutische Daten, Suchterkrankungen, HIV-Daten, genetische Informationen, reproduktionsmedizinische Daten, Gewalterfahrungen, Behinderungsdaten und seltene Erkrankungen.

Besonders deutlich wird das Problem bei Medikationsdaten. Medikamente können Diagnosen offenbaren. Antipsychotika, Antidepressiva, Substitutionsmittel, HIV-Medikamente, Hormontherapien oder Medikamente bei Suchterkrankungen können stigmatisierende Rückschlüsse ermöglichen. Es reicht deshalb nicht aus, nur ganze Medikationslisten verbergen zu können. Patientinnen und Patienten müssen einzelne Medikamente gezielt ausblenden können, wenn diese für die konkrete Behandlung nicht erforderlich sind.

Psychotherapeutische und psychiatrische Daten benötigen eine besondere Schutzstufe. Sie enthalten häufig Angaben, die weit über medizinische Fakten hinausgehen: familiäre Beziehungen, Gewalterfahrungen, biografische Belastungen, Sexualität, Sucht, Selbstgefährdung, Arbeitskonflikte, soziale Ängste, Traumata oder intime Lebensentscheidungen. Diese Daten dürfen nicht wie gewöhnliche Gesundheitsinformationen behandelt werden.

Die ePA muss außerdem mindestens so gut geschützt sein wie klassische Patientenakten. Wegen ihrer zentralen, strukturierten und leichter durchsuchbaren Form braucht sie sogar einen besonders klaren rechtlichen Schutz. Es muss ausdrücklich geregelt werden, dass ePA-Daten nicht ohne Weiteres für Ermittlungs-, Sicherheits-, Strafverfolgungs-, Ausländer-, Sozial- oder andere behördliche Zwecke genutzt oder beschlagnahmt werden dürfen.

Schließlich müssen Patientinnen und Patienten jederzeit verständlich nachvollziehen können, wer auf ihre ePA zugegriffen hat, wann der Zugriff erfolgt ist, auf welche Daten zugegriffen wurde und zu welchem Zweck. Protokolle dürfen nicht nur technisch vorhanden sein, sondern müssen laienverständlich, barrierefrei und vollständig nutzbar sein.

5. Erweiterte Datennutzung durch Krankenkassen ist besonders kritisch

Einer der schwerwiegendsten Punkte des Entwurfs ist die geplante Ausweitung der Datennutzung durch Kranken- und Pflegekassen. Krankenkassen sollen künftig ePA-Daten und zusätzliche personenbezogene Daten für datengestützte Auswertungen, Hinweise und Versorgungsangebote nutzen können. Außerdem sollen sie zusätzliche Daten bei Versicherten oder bei anderen Stellen erheben können.

Dies ist datenschutzrechtlich und versorgungspolitisch hoch problematisch. Krankenkassen sind Kostenträger. Sie entscheiden über Leistungen, prüfen Ansprüche, finanzieren Versorgung und haben zugleich wirtschaftliche Interessen. Sie stehen nicht in einem heilberuflichen Vertrauensverhältnis zu Patientinnen und Patienten. Daten, die im vertraulichen Gespräch mit Ärztinnen, Psychotherapeutinnen, Pflegekräften oder Kliniken entstehen, dürfen nicht in einen kassenbezogenen Auswertungs- und Steuerungskontext verschoben werden.

Die ärztliche und psychotherapeutische Schweigepflicht schützt nicht nur vor beliebiger Weitergabe. Sie schützt das Vertrauen in Behandlung. Dieses Vertrauen wird beschädigt, wenn Patientinnen und Patienten befürchten müssen, dass ihre Behandlungsdaten später von ihrer Krankenkasse ausgewertet und für Hinweise, Steuerung oder Risikobewertung genutzt werden.

