Deutscher Bundestag
Ausschuss f. Gesundheit

Ausschussdrucksache
20(14)165(11)
gel. VB zur öffent Anh am
15.11.2023 - GDNG
13.11.2023

Innovationsverbund Öffentliche Gesundheit

Stellungnahme zum Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG)

Bianca Kastl, Innovationsverbund Öffentliche Gesundheit e. V. (InÖG)

Stuttgart, 13.11.2023

Bianca Kastl
2023.11.13 07:48:53
+01'00'

Vorbemerkung

Diese Stellungnahme befasst sich zu Beginn mit den vorgeschlagenen Änderungen durch den Gesetzentwurf (BT-Drucksache: 20/9046), um in Folge eine grundlegende Bewertung↘ vorzunehmen, speziell auch mit der Frage, ob der Gesetzentwurf „dabei stets dem Patienten- und dem Gemeinwohl dient und die Bürgerinnen und Bürger ins Zentrum aller Aktivitäten“ stellt. Technische Aspekte werden in dieser Stellungnahme nur begrenzt betrachtet. Bei Übereinstimmung in Teilaspekten werden andere bereits vorliegende Stellungnahmen referenziert.

Sofern Aspekte aus dem Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) (BT-Drucksache: 20/9048) für die Betrachtung im Kontext wichtig sind, werden diese hier zum besseren Verständnis erläuternd betrachtet.

Zusammenfassung der wichtigsten Aspekte

😍 **Positiv:** Veröffentlichung von Anträgen und Ergebnissen↘, Datenschutzaufsicht bei länderübergreifenden Gesundheitsforschungsvorhaben↘, Geheimhaltungspflichten und Strafvorschriften↘

👷 **Ausbaufähig:** Offenlegung der verwendeten technischen Systeme, Sandboxen und Audits↘, Weiterverarbeitung von Versorgungsdaten bei Gesundheitseinrichtungen↘, Nutzer*innenkreis und Anwendungsfälle↘, Nicht barrierefreies Opt-out-Management↘

🤨 **Bemerkenswert:** Schwammige Anwendung von Pseudonymisierung im Kontext der Krebsregister↘, Vertrauensstellen, Arbeitsnummern und Komplexität der Systemarchitektur↘, Vorabübermittlung vorläufiger Daten zur Abrechnung↘, Speicherfrist↘

🤔 **Klärungsbedürftig:** Finanzierung↘

😾 **Problematisch:** Information auf Verlangen bei Weiterverarbeitung von Versorgungsdaten↘, Datengestützte Erkennung durch Kranken- und Pflegekassen↘, Bruch mit informationeller Selbstbestimmung bei Forschungszwecken aus ePA↘, Nicht angemessenes Consent-Management↘, Interessenskonflikt Ansiedlung nationale Datenzugangs- und Koordinierungsstelle↘

😶 **Nicht adressierte, aber relevante Themen:** Fehlende logische Trennung von Entwicklung und Ausführung automatisierter Entscheidungsfindungssysteme↘, Fehlende konsistente Berücksichtigung der passenden Auflösung von Daten↘, Governance über automatisierte Entscheidungsfindungssysteme↘

Vorbemerkung, Teil 2:

Wegen Befassung mit dem GDNG wird diese Stellungnahme die Thematik Opt-Out nur in dem Kontext aufgreifen, wie dies in Behandlung des GDNG sinnhaft ist. Im Sinne des Rechts auf informationenelle Selbstbestimmung vertritt die Sachverständige auch den neuen Aspekten des Digitalgesetzes gegenüber **eine grundsätzliche Opt-in-Haltung**, was hier aber thematisch nur bedingt zur Sprache kommen kann.

Die folgenden Aspekte orientieren sich lose an der Reihenfolge des Entwurfs, teils auch in gebündelten Sinneinheiten. Es besteht kein Anspruch auf Vollständigkeit.

Aspekte betreffend GDNG

😍 Veröffentlichung von Anträgen und Ergebnissen

Grundsätzlich zu begrüßen ist die Zielsetzung, Anträge und Ergebnisse zu den über die Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten gestellten Anträgen zu veröffentlichen (§3 Absatz 2 GDNG) sowie die Publikationspflicht nach §8 GDNG bei öffentlichem Interesse.

👷 Offenlegung der verwendeten technischen Systeme, Sandboxen und Audits

Bei der Datenzugangs- und Koordinierungsstelle werden zwar viele Aufgaben der Bekanntmachung von Anträgen etc. durchgeführt, für die in §3 Absatz 2 Satz 9 GDNG genannten Konzepte und darauf aufbauenden technischen Systeme muss aber gelten, dass diese vollständig offengelegt werden. Da es sich bei diesen Systemen um Systeme handelt, die sensibelste Daten verarbeiten, ist eine externe Einsehbarkeit zur Vertrauensbildung unabdingbar. Es gilt hier in Anlehnung an die Petersberger Erklärung der DSK: **Je sensibler die Daten, die verarbeitet werden, desto transparenter muss die Funktionsweise der verwendeten Systeme sein.**

Darauf aufbauend sind Sandboxen der verwendeten Systeme mit Zufallsdaten (keine synthetischen Daten wegen Risiken der Rekonstruktion) anzudenken, um einerseits den Schulungsaufwand zu senken, andererseits Einblick von extern in die Verarbeitung zu ermöglichen.

Darüber hinaus ist die Veröffentlichung von regelmäßigen Audits von forschenden Organisationen anzudenken, analog zu den Data Sharing Audits des NHS in UK.

🤨 Schwammige Anwendung von Pseudonymisierung im Kontext der Krebsregister

Die Anwendung von Pseudonymisierung im Kontext Verknüpfung von Daten des Forschungsdatenzentrums mit den Krebsregistern ist höchst schwammig definiert und das bereits auf Ebene der Zuständigkeiten und rechtlichen Definition. Einerseits wird das spezifische Re-Identifikationsrisiko versucht zu minimieren (§4 Absatz 2 Satz 3 GDNG), andererseits wird die unabsichtliche Re-Identifikation im Text bereits erwähnt (§4 Absatz 2 Satz 8 GDNG), von einem Verfahren, das aber nur „im Benehmen“ mit BSI und BfDI abgestimmt werden soll. (§4 Absatz 2 Satz 8 GDNG). Hier ist eine Präzisierung „im Einvernehmen“ mit BSI und BfDI anzustreben.

Bianca Kastl (bianca.kastl@inoeg.de)

😍 Datenschutzaufsicht bei länderübergreifenden Gesundheitsforschungsvorhaben

Grundsätzlich zu begrüßen ist die Regelung zur **Vereinfachung der Datenschutzaufsicht** bei länderübergreifenden Gesundheitsforschungsvorhaben (§5 GDNG).

👷 Weiterverarbeitung von Versorgungsdaten bei Gesundheitseinrichtungen

In §6 GDNG wird Gesundheitseinrichtungen die Weiterverarbeitung von Versorgungsdaten eingeräumt und das ohne Einwilligung. Immerhin gibt es eine Informationspflicht. Das ist aus der Realität insofern nachzuvollziehen, weil Gesundheitseinrichtungen damit Daten verarbeiten, die sie ohnehin schon haben.

Kritisch sollte die Verwendung zu „zur medizinischen, zur rehabilitativen und zur pflegerischen Forschung“ gesehen werden, da hier durch eine regulatorische Lücke an der Opt-out-Möglichkeit zu Forschungsdaten der Patient*innen hinweg Forschungsdaten ausgeleitet werden könnten. Ähnlich äußert sich hier die Bundespsychotherapeutenkammer.

😾 Information auf Verlangen bei Weiterverarbeitung von Versorgungsdaten

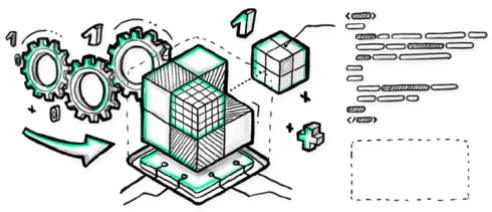
In §6 Absatz 4 Satz 3 GDNG wird der betroffenen Person das Recht eingeräumt, auf Verlangen über die Verarbeitung ihrer Daten durch datenverarbeitende Gesundheitseinrichtungen informiert zu werden. Das ist nicht mehr zeitgemäß und keinesfalls patient*innenzentriert. Hier sind einheitliche Konzepte anzustreben, die Patient*innen einen möglichst umfassenden Einblick in die sie betreffenden Datenverarbeitungen erlauben und zwar idealerweise proaktiv (und sicher). Ähnlich äußert sich hier auch die Stellungnahme des Caritasverbands.

😍 Geheimhaltungspflichten und Strafvorschriften

Grundsätzlich begrüßenswert ist, dass der Entwurf Geheimhaltungspflichten (§7 GDNG) und Strafvorschriften (§9 GDNG) in entsprechendem Maße vorsieht, wobei das für die Sicherheit des Gesamtsystems aber **nur als passive und reaktive organisatorische Sicherheitsmaßnahme** angesehen werden kann und somit nur dann wirkt, wenn alle anderen Sicherheits-Maßnahmen scheitern.

Aspekte betreffend Änderungen SGB V

😾 Datengestützte Erkennung durch Kranken- und Pflegekassen



Absolutes No-Go (§25b SGB V). Neben den medizinischen Aspekten (vgl. Stellungnahmen von Bundesärztekammer, Bundespsychotherapeutenkammer und KZBV und BZÄK) sprechen Aspekte des Datenschutzes (Profiling etc., vgl. ältere Stellungnahme BfDI), die unpräzise Datenlage der Abrechnungsdaten als auch der Aspekt des Konflikts mit der Kostenträgerschaft dagegen. Darüber hinaus ist die nicht ausgeführte Governance↘ und beschränkte Qualitätssicherung für eine mögliche Anwendung auf potentiell Millionen Datensätzen als **abenteuerlich** zu bezeichnen. Bei möglichem Inkrafttreten des Gesetzes Anfang 2024 wird nach §25b Absatz 7 SGB V eine erste Auswertung erst Mitte 2026 angesetzt. Bei einem technischen Feld, das gerade durch das Aufkommen von sogenannter

Bianca Kastl (bianca.kastl@inoeg.de)

KI stark im Wandel ist, ist dieser Zeitraum bis zur ersten systematischen Validierung zu lang und bedürfte kürzeren Intervallen oder beschränkten Pilotierungen (vgl. Bundesärztekammer).

Das von Krankenkassen möglicherweise geäußerte Argument, dass nur Krankenkassen einen vollständigen Blick auf Medikationen hätten (vgl. AOK) relativiert sich durch Konzepte wie den elektronischen Medikationsplan (vgl. Digitalgesetz).

🤨 Vertrauensstellen, Arbeitsnummern und Komplexität der Systemarchitektur

Am Beispiel der Vertrauensstelle am RKI (§64e SGB V) lässt sich (kurzer Ausflug in die Technik) zeigen, dass die im Gesetzentwurf skizzierten Methoden zur Vernetzung von Datensätzen speziell für Modellvorhaben eher aufwändig, vielschichtig und unter Beteiligung unnötig vieler Akteure stattfinden. Dies ist aus Sicht der Erhaltung der Privatsphäre der Beteiligten aber auch im Sinne der Systemresilienz nicht anzuraten.

Generell setzen die Pseudonymisierungs- und Verlinkungsmethoden im Gesetzentwurf konzeptionell **stark auf zentralisierte und damit aus Sicht von Cyberkriminellen lohnenswertere Akteure**, die kompromittiert und angegriffen werden könnten, wie das Forschungsdatenzentrum, Vertrauensstellen o. ä. (Teile davon sind auch ursächlich im EHDS zu sehen). Aus Sicht der Patient*innenzentrierung ließen sich diese Verfahren durch Ansätze von patient*innenindividuellen, persönlichen Datenräumen mit entsprechenden eigenständigen Verarbeitungsmöglichkeiten (auch mit der Möglichkeit der Delegation an vertrauenswürdige Dienstleister etc.), Pseudonymisierung an der Datenquelle, Methoden des verteilten Rechnens, föderierten Lernens sowie weitere privatsphärendeschonende Verfahren in ihrer Systemarchitektur stark vereinfachen und würden das Vertrauen in diese Verfahren steigern. Methoden dieser Art hätten auch die Möglichkeit eines einfacheren Rückkanals.

Erkenntnisse bei Anwendung dieser Verfahren könnten auch dem Auftrag der gematik nach Digitalgesetz zur Weiterentwicklung der elektronischen Patientenakte zugutekommen (vgl. Digitalgesetz).

🤨 Vorabübermittlung vorläufiger Daten zur Abrechnung

Der Mehrwert der Übermittlung von vorläufigen Abrechnungsdaten, unverifizierten Daten also, erschließt sich nicht (§ 295b SGB V), zumal die Abrechnungsdaten kein präzises Bild zeichnen. Es sei hierzu auch verwiesen auf die Bundespsychotherapeutenkammer, die Bundesärztekammer und die KZBV und BZÄK.

🤨 Speicherfrist

Eine Verlängerung der Speicherfrist im Forschungsdatenzentrum auf bis zu 100 Jahre (§ 303d Absatz 3) führt zu einem **Worst-Case-Szenario im Kontext der Informationssicherheit**. Es gibt hier um die Sicherung von Millionen sensiblen Datensätzen bei noch nicht mal ansatzweise bekannten äußeren und inneren technischen Risiken über den Zeitverlauf von 100 Jahren. Die medizinisch als Grund hervorgebrachten longitudinalen Analysen über diese Zeiträume sollten gezielt geplant werden, um ausgewählte Datenpunkte vom Datenbestand im Forschungsdatenzentrum isoliert über so einen langen Zeitraum vorzuhalten. Ein Datenspeicher mit 100 Jahren Speicherdauer funktioniert sinnvollerweise konzeptionell anders.

Bianca Kastl (bianca.kastl@inoeg.de)

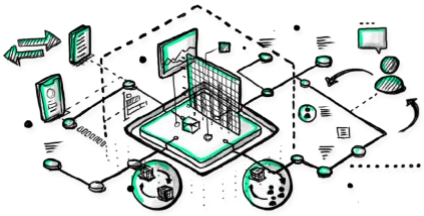
👷 Nutzer*innenkreis und Anwendungsfälle

In §1 GDNG wird von **gemeinwohlorientierter Forschung** gesprochen, generell öffnet sich das GDNG aber klar auch für privatwirtschaftliche Zwecke. Die Publikationspflicht unter §8 GDNG bietet durchaus Wege, die Registrierungs- und Publikationspflicht zu umgehen. § 303e SGB Absatz 2 öffnet die Nutzung für natürliche und juristische Personen im Anwendungsbereich der DSGVO, sofern die Zwecke erfüllt werden.

Es wäre daher im Sinne der Patient*innen zu klären, was das Gesetz eigentlich sein will: Klar gemeinwohlorientiert oder offen für alle, die dann aber als Unternehmen mit harten wirtschaftlichen Interessen sorgsam mit dem Label gemeinwohlorientiert umgehen sollten.

Das hat auch erhebliche Auswirkungen auf die Bereitschaft von Patient*innen, Daten im Sinne des Gemeinwohls zu teilen oder eben nicht. Einseitiges Datenteilen von Patient*innen mit Billigung durch das Label „Für das Gemeinwohl", bei dem dann privatwirtschaftliche Unternehmen durch Datennutzung ihre eigenen Kosten senken, der Gemeinschaft aber auf der anderen Seite nichts zurückgeben, verstärkt **Machtasymmetrien** und ist aus Sicht der digitalen Zivilgesellschaft, zu der sich auch der InÖG zählt, **gegen das Gemeinwohl**.

😾 Bruch mit informationeller Selbstbestimmung bei Forschungszwecken aus ePA



Die Standardeinstellung der Weitergabe von Patientendaten an Dritte in der elektronischen Patientenakte ist abzulehnen (§363 SGB V), da sie (weiterführend zu den hier nicht besprochenen Aspekte des Digitalgesetzes) einen klaren Bruch mit den Prinzip der informationellen Selbstbestimmung darstellen. Dies findet sich (erwartungsgemäß) auch in einer älteren Stellungnahme des BfDI.

Diese Einstellung verändert auch die Einstellung von Krankenkassen, Ministerien etc. zu der Art, in wie weit sie von sich aus über digitale Systeme aufklären. Nicht handeln und nicht ausreichend informieren ist im Falle eines Opt-out eher günstig für die, die vom nicht Opt-out profitieren.

Im Opt-in-Konzept würde es im Sinne aller Beteiligten liegen, gut über die Vorhaben zu informieren, um zu einer informierten Einwilligung zu motivieren. In Kombination mit der noch unklaren Definition von Gemeinwohl↘ im Gesetzentwurf führt dies zu einer noch **stärkeren Machtasymmetrie** gegenüber Patient*innen. Nutzer*innenzentriert und wohlinformiert geht anders.

Eine ähnliche Ablehnung findet sich bei der Bundespsychotherapeutenkammer.

😾 Nicht angemessenes Consent-Management

Die Thematik des **Consent-Management** (welche Daten ich genau mit wem teilen möchte) für Daten ist im Zweifelsfall **immer individuell.** Sie ist für die jeweils betroffene Person nicht immer passgenau und muss manchmal erst durch viel Aufwand, der zuerst einmal in Verantwortung der einzelnen Person liegt, passgenau gemacht werden, teils auch kontinuierlich.

Auf der einen Seite kann **eine vollständige Responsibilisierung des Individuums nicht vorausgesetzt** werden (vgl. aktuelle Masterarbeit von Mareike Lisker zu einem ähnlich gelagerten

Bianca Kastl (bianca.kastl@inoeg.de)

Thema). Auf der anderen Seite gibt es nach wie vor **Diskriminierung und Stigmatisierung aufgrund von bestimmten Daten**. Dies bringt auch das Digitalgesetz zur Sprache, in dem es bei der Speicherung dieser Daten in die ePA zumindest Rückfragemomente einfügt. Daten, deren Bekanntwerden Anlass zu Diskriminierung oder Stigmatisierung des Versicherten geben kann, insbesondere zu sexuell übertragbaren Infektionen, psychischen Erkrankungen und Schwangerschaftsabbrüchen (vgl. Digitalgesetz).

Hinsichtlich der Weitergabe von Daten an Dritte kann es hier noch weitere Komplikationen mit Forschungsdaten im Sinne einer Vertrauensbeziehung geben. Betroffene können ganz bewusst den Weg gehen wollen, sensible Daten mit ihrer vertrauten Ärzt*in Daten ganz bewusst digital nutzen zu wollen. Nur kann es möglicherweise den Fall geben, dass diese sensiblen Daten nicht an Dritte weitergegeben werden sollen. Hier findet sich dann eine Lücke in der Einstellungsmöglichkeit. Die einzige Möglichkeit zum Abstellen der Übertragung wäre ein Opt-out.

Anknüpfend an die Gedanken der Bundespsychotherapeutenkammer wäre hier darauf hinzuweisen, dass es möglicherweise ein tiefergreifendes Consent-Management braucht. Um diese Einstellungen entsprechenden nutzer*innen-freundlich zu halten und die sich verändernden Consent-Einstellungen möglichst aktuell, ist eine Einbindung von Betroffenenorganisationen in dieser Frage anzuraten (z. B. Deutsche Aidshilfe). **Betroffenenorganisationen könnten entsprechend gepflegte Einstellungsempfehlungen** zur Verfügung stellen, die Betroffene einfach anwenden könnten und zu ihren individuellen ePA-Einstellungen und Datenteileinstellungen übertragen könnten.

Das kann in dieser Form auch komplexe Consent-Situationen vereinfachen und die Verantwortung nicht ausschließlich allein auf die Betroffenen verlagern. Dies gilt auch für die ebenso komplexe Frage der Verschattung bzw. Teilverschattung von Informationen in der ePA.

👷 Nicht barrierefreies Opt-out-Management

Nach §363 SGB V ist ein Widerspruch nur mit Endgerät im Frontend möglich. Das liegt nach Erläuterung begründet in der Ende-zu-Ende-Verschlüsselung. Es ist aber kein Grund, diesen Vorgang nicht barrierefrei anzubieten. Dieser Umstand sollte ausgeräumt werden, weil es onst noch mehr Machtasymmetrie gibt, speziell bei ohnehin schon diskriminierten Gruppen.

😾 Interessenskonflikt Ansiedlung nationale Datenzugangs- und Koordinierungsstelle

Eine **Ansiedlung des Forschungsdatenzentrums** (§303d SGB V) beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), beide unter Hoheit des BMG, ist als **Interessenskonflikt** zu sehen. Zugang und Freigabe unter der gleichen Aufsichtsbehörde resultieren nicht automatisch in einer sinnvollen Abwägung von individuellen Schutzbedürfnissen versus medizinischen Interessen (vgl. auch Stellungname des Caritasverband).

Generelle Aspekte

😶 Fehlende logische Trennung von Entwicklung und Ausführung automatisierter Entscheidungsfindungssysteme

Im Entwurf findet aus technischer Sicht keine logische Trennung der Entwicklung und Ausführung automatisierter Entscheidungssysteme statt. Da die Anwendung von automatisierten Entscheidungssystemen in den meisten Fällen dezentral auf dem Endgerät der Patient*in in ihrer ePA

Bianca Kastl (bianca.kastl@inoeg.de)

oder z. B. individuell in der ärztlichen Praxis vertrauenswürdiger durchgeführt werden könnte, ist zu prüfen, in wie weit sich unterschiedliche rechtliche Möglichkeiten für die Entwicklung und Ausführung von automatisierten Entscheidungsfindungssystemen anbieten.

😶 Fehlende konsistente Berücksichtigung der passenden Auflösung von Daten

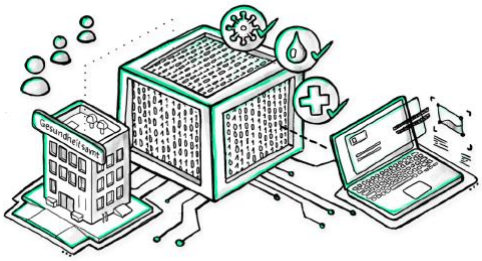
In vielen Aspekten des Gesetzentwurfs wird durchgängig nur von pseudonymisierten Daten gesprochen. Anonyme Daten werden nur in der Erläuterung erwähnt. Die Erwähnung aggregierter Daten fehlt als eigene Datenkategorie in der Gesamtbetrachtung.

In Anlehnung an Security-Prämissen wie das Principle of least Privilege (habe nur genau soviel Zugriff wie du brauchst) wäre zu prüfen, in wie weit die Anträge auf Forschungsdaten eine Angabe der Auflösung mitberücksichtigen können. Dies würde aufgrund des reduzierten Schutzbedarfs manche Anträge in ihrer Freigabe erheblich beschleunigen. Ähnliche Gedanken finden sich bei der Bundesärztekammer.

🤔 Finanzierung

In der Auflistung der Finanzierung der jeweils für die Forschungsdateninfrastruktur notwendigen Knotenpunkte (Forschungsdatenzentrum, Stellen am BfArM und RKI) ergeben sich relativ geringe Personalkosten für neuralgische Punkte in der Gesamtinfrastruktur für voraussichtlich ein paar Millionen Datensätze. Angesichts des Wertes dieser Daten bei Datenverkauf oder Ransomwareangriffen ergibt sich hier möglicherweise ein Risiko durch zu dürftige Personalausstattung. 73 Millionen Datensätze, die zukünftig mit Daten aus der ePA angereichert bzw. verknüpfbar werden, dürften in dunklen Ecken des Webs auch einen erhöhten finanziellen Einsatz seitens Angreifern auslösen. In Kombination mit der vorgeschlagenen Speicherfrist↘ von 100 Jahren erhöht sich dieses Risiko zusätzlich.

😶 Governance über automatisierte Entscheidungsfindungssysteme



In vielen Abschnitten des Gesetzes werden automatisierte Entscheidungsfindungssysteme (neudeutsch sogenannte KI) angedeutet. Angesichts der Regelungstiefe mancher Details verwundert es durchaus, dass bei der Anwendung dieser Systeme im medizinischen Kontext grundlegende Qualitätssicherungsmaßnahmen unerwähnt bleiben. Diese werden nur ansatzweise im Kontext der Krankenkassen↘ angeschnitten.

Ungeachtet von den Entwicklungen im AI Act ist angesichts der möglichen Auswirkungen von automatisierten Entscheidungsfindungssystemen im Medizinbereich über eine systematische Erfassung der verwendeten Systeme speziell auch im medizinischen Kontext nachzudenken. Dazu gehört mindestens eine systematische, regelmäßige Auswertung von False Positive Raten, Bemühungen zum Bewerten von Bias, ein Verzeichnis der verwendeten Verfahren und die Klärung der Frage, ob in bestimmten Anwendungsszenarien eventuell ein deterministisches System einem stochastischen System vorgezogen werden sollte.

Bianca Kastl (bianca.kastl@inoeg.de)

Abschließende Bewertung

Die Forderungen nach Gesundheitsdatennutzung folgen in diesen Tagen oftmals dem Leitspruch „Daten retten Leben“, der rechtfertige, dass nun „Datenschätze zum Wohle der Patient*innen gehoben“ werden müssten. Durch Überstrapazierung dieses Narratives entstehen aber keine guten digitalen Systeme, die die auch die Bedürfnisse der Patient*innen und Leistungserbringer angemessen berücksichtigen würden. Die fehlende Patient*innenorientierung zeigt sich bereits in diesem Entwurf. Es sei aber der Fairness halber angemerkt, dass das vorliegende Gesetz nicht 20 Jahre Herumirren im digitalen Gesundheitswesen auf einmal aufholen kann. Dem Gesetz ist aber anzumerken, dass es primär um die Erreichung politischer Zielmarken geht, wie etwa den 80 Prozent ePA-Durchdringung 2025.

Im Ansatz der Nutzbarmachung von Gesundheitsdaten verfolgt das Gesetz zumindest klar eine zur elektronischen Patientenakte passende Zielrichtung. Ebenso wie die elektronische Patientenakte, die das elektronisch schon im Namen trägt, ist das Gesundheitsdatennutzungsgesetz kein genuin digitales Gesetz, sondern setzt an vielen Stellen auf Aspekte der Elektrifizierung statt nativer Digitalisierung.

Damit wird das GDNG aber auf keinen Fall dem Ziel der Verarbeitung von Gesundheitsdaten gerecht, dass die Bürgerinnen und Bürger ins Zentrum aller Aktivitäten stellt. Im Zentrum des Gesetzes steht eher die Forschung, Bürgerinnen und Bürger sind eher nur am Rande Teil dieses Ökosystems, wenn sie auch wichtig als Datenlieferanten sind – zusammen mit den Leistungserbringer*innen, deren Anteil an der Datengenerierung ebenfalls wenig gewürdigt wird, weder finanziell noch durch ausreichende digitale Mitwirkungsmöglichkeiten.

Verglichen mit wirklich bürger*innenzentrierten Anwendungen wie der Corona-Warn-App oder zum Teil der Corona-Datenspende App, welche in kürzerer Zeit – wenn auch unter pandemischen Bedingungen – eine größere Durchdringung und ein höheres Vertrauen in der Bevölkerung erreicht haben, wirken die Grundlagen, die das GDNG legt, wie ein Rückschritt. Speziell auch im Bereich Datenschutz und Informationssicherheit. Dies gilt auch im Beispiel der Corona-Datenspende App für das Zusammenführen von Behandlungsdaten und patient*innen-eigenen Daten etwa von Wearables, die hier gar nicht Teil der Betrachtung waren.

Trotz der Bemühungen um einen schnellen Rollout der elektronischen Patientenakte muss 2023 die Frage gestellt werden, ob in der Art „elektrifizierte Akten“ der Art noch zeitgemäß sind oder ob es nicht ein neues, genuin digitales Konzept eines digitalen Patientenclient in Patient*innenhand bräuchte, auch um den Belangen hochvernetzer individueller medizinischer Forschung besser zu genügen.

Digitale medizinische Forschung im Jahr 2023 muss eigentlich noch viel näher zu den Menschen, braucht stärkere Einbeziehung dieser, braucht einen echten Forschungsdialog auf Augenhöhe – bei gleichzeitiger weitgehender Datenautonomie und großer Transparenz für die Patient*innen. Nur so kann das nötige Vertrauen in das digitale Gesundheitswesen in Deutschland geschaffen werden. Die Art von Forschung, die das GDNG hier beschreibt, ist näher bei großen Forschungseinrichtungen denn bei den betroffenen Menschen. Daran ändern auch Entwicklungen im Bereich KI nichts, sie verschärfen die Machtasymmetrie eher noch zusätzlich nach aktueller Ausgestaltung.

Ein besseres, forschendes und lernendes digitales Gesundheitswesen, das Bürger*innen wirklich ins Zentrum stellt wäre möglich – aber nicht mit diesem Entwurf.

Bianca Kastl (bianca.kastl@inoeg.de)

Bezug der Sachverständigen zum Themengebiet

Bianca Kastl ist 1. Vorsitzende des Innovationsverbund Öffentliche Gesundheit und engagiert sich für eine bessere Digitalisierung von Verwaltung und Gesundheitswesen in Deutschland.

Ihr fachlicher Schwerpunkt sind skalierende, sichere digitale Infrastrukturen, Systemarchitekturen, Cloud native Anwendungen, IT-Security mit dem Fokus auf Zero Trust Prinzipien, Privacy sowie Barrierefreiheit und User Experience.

Thematisch an das Thema GDNG anschließend ist sie beratend tätig zur Zero Trust Architektur für die Telematikinfrastruktur (TI 2.0). In der Pandemie war sie vor allem tätig im Bereich digitaler Kontaktnachverfolgung und Meldewesen mit dem Fokus auf digitalen Infrastrukturen und kennt daher die beschriebenen Problematiken aufgrund der fehlenden Datenverfügbarkeit und Interoperabilität aus eigener Erfahrung.

Mit einer Gruppe weiterer zivilgesellschaftlicher Akteur*innen und Betroffenengruppen (u. a. von der Deutschen Aidshilfe) unter Organisation des Superrr Lab hat sie an dem Positionspapier Was Menschen vom digitalen Gesundheitssystem erwarten mitgewirkt.

Beruflich ist sie als Tech Lead und Chief Product Owner im Öffentlichen Dienst tätig und entwickelt vernetzte Anwendungsplattformen für den Öffentlichen Gesundheitsdienst nach Stand der Technik in Hessen, hat also auch beruflich Bezugspunkte zur Umsetzung des GDNG.

Über den Innovationsverbund Öffentliche Gesundheit e. V. (InÖG)

Der Innovationsverbund Öffentliche Gesundheit (InÖG) entstand 2020 aus einem Zusammenschluss von Projekten, die sich im Rahmen des #WirVsVirus Hackathons unter der Schirmherrschaft des Bundeskanzleramts verknüpft haben. In der Tradition etablierter zivilgesellschaftlicher freier Träger und in Anlehnung an das THW wird der Öffentliche Gesundheitsdienst als Schnittstelle von Verwaltung und Gesundheitswesen gezielt und nachhaltig mit Open Source Technologie unterstützt. In Zusammenarbeit mit der Björn Steiger Stiftung entstand als erstes Digitalprojekt IRIS connect. IRIS connect ist eine der ersten nach Zero Trust Prinzipien aufgebauten interoperablen Kommunikationsinfrastrukturen im öffentlichen Gesundheitsdienst und wurde in der Pandemie über vier Bundesländer hinweg eingesetzt.

Darüber hinaus hat der InÖG eine Privatsphäre-freundliche, deutschlandweit skalierbare Impfplattform in der Pandemie entwickelt.

Im Kontext Europäischer Gesundheitsdatenraum hat der InÖG den Offenen Brief der EDRI (European Digital Rights Initiative) zu Patient*innenrechten im EHDS mitgezeichnet.

Der InÖG arbeitet an der Schnittstelle zwischen Akademia, Politik, Verwaltung und Open Source Community. Das interdisziplinäre Team besteht aus Software Entwickler*innen, Forscher*innen, Unternehmer*innen, Hacker*innen, Berater*innen, Software Architekt*innen und Mitarbeiter*innen des öffentlichen Dienstes und Gesundheitswesens.

Der InÖG agiert überparteilich, gemeinwohlorientiert sowie unabhängig von Unternehmen und Verbänden.