

Gesundheitsdatennutzungsgesetz GDNG - Inhalte

Leitgedanken

1. Der aktuelle Vorschlag der EHDS-Verordnung deckt in Bezug auf die Sekundärnutzung von Gesundheitsdaten nur einen singulären spezifischen Prozess ab (einwilligungsfrei und über staatliche Zugangsstellen). Das GDNG sollte jedoch einen **holistischen Rahmen** schaffen, um möglichst für alle Arten von Gesundheitsdaten deren unterschiedliche Verarbeitung, Aggregation, Speicherung, und Übermittlung zur anschließenden primären und sekundären Nutzung für unterschiedliche Nutzergruppen