Stellungnahme zur Digitalisierungsstrategie des Bundesgesundheitsministeriums für das Gesundheitswesen und die Pflege

Das Bundesministerium für Gesundheit (BMG) hat mit der am 9. März 2023 vorgestellten Digitalisierungsstrategie einen großen und mutigen Entwurf für ein modernes, die Chancen der Digitalisierung nutzendes, datengetriebenes Gesundheitssystem vorgestellt. Wie immer können mit dieser ersten Positionierung noch nicht alle Themen ausreichend konkret geregelt werden.

Gesundheitsdaten sind zu Recht gesetzlich besonders geschützt und ihre Verwendung ohne Vorliegen einer spezifischen Zustimmung ist auf Situationen beschränkt, in denen die Bürger:innen einen unmittelbaren oder mittelbaren Nutzen davon haben. Die Analyse von Daten, die unmittelbar aus der Versorgung kommen, kann jedoch einen großen Unterschied in der bestmöglichen Behandlung von Patient:innen sowie der Entwicklung und Überwachung von Therapieansätzen, Medikamenten und Medizinprodukten bedeuten. Diese Potentiale sind bisher weitgehend ungenutzt, und zwar sowohl hinsichtlich der Datenverfügbarkeit und Nutzbarkeit für die unmittelbare Versorgung der Patient:innen als auch deren Verwendung für die Forschung. Die Gründe für diesen Missstand sind vielfältig, führen im Ergebnis aber dazu, dass Deutschland seine Attraktivität als Forschungsstandort verliert. Wichtige Digitalisierungsvorhaben sind mit Verweis auf datenschutzrechtliche Bedenken nur unzureichend umgesetzt worden. Die gesetzlichen Rahmenbedingungen möchte das BMG im Rahmen der Digitalisierungsstrategie für das Gesundheitswesen und die Pflege nun ändern.

Zur Umsetzung der Digitalisierungsstrategie hat das BMG einen Entwurf für ein Digitalgesetz und ein Gesundheitsdatennutzungsgesetz angekündigt, die wichtige Änderungen an bestehenden Gesetzen enthalten werden. Auf neue Rahmenbedingungen für das gesamte Gesundheitsdatenökosystem deuten die bisherigen Verlautbarungen jedoch nicht hin. Der nachfolgend beschriebene Reformbedarf ist für den Erhalt des Forschungsstandorts Deutschland allerdings ebenso beachtlich wie die Reform der elektronischen Patientenakte (ePA) und des Forschungsdatenzentrums (FDZ).

Für einen Erfolg der Digitalisierungsstrategie sollte das BMG daher die folgenden Aspekte ebenfalls weiterentwickeln:

1. Klare und spezifische Erlaubnisnormen für das gesamte Gesundheitsdatenökosystem
2. Transparenz und Partizipation bei der Datenverwendung
3. Freiwilligkeit der Bereitstellung von Gesundheitsdaten für Forschung
4. Forschung ist ein Prozess mit vielen Zwischenzielen
5. Datenmangel in der Forschung
6. Qualität der verfügbaren Daten
7. Sichere IT und Datenverarbeitung
8. Zertifizierungen für Datenverarbeiter
9. Souveräne europäische Datenverarbeitungsstrukturen

Wir möchten uns mit dieser Stellungnahme auf die noch offenen Herausforderungen rund um die Bereitstellung, Verarbeitung, Aufbereitung, Kombination und Anonymisierung von Gesundheitsdaten (v.a. von Real World Data) zum Zwecke der medizinischen Forschung fokussieren und führen die oben genannten Aspekte hier näher aus.

1. Klare und spezifische Erlaubnisnormen für das gesamte Gesundheitsdatenökosystem

Eine Ursache für die bisher ungenutzten Potentiale von Gesundheitsdaten aus der Versorgung ist der wenig differenzierte Rechtsrahmen, unter dem die Datennutzung den Akteuren grundsätzlich untersagt wird. Zwar sind auch schon heute einzelne gesetzliche Insellösungen vorgesehen, wie etwa das FDZ oder die Forschung durch den Innovationsausschuss des Gemeinsamen Bundesausschusses der gesetzlichen Krankenversicherungen. Es fehlen jedoch klare Erlaubnisnormen, die es allen relevanten – auch privaten - Akteuren im Gesundheitsdatenökosystem ermöglichen, Gesundheitsdaten für die Forschung zu nutzen. Zu diesen Akteuren zählen insbesondere auch Datentreuhänder und Research Data Hubs wie Honic, die einen wesentlichen Beitrag zur Verfügbarmachung von Daten für die Forschung in einem dezentralen Ökosystem leisten.