Besonders problematisch ist, dass Krankenkassen zugleich ein Interesse an guter Versorgung und ein Interesse an Kostenkontrolle haben. Diese Doppelrolle führt zu einem strukturellen Interessenkonflikt. Für Versicherte ist oft nicht erkennbar, ob ein Hinweis wirklich ihrem Wohl dient, der Kostenreduktion, der Steuerung in bestimmte Programme oder der Vermeidung teurer Leistungen.

Auch eine Einwilligung gegenüber der Krankenkasse löst dieses Problem nicht. Viele Menschen befinden sich gegenüber ihrer Krankenkasse in einem Abhängigkeitsverhältnis. Wer Krankengeld, Psychotherapie, Reha, Hilfsmittel, Pflegeleistungen, Assistenz oder stationäre Behandlung benötigt, erlebt eine Anfrage der Krankenkasse nach zusätzlichen Daten möglicherweise nicht als frei ablehnbar. Eine formal erklärte Einwilligung kann unter solchen Bedingungen faktisch unfrei sein.

Besonders kritisch ist die Möglichkeit, zusätzliche personenbezogene Daten bei „anderen Stellen“ zu erheben. Dieser Begriff ist zu unbestimmt. Es muss ausgeschlossen werden, dass Krankenkassen Gesundheits- oder Sozialdaten bei Arbeitgebern, Behörden,

Arbeitsagenturen, Jobcentern, Bildungseinrichtungen, digitalen Plattformen oder sonstigen Dritten erheben können, um individuelle Risiken oder Versorgungsbedarfe zu bewerten.

Die Verbindung von ePA-Daten, Abrechnungsdaten, Selbstauskünften und zusätzlichen Daten kann zu umfassenden Gesundheitsprofilen führen. Daraus können Risikobewertungen, Prognosen, Hinweise oder Steuerungsimpulse entstehen. Besonders bei psychischen Erkrankungen wäre dies gefährlich, weil Daten über Therapieabbrüche, Medikamentenwechsel, Krisenbehandlungen, Arbeitsunfähigkeit oder stationäre Aufenthalte zu stigmatisierenden Risikoprofilen verdichtet werden könnten.

Deshalb muss klar geregelt werden: Keine Nutzung von ePA-Daten durch Krankenkassen zur individuellen Risikobewertung, Verhaltenssteuerung, Leistungssteuerung oder Profilbildung.

6. Reallabore der Krankenkassen begrenzen

Der Entwurf sieht Reallabore der Krankenkassen vor, in denen innovative Datenverarbeitungen erprobt werden können. Dies soll auch besondere Kategorien personenbezogener Daten umfassen. Innovation ist wichtig. Aber Gesundheitsdaten dürfen nicht zum Experimentierfeld werden, ohne dass Patientinnen und Patienten wirksam geschützt sind.

Reallabore bergen das Risiko, dass bestehende Grenzen der Datenverarbeitung schrittweise ausgeweitet werden. Sie können zur Verknüpfung verschiedener Datenquellen, zur Profilbildung und zur Normalisierung immer weitergehender Datennutzung führen. Für psychisch kranke und behinderte Menschen besteht das besondere Risiko, dass komplexe Lebens- und Krankheitsverläufe in Datenmodellen abgebildet und bewertet werden.

Reallabore dürfen daher nur unter engen Bedingungen zugelassen werden. Bei besonders sensiblen Daten muss ein ausdrückliches Opt-in erforderlich sein. Außerdem braucht es unabhängige Kontrolle, öffentliche Transparenz, eine Datenschutz-Folgenabschätzung, verbindliche Beteiligung von Patienten- und Behindertenvertretungen, klare Zweckbegrenzungen, kurze Laufzeiten, verbindliche Löschung oder Anonymisierung nach Projektende und wirksame Sanktionen bei Zweckü̈berschreitung.

Reallabore dürfen nicht dazu führen, dass Krankenkassen schrittweise neue Formen der Datenauswertung etablieren, die später zum Regelfall werden.

7. Forschungskennziffer und Sekundärnutzung

Die Sekundärnutzung von Gesundheitsdaten kann einen erheblichen Nutzen haben. Forschung kann bessere Erkenntnisse über Versorgung, Krankheitsverläufe, Arzneimittelsicherheit, seltene Erkrankungen, psychische Erkrankungen und Versorgungsungleichheiten ermöglichen.

Gleichzeitig ist die geplante Forschungskennziffer ein sehr weitreichendes Instrument. Sie ermöglicht die Verknüpfung von Gesundheitsdaten über verschiedene Datenquellen hinweg. Dadurch können langfristige, umfassende Gesundheitsprofile entstehen.

Pseudonymisierung ist wichtig, aber sie ist kein vollständiger Schutz. Bei seltenen Erkrankungen, komplexen Behinderungen, spezifischen psychischen Krankheitsverläufen oder besonderen Kombinationen aus Alter, Region, Diagnose, Medikation und Behandlungsgeschichte kann eine Reidentifizierung möglich sein.

Die Forschungskennziffer darf deshalb kein Fundament für umfassende staatliche, wissenschaftliche oder versicherungsbezogene Gesundheitsprofile werden. Jede Datenverknüpfung muss transparent, zweckgebunden, kontrolliert und widerspruchsfest sein. Besonders sensible Daten benötigen zusätzliche Schutzschwellen. Datennutzung darf nicht individualisiert gegen Betroffene zurückwirken.

8. Digitale Bedarfseinschätzung und Versorgungseinstieg

Der Entwurf sieht digitale Instrumente zur Bedarfseinschätzung, Ersteinschätzung und Terminvermittlung vor. Dies kann den Zugang zur Versorgung erleichtern. Gleichzeitig bestehen erhebliche Risiken.

Digitale Bedarfseinschätzung kann Menschen fehlleiten, wenn Symptome nicht richtig erfasst werden. Das gilt besonders bei psychischen Krisen, Suizidalität, Traumafolgen, neurodivergenter Kommunikation, psychosomatischen Beschwerden, kognitiven Einschränkungen, Sprachbarrieren, Mehrfacherkrankungen und Behinderungen.

Digitale Systeme dürfen nicht darüber entscheiden, ob ein Mensch berechtigten Zugang zu Behandlung erhält. Sie können unterstützen, aber nicht ersetzen. Besonders bei psychischen Krisen muss sichergestellt sein, dass digitale Systeme nicht zu Fehlsteuerung, Verzögerung oder Bagatellisierung führen.

Zudem darf der digitale Versorgungseinstieg nicht genutzt werden, um Einwilligungen zur weitergehenden Datennutzung einzuholen. Wer dringend einen Termin, eine Einschätzung

oder Hilfe benötigt, befindet sich nicht in einer freien Entscheidungssituation. Eine Einwilligung in dieser Lage ist besonders problematisch.

Digitale Bedarfseinschätzung darf daher nur als unterstützendes Angebot ausgestaltet werden. Sie darf nicht zum Pflichtweg werden, darf keine Benachteiligung bei Nichtnutzung auslösen und darf nicht mit automatischer Speicherung sensibler Ersteinschätzungen in der ePA verbunden werden.

9. Barrierefreiheit und digitale Teilhabe

Datenschutzrechte dürfen nicht nur auf dem Papier bestehen. Sie müssen praktisch nutzbar sein. Viele Menschen können digitale Systeme nicht oder nur eingeschränkt bedienen. Gründe können fehlendes Smartphone, fehlender Internetzugang, Armut, Wohnungslosigkeit, Seh- oder Hörbehinderung, kognitive Einschränkungen, Lernschwierigkeiten, psychische Krisen, Angststörungen, Sprachbarrieren oder geringe digitale Kompetenz sein.

Ein Opt-out oder eine Zugriffseinstellung schützt nur diejenigen, die das System verstehen und bedienen können. Wer das nicht kann, verliert faktisch Kontrolle über seine Daten.

Deshalb müssen alle Datenschutzrechte barrierefrei, niedrigschwellig und mehrkanalig ausübbar sein. Widerspruch, Einwilligung, Zugriffskontrolle, Datenkorrektur und Beschwerde müssen digital, telefonisch, schriftlich und persönlich möglich sein. Informationen müssen in Leichter Sprache, Gebärdensprache und screenreadergeeigneten Formaten bereitstehen. Unterstützung darf nicht allein von Krankenkassen abhängen, sondern muss auch durch unabhängige Beratungsstellen möglich sein.

Digitale Versorgung darf nicht bedeuten, dass Menschen ohne Smartphone, ohne stabile Lebensverhältnisse, ohne digitale Kompetenz oder in psychischen Krisen schlechteren Zugang zur Versorgung erhalten.

10. Schutz vor Benachteiligung im Arbeitskontext

Besonders sensibel ist der Zugriff auf ePA-Daten im betriebsärztlichen oder arbeitsbezogenen Kontext. Gesundheitsdaten können dort unmittelbare Auswirkungen auf Beschäftigung, Einsatzfähigkeit, berufliche Entwicklung, Verbeamtung, Beförderung oder Arbeitsplatzsicherheit haben.

Für Menschen mit Behinderungen und psychischen Erkrankungen ist das Offenbarungsrisiko besonders hoch. Bereits die Information, dass jemand in psychiatrischer oder psychotherapeutischer Behandlung war, kann zu Vorurteilen führen.

Deshalb darf es im arbeitsbezogenen Kontext keinen Zugriff auf ePA-Daten ohne ausdrückliches Opt-in geben. Ein bloßes Opt-out reicht nicht aus, weil Beschäftigte faktischen Druck erleben können. Die Verweigerung einer Datenfreigabe darf keine arbeitsrechtlichen oder faktischen Nachteile haben. ePA-Daten dürfen nicht für arbeitsrechtliche Entscheidungen oder mittelbare Leistungsbewertungen genutzt werden.

Der Gesetzgeber muss ausdrücklich verhindern, dass digitale Gesundheitsdaten in Beschäftigungskontexten zu Diskriminierung führen.

11. Schutz vor falschen, veralteten und missverständlichen Daten

Datenschutz umfasst auch Datenqualität. Falsche oder veraltete Gesundheitsdaten können erheblichen Schaden verursachen.

Besonders problematisch sind Verdachtsdiagnosen, Abrechnungsdiagnosen, veraltete psychiatrische Diagnosen, unvollständige Arztbriefe, nicht mehr aktuelle Medikationsdaten, missverständliche Krisenberichte, fehlerhafte Pflegeinformationen, Daten aus digitalen Ersteinschätzungen oder automatisch erzeugte Risikohinweise.

Bei psychischen Erkrankungen können falsche oder unvollständige Angaben besonders stigmatisierend wirken. Eine frühere Verdachtsdiagnose darf nicht dauerhaft den späteren Behandlungsweg prägen.

Patientinnen und Patienten brauchen deshalb wirksame Rechte auf Einsicht, Berichtigung, Ergänzung, Gegendarstellung, Sperrung, Löschung und unabhängige Beschwerde. Es muss eine einfache, barrierefreie Stelle geben, an die sich Betroffene wenden können, wenn ePA-Daten falsch, unvollständig oder schädlich sind.

12. Besondere Schutzkategorien für hochsensible Gesundheitsdaten

Der Entwurf behandelt Gesundheitsdaten zu einheitlich. In der Praxis gibt es jedoch erhebliche Unterschiede in Sensibilität und Missbrauchsrisiko.

Besonders schutzbedürftig sind psychiatrische und psychotherapeutische Daten, Suchterkrankungen, Suizidalität, Selbstverletzung, Zwangsmaßnahmen, Traumatisierung, Gewalterfahrungen, HIV und andere stigmatisierende Infektionen, genetische Daten, reproduktionsmedizinische Daten, Schwangerschaftsabbrüche, sexuelle Gesundheit, Behinderungsdaten, Pflegebedürftigkeit, seltene Erkrankungen sowie Daten über Kinder und Jugendliche.

Für diese Daten muss das Gesetz besondere Schutzmechanismen vorsehen. Eine pauschale Behandlung aller Gesundheitsdaten genügt nicht. Je sensibler eine Information ist und je größer das Risiko von Stigmatisierung, Diskriminierung oder Fehlinterpretation, desto höher müssen die Anforderungen an Zugriff, Weitergabe, Speicherung und Sekundärnutzung sein.

13. Konkrete Forderungen

Aus den genannten Gründen werden folgende Änderungen gefordert:

13.1 Das Gesetz muss Datenschutz als gleichrangiges Ziel aufnehmen

Der Zweck des Gesetzes darf nicht allein in Datennutzung, Innovation und Interoperabilität bestehen. Datenschutz, Vertraulichkeit, informationelle Selbstbestimmung, Barrierefreiheit und Schutz vulnerabler Gruppen müssen ausdrücklich als gleichrangige Gesetzesziele aufgenommen werden.

13.2 Keine erweiterte Nutzung von ePA-Daten durch Krankenkassen

Die geplante Nutzung von ePA-Daten durch Kranken- und Pflegekassen zur individuellen Risikoerkennung, Versorgungsempfehlung, Verhaltenssteuerung oder sonstigen Profilbildung ist zu streichen.

13.3 Keine Datenerhebung durch Krankenkassen bei unbestimmten „anderen Stellen“

Die Möglichkeit zusätzlicher Datenerhebung bei „anderen Stellen“ ist zu streichen oder eng zu begrenzen. Arbeitgeber, Behörden, Jobcenter, Arbeitsagenturen, Bildungseinrichtungen und vergleichbare Stellen müssen ausdrücklich ausgeschlossen werden.

13.4 Keine Einwilligung unter strukturellem Druck

Einwilligungen gegenüber Krankenkassen dürfen nicht als Grundlage für weitreichende Gesundheitsdatenverarbeitung dienen, wenn Versicherte zugleich Leistungen benötigen oder sich in Beratung, Krankheit, Krise, Terminnot oder Abhängigkeit befinden.

13.5 Feingranulares Berechtigungsmanagement der ePA

Die ePA muss eine einfache, barrierefreie und mehrkanalige Steuerung von Zugriffsrechten ermöglichen — mindestens auf Dokumentenebene, bei besonders sensiblen Daten auch auf Datenfeld- und Einzeleintragsebene.

13.6 Einzelne Medikationsdaten müssen ausblendbar sein

Versicherte müssen einzelne Medikamente gezielt verbergen können, wenn diese Rückschlüsse auf stigmatisierende Erkrankungen oder Lebenssituationen zulassen.

13.7 Besonderer Schutz psychischer Gesundheitsdaten

Psychiatrische, psychotherapeutische, Sucht-, Trauma-, Suizidalitäts- und Krisendaten müssen besonderen Schutz erhalten. Sie dürfen nicht automatisch sichtbar, nicht pauschal freigegeben und nicht durch Krankenkassen ausgewertet werden.

13.8 Beschlagnahmeschutz für ePA-Daten

ePA-Daten müssen ausdrücklich vor Beschlagnahme und zweckfremder Nutzung durch Ermittlungs-, Sicherheits- oder andere Behörden geschützt werden.

13.9 Reallabore streng begrenzen

Reallabore dürfen nur mit unabhängiger Kontrolle, öffentlicher Transparenz, Patientenbeteiligung, Datenschutz-Folgenabschätzung und ausdrücklichem Opt-in bei besonders sensiblen Daten zugelassen werden.

13.10 Forschungskennziffer absichern

Die Forschungskennziffer darf nicht zur umfassenden Profilbildung führen. Datenverknüpfungen müssen transparent, zweckgebunden, kontrolliert und widerspruchsfest sein.

13.11 Digitale Versorgung darf nicht zum Pflichtweg werden

Für digitale Bedarfseinschätzung, Terminvermittlung, ePA-Verwaltung, Widerspruch, Einwilligung und Datenkorrektur müssen gleichwertige analoge, telefonische, schriftliche und persönliche Wege bestehen.

13.12 Keine Einwilligung zur Sekundärnutzung im Versorgungskontext

Einwilligungen zur erweiterten Datennutzung dürfen nicht eingeholt werden, wenn Menschen gerade medizinische Hilfe, Termine, Ersteinschätzung oder Versorgung suchen.

13.13 Schutz im Arbeitskontext

Betriebsärztliche Zugriffe auf ePA-Daten dürfen nur mit ausdrücklichem Opt-in erfolgen. Die Verweigerung darf keinerlei arbeitsrechtliche oder faktische Nachteile haben.

13.14 Unabhängige Beratungs- und Beschwerdestellen

Es braucht unabhängige Stellen für Beratung, Widerspruch, Datenkorrektur, Beschwerden, ePA-Zugriffskontrolle, Forschungsdatennutzung und Reallabore. Krankenkasseninterne Ombudsstellen reichen nicht aus.

13.15 Verbindliche Korrektur falscher Daten

Falsche, veraltete oder missverständliche ePA-Daten müssen schnell korrigiert, ergänzt, gesperrt oder gelöscht werden können. Dafür braucht es klare Fristen und unabhängige Eskalationsmöglichkeiten.

14. Neuer Leitgedanke des Gesetzes

Der Entwurf sollte an zentraler Stelle neu ausgerichtet werden. Nicht die möglichst weitgehende Nutzbarkeit von Gesundheitsdaten darf Leitprinzip sein, sondern eine vertrauenswürdige digitale Gesundheitsversorgung.

Ein geeignetes Leitbild wäre:

Digitale Innovation im Gesundheitswesen muss dem Schutz, der Versorgung und der Selbstbestimmung der Patientinnen und Patienten dienen. Gesundheitsdaten dürfen nur in dem Umfang genutzt werden, in dem dies erforderlich, transparent, kontrollierbar, diskriminierungsfrei und mit besonderem Schutz vulnerabler Gruppen vereinbar ist.

Das Gesetz sollte deshalb nicht nur Datenverfügbarkeit schaffen, sondern bestehende Datenschutzdefizite der ePA beheben. Es muss den Patientinnen und Patienten echte Kontrolle geben. Es muss besonders sensible Daten besonders schützen. Es muss verhindern, dass Krankenkassen, Behörden, Arbeitgeber oder andere Akteure aus Gesundheitsdaten Macht über Menschen gewinnen.

15. Fazit

Der GeDIG-Entwurf ist in seiner jetzigen Form unausgewogen. Er stärkt Datennutzung, Innovation und digitale Steuerung, ohne die bestehenden Datenschutzprobleme der ePA ausreichend zu lösen.

Gerade für behinderte und psychisch kranke Menschen kann dies gravierende Folgen haben. Ihre Daten sind besonders sensibel, besonders stigmatisierungsanfällig und besonders folgenrelevant. Wer auf Versorgung, Hilfsmittel, Psychotherapie, Pflege, Krankengeld oder Reha angewiesen ist, braucht besonderen Schutz vor Offenbarung, Profilbildung, Benachteiligung und faktischem Druck.

Das Gesetz muss deshalb grundlegend nachgeschärft werden. Es darf nicht nur neue Datenräume eröffnen, sondern muss Vertrauen schaffen. Es muss Datenschutz, Barrierefreiheit und Selbstbestimmung als Voraussetzung digitaler Innovation begreifen.

Die zentrale Forderung lautet:

Aus dem „Gesetz für Daten und digitale Innovation im Gesundheitswesen“ muss ein „Gesetz für Datenschutz und digitale Innovation im Gesundheitswesen“ werden.

Oder anders formuliert:

Digitale Innovation ja – aber nur mit wirksamem Datenschutz, echter Patientenkontrolle, besonderem Schutz vulnerabler Gruppen und klarer Begrenzung der Datennutzung durch Krankenkassen und andere nicht behandelnde Akteure.

Mit freundlichen Grüßen

Thomas Seerig