Diese schwierige Ausgangssituation kann nur durch weitere spezifische Erlaubnisnormen behoben werden. Die Voraussetzungen jeder neuen Erlaubnisnorm müssen dabei das Ergebnis einer Abwägung der Interessen der Bürger:innen und dem verfolgten Zweck sein. Das Ergebnis sollte sich auch in konkreten Anforderungen an die Schutzkonzepte und IT-Infrastruktur der jeweiligen Akteure widerspiegeln. So sollte eine Pseudonymisierung beispielsweise stets von einer selbstständigen Stelle durchgeführt werden, die sich von der Rechtsperson der Stelle, die die pseudonymisierten Daten anschließend für Forschung verwendet, unterscheidet.

Eine entsprechende Interessenabwägung sieht heute bereits der § 27 Bundesdatenschutzgesetz vor – allerdings überlässt die Norm die Abwägungsentscheidung den Datenverarbeitern. Dies führt zu einer großen Verunsicherung auf Seiten der Datenverarbeiter und einem uneinheitlichen Datenschutzniveau innerhalb Deutschlands. Gerade das unterschiedliche Datenschutzniveau gefährdet die Akzeptanz der Datennutzung in Deutschland.

Die neuen Erlaubnisnormen müssen sich selbstverständlich widerspruchlos in den übrigen regulatorischen Rahmen, insbesondere den European Health Data Space (EHDS), einfügen und leicht verständliche Voraussetzungen normieren. Denn der Aufwand und die Kosten dafür, bestehende Rechtsunsicherheiten aufzulösen, binden die ohnehin limitierten Ressourcen der Leistungserbringenden im Gesundheitswesen für eine bessere Nutzung von Gesundheitsdaten.

Daneben befürworten wir den weiteren Ausbau des FDZ hin zu mehr Datenquellen (Register, ePA-Daten). Auf der Zeitachse wird mit diesen Daten aber erst in einigen Jahren geforscht werden können. Dabei entsteht schon heute in Deutschland und Europa ein Ökosystem rund um Gesundheitsdaten, das deutlich kurzfristiger der medizinischen Forschung Daten zur Verfügung stellen kann. Dieses Ökosystem benötigt klare Anforderungen, die dann aber auch in Erlaubnisnormen münden.

2. Transparenz und Partizipation bei der Datenverwendung

Für eine breite Unterstützung der umfassenden Datennutzung, wie sie die Gesetzesvorhaben des BMG vorsehen dürften, ist es unabkömmlich, dass die Datennutzung für die Bürger:innen transparent ist. Informationspflichten ergeben sich bereits aus den

Datenschutzgesetzen, zusätzliche Transparenzpflichten stärken jedoch die gesellschaftliche Akzeptanz und das Vertrauen in die entwickelten Lösungen. Dies gilt insbesondere, da auf diese Weise auch der gesellschaftliche Nutzen der Datenverwendung für die Bürger:innen nachvollziehbar wird. Obgleich sich nicht alle Bürger:innen für die Verwendung ihrer Daten interessieren und richtigerweise darauf vertrauen, dass ihre demokratisch legitimierten Vertreter die Grundsatzscheidungen in ihrem Interesse treffen und auch die Einhaltung der Gesetze durchsetzen, ist eine aktive Partizipation von Bürgervertretungen im Bereich der Gesundheitsdatennutzung besonders wertvoll. Die Rolle der Bürgervertretungen besteht dabei nicht nur darin, die Datenverwendung zu überwachen, viel wichtiger ist die Beratung der relevanten Akteure, um die Datenverwendung von Anfang an auf die Interessen und Bedürfnisse der Bürger:innen auszurichten.

Die adressatengerechte Erfüllung des Transparenzgebots stellt die Akteure dabei vor einige Herausforderungen – wie, durch wen und vor allem in welcher Situation sollten interessierte Bürger:innen über die Nutzung der Gesundheitsdaten informiert werden bzw. sich informieren können? Diese Fragen müssen geklärt werden, um den verantwortlichen Akteuren wirksame und einheitliche Transparenzpflichten als klare Handlungsanweisungen zu geben. Eine Standardisierung der Transparenzmaßnahmen wird für sich bereits dazu führen, dass die Informationen von interessierten Bürger:innen leicht aufgefunden werden. So könnten für Bürger:innen beispielsweise zentrale Informations- und Widerspruchsstellen für den gesamten Forschungssektor etabliert werden. Diese müssten von vertrauenswürdigen Institutionen betrieben werden, deren einziger Zweck es ist, die Bürger:innen adäquat zu informieren und ihre berechtigten Interessen gegenüber den jeweiligen Akteuren im Forschungsbereich durchzusetzen.

3. Freiwilligkeit der Bereitstellung von Gesundheitsdaten für Forschung

Die Verwendung pseudonymisierter Gesundheitsdaten für gemeinnützige Forschung ist dringend geboten. Die Verarbeitung dieser Daten in sicheren Einsatzumgebungen unter Einhaltung des Transparenzgebots findet auch eine breite Unterstützung in der Gesellschaft. Nichtsdestotrotz gibt es Menschen, die berechtigte Interessen geltend machen können, wegen derer ihre Daten nicht für jede Art von Forschung verwendet werden sollten. Für diese Menschen muss eine leichtzugängliche Widerspruchsmöglichkeit gewährleistet sein.

Die Datenschutz-Grundverordnung (DS-GVO) sieht verschiedene Rechtsgrundlagen für die Verarbeitung von Gesundheitsdaten für die Forschung vor. Nach Jahren kategorischer Ablehnung innovativer Forschungsansätze durch Datenschutzbeauftragte und Datenschutzaufsichten und im Versuch, die deutsche Rechtstradition der individuellen Einwilligung mit den Anforderungen moderner medizinischer Forschung in Einklang zu bringen, wurde in Deutschland der sog. „Broad Consent“ entwickelt. Der Broad Consent ist nicht nur unionsrechtlich angreifbar, sondern auch auf tatsächlicher Ebene oft nicht geeignet, um die Lücke hinsichtlich forschungsfreundlicher Erlaubnisnormen für den gesamten Forschungsbereich zu schließen.

Nicht nur im Gesundheitsbereich wird die datenschutzrechtliche Einwilligung zu Recht sehr kritisch gesehen. Häufig werden solche Einwilligungen in Situationen eingeholt, in denen die Personen weder wirklich frei von allen Zwängen entscheiden können noch in angemessener Weise informiert werden können. Zudem sind beim Bestehen auf die individuelle

Zustimmung viele (insbesondere retrospektive) Datensätze von der Verwendung für die Forschung ausgeschlossen. Rein einwilligungsbasierte Ansätze führen so zu starken Verzerrungen der Daten, womit diese für die Forschung im Ergebnis kaum nutzbar sind. Andere EU-Länder zeigen erfolgreich, dass Forschung auch ohne Einwilligung möglich ist. Dies sollte auch in Deutschland zur Norm werden, wenn die Datentreuhänder und Research Data Hubs entsprechend hohe Anforderungen – formal, prozessual und technologisch – erfüllen.

4. Forschung ist ein Prozess mit vielen Zwischenzielen

Die DS-GVO stellt in den Erwägungsgründen ausdrücklich klar, dass der Begriff „Forschung“ weit verstanden werden soll. Auch den Akteuren in den unterschiedlichen Bereichen der Forschung ist klar, dass „Forschung“ aus vielen Prozessschritten besteht. Diese schließen die Verarbeitungen der Daten ein, die erforderlich sind, um die Forschungshypothese zu entwickeln, die Daten aufzubereiten sowie zu aggregieren, sie zu analysieren und die Ergebnisse zu interpretieren und zu disseminieren.

Die Voraussetzungen, unter denen Daten für Forschung verwendet werden können, müssen sich an den mit der Datenverwendung zu erwartenden Risiken für die Bürger:innen orientieren. Während umfassende Analysen von großen Datenmengen zusätzliche Sicherheitsmaßnahmen erfordern, sollten für explorative Dateneinblicke im Rahmen der ersten Prozessschritte für ein Forschungsprojekt weniger strenge Anforderungen definiert werden, d.h. insbesondere keine umfassenden Folgenabschätzungen oder Ethikvoten. "Explorative Forschung“ dient der vorbereitenden Machbarkeitsprüfung, indem Forschende sich beispielsweise einen Überblick über die verfügbaren Daten verschaffen und Forschungshypothesen auf Grundlage des Überblicks entwickeln.

Darüber hinaus ist eine Unterscheidung nach privaten (vermeintlich „bösen“) und öffentlichen (vermeintlich „guten“) Forschungseinrichtungen nicht nur von der DS-GVO nicht vorgegeben, sie ist auch nicht zielführend. Bereits heute arbeiten universitäre Forschende Hand in Hand mit privaten Forschenden und verbessern auf diese Weise die Ausgangslage für die Forschung erheblich.

Das heißt jedoch nicht, dass es keine limitierenden Anforderungen an die konkreten Forschungsprojekte geben sollte. Insbesondere sollten Gesundheitsdaten nur für Forschung verwendet werden, wenn die Forschung einen gesellschaftlichen Nutzen hervorbringen kann. Dieser Nutzen kann unter anderem darin bestehen, dass Medikamente und Medizinprodukte bedarfsspezifisch entwickelt oder nach Inverkehrbringung beobachtet werden sowie neue zielgerichtete Versorgungskonzepte entwickelt werden.

5. Datenmangel in der Forschung

Forschende sind bisher in Deutschland in den allermeisten Projekten auf die Auswertung von Daten limitiert, die aufgrund von prospektiven Studien erhoben wurden. Auf diese Weise bleiben große Datenmengen für die Forschung vollkommen ungenutzt. Die seit langem geforderte und nun vorgeschlagene Reform der ePA und des FDZ wird die Menge der für die Forschung verfügbaren Daten zwar in einigen Jahren vermehren. Die Erfahrung zeigt aber, dass selbst das vom Gesundheitsminister ausgerufene Ziel, mindestens 300

Forschungsprojekte anhand von Daten, die das FDZ bereitstellt, bis 2026 durchzuführen, noch in weiter Ferne ist.

Bereits heute ist klar, dass die Mehrung der für die Forschung verfügbaren Daten nur mit einem Kulturwandel erreichbar ist. Es herrscht eine Kultur des Neinsagens bei Datenschützern und bei den Leistungserbringenden die Angst vor datenschutz- und strafrechtlichen Konsequenzen. Zudem fehlen die Anreize, die mit der Verfügbarmachung von Daten entstehenden Aufwände zu erbringen. Der Kulturwandel muss jetzt durch Einführung klarer, rechtlicher Erlaubnisnormen begründet werden, damit auch heute schon Daten für die Forschung verfügbar werden. Ein Abwarten auf die Aufnahme des Betriebs des reformierten FDZ und der im EHDS geplanten europaweiten Forschungsinfrastruktur wäre höchst fahrlässig.

Darüber hinaus sollten insbesondere bereits vorhandene große Datensammlungen für die Forschung verfügbar gemacht werden. Hier gilt es auch Datenaggregatoren wie Abrechnungszentren und IT-Dienstleister im Gesundheitswesen spezifisch zu ermächtigen, gesammelte Daten für die Forschung verfügbar zu machen. Auch sollten die von den Krankenkassen gesammelten Abrechnungsdaten nicht erst beim FDZ für die Forschung verfügbar gemacht werden. Diese Daten sollten vielmehr ggf. kombiniert mit anderen relevanten Daten bereits heute für die Forschung verfügbar sein.

6. Qualität der verfügbaren Daten

Die Daten müssen für die primäre Nutzung zur Versorgung in geeigneter Form erfasst werden. Daneben ist es jedoch essenziell, dass bereits bei der Erhebung der Daten die Anforderungen an diese im Bereich der Sekundärnutzung beachtet werden. Die aktuell vorhandenen Daten aus der medizinischen Versorgung sind nur nach umfangreicher Aufbereitung für die Forschung auswertbar. Der zur Datenaufbereitung erforderliche Aufwand sollte insbesondere durch gesetzliche Codiervorgaben für die Dateneingabe und die Errichtung von für die Bedürfnisse der Forschung strukturierten verpflichtenden Schnittstellen reduziert werden. Hierzu müssten z.B. die Eingabemasken von teilweise jahrzehntealten Praxis-Management-Systemen angepasst und verbessert werden, um Daten nach einheitlichen Standards zu erheben.

Statt direkte Datenbankzugriffe zu gewähren, die datenschutzrechtlich und IT-sicherheitsrelevant sind, sollten insbesondere Aggregatoren von Gesundheitsdaten verpflichtet werden, Schnittstellen zu errichten, über die die relevanten Akteure (Datentreuhänder und Research Data Hubs) die für die Forschung kuratierten Daten erhalten können. Die bestehenden Pflichten zum Angebot von Schnittstellen wie z.B. die Schnittstellenfestlegungen für die PVS-Archivierungs- und Wechselschnittstelle der kassenärztlichen Bundesvereinigung entsprechen nicht mehr dem Stand der Technik und erzeugen keine für Forschung auswertbaren Daten.

Der auch im EHDS verfolgte Ansatz, die von Wearables erhobenen Daten für die Forschung verfügbar zu machen, ist zu begrüßen. Kombiniert mit Versorgungsdaten können diese den Aussagewert der Daten deutlich erhöhen. Nichtsdestotrotz ist es essenziell, dass die Bemühungen, die Daten von Wearables verfügbar zu machen, nicht dazu führen, dass die Bestrebungen in den Hintergrund treten, die seit Jahrzehnten bekannten Hindernisse für die

Erhebung von auswertbaren Daten endlich holistisch durch Etablierung von Standards zur Gewährleistung der Interoperabilität zu lösen.

7. Sichere IT und Datenverarbeitung

Der Gesetzgeber sollte klare Anforderungen an die IT-Sicherheit für die Erschließung, den Transport, die Speicherung sowie die Verarbeitung der Gesundheitsdaten normieren, damit ein einheitliches Ende-zu-Ende Sicherheitsniveau entsteht – von der Quellumgebung, in der die Daten erschlossen werden, bis zur Umgebung, in der die verschiedenen Datenklassen konsolidiert und zur Auswertung gebracht werden („Defense-in-Depth“). Auf diese Weise muss ein Verlust der Kontrolle über die Gesundheitsdaten effektiv verhindert werden.

Eine sichere Verarbeitungsumgebung ist das Fundament für eine Auswertung von umfangreichen pseudonymisierten oder anonymisierten Datensätzen. Dabei ist auch zu klären, welche Verfahren zu Pseudonymisierung und Anonymisierung von Datenquellen allgemeinhin akzeptiert werden und zulässig sind.

Eine Anonymisierung von Gesundheitsdaten, nach der das Re-Identifizierungsrisiko dauerhaft ausgeschlossen ist, ist häufig nur bei einem gleichzeitigen Verlust der Aussagekraft der Daten möglich. Datensätze können allerdings durch bewährte Maßnahmen so verändert werden, dass nach allgemeinem Ermessen wahrscheinlich keine Mittel mehr für eine Re-Identifizierung zur Verfügung stehen, sofern diese in einer kontrollierten IT-Umgebung verarbeitet werden. Im Gegensatz dazu wird die öffentliche Verfügbarmachung anonymisierter Datensätze nur in Ausnahmefällen möglich sein.

8. Zertifizierungen für Datenverarbeiter

Die Datensilos für Gesundheitsdaten werden durch die aktuellen Initiativen endlich aufgebrochen. Neben dem FDZ und der für den EHDS vorgesehenen Forschungsinfrastruktur wird es andere Research Data Hubs geben, die Gesundheitsdaten für die Forschung verfügbar machen und aufbereiten werden. Für diese Akteure sollten spezifische, ggf. freiwillige, Zertifizierungsmöglichkeiten bestehen.

Zertifizierungen stellen ein einheitliches Datenschutz- und Sicherheitsniveau sicher und schaffen Vertrauen. Eine Zertifizierung sollte jedoch nicht dem Selbstzweck dienen, sondern die zertifizierte Stelle auch ausdrücklich datenschutzrechtlich berechtigen, die Gesundheitsdaten für die ihrer Funktion entsprechenden privilegierten Zwecke zu nutzen. Eine Zertifizierungspflicht, bei der für die Datenverarbeiter trotz der Erfüllung aller Zertifizierungsanforderungen weiterhin (datenschutz-)rechtliche Unsicherheiten bestehen, bindet weitere Ressourcen der Datenverarbeiter und wird die Entwicklung forschungsfördernder Geschäftsmodelle lähmen.

9. Souveräne europäische Datenverarbeitungsstrukturen

Souveräne Datenverarbeitungsstrukturen in Deutschland und Europa müssen stärker gefördert werden. Die datenschutzrechtlichen Diskussionen und gerichtlichen Verfahren rund um die Übermittlung von personenbezogenen Daten in Drittländer beim Einsatz von Dienstleistern, deren Konzernmutter nicht innerhalb der EU sitzt, bedeuten unkalkulierbare Risiken für die Akteure im Gesundheitsbereich. Diese Risiken beruhen jedoch auch auf

reellen Gefahren für den Schutz der Privatsphäre und die Durchsetzung unserer deutschen und europäischen Werte und sind somit keineswegs unbeachtlich. Die Diskussionen über den Drittlandsdatentransfer werden erst enden, wenn souveräne, europäische Datenverarbeitungsstrukturen nicht nur datenschutzrechtlich die bessere Alternative sind, sondern auch mindestens ebenso leistungsfähig wie die internationale Konkurrenz. Um dieses Ziel zu erreichen, bedarf es gezielter Wirtschaftsförderung und regulatorischer Maßnahmen, die die Datenübermittlung von Gesundheitsdaten in Drittländer zum angemessenen Schutz dieser Daten nur in Ausnahmenfällen erlauben.

Berlin, den 17. März 2023

Honic – Daten für eine bessere Medizin

Honic entwickelt eine DSGVO-konforme Plattform für medizinische Gesundheitsdaten, die Forschung und Entwicklung auf Basis von Versorgungsdaten ermöglicht. Die Honic Plattform, eine unternehmerische Lösung *made in Germany* entsteht mit starken Partnern in enger Zusammenarbeit mit der Datenschutzaufsicht. Durch *Security by Design* und in Abstimmung mit der IT-Sicherheitsszene wird ein Höchstmaß an Datensicherheit erreicht.

Das Honic Team verbindet jahrzehntelange Erfahrung in Gesundheitswesen, Regulatorik, Gesundheitsdatenschutz und digitaler Medizin mit fundiertem Know-How bei der Entwicklung digitaler Technologien und Lösungen. Renommierte Mediziner:innen sind Teil des interdisziplinären Teams ebenso wie Digital Health Pioniere, Datenschutzexpert:innen und Architekt:innen komplexer Plattform-Lösungen.

secunet – Schutz für digitale Infrastrukturen

secunet ist Deutschlands führendes Cybersecurity-Unternehmen. In einer zunehmend vernetzten Welt sorgt das Unternehmen mit der Kombination aus Produkten und Beratung für widerstandsfähige, digitale Infrastrukturen und den höchstmöglichen Schutz für Daten, Anwendungen und digitale Identitäten. secunet ist dabei spezialisiert auf Bereiche, in denen es besondere Anforderungen an die Sicherheit gibt – wie z. B. Cloud, IIoT, eGovernment und eHealth. Mit den Sicherheitslösungen von secunet können Unternehmen höchste Sicherheitsstandards in Digitalisierungsprojekten einhalten und damit ihre digitale Transformation vorantreiben.

Über 1000 Expert*innen stärken die digitale Souveränität von Regierungen, Unternehmen und der Gesellschaft. Zu den Kunden zählen die Bundesministerien, mehr als 20 DAX-Konzerne sowie weitere nationale und internationale Organisationen. Das Unternehmen wurde 1997 gegründet. Es ist im SDAX gelistet und erzielte 2022 einen Umsatz von rund 345 Mio. Euro (vorläufiges Ergebnis, Stand: 23. Januar 2023). secunet ist IT-Sicherheitspartner der Bundesrepublik Deutschland und Partner der Allianz für Cyber-Sicherheit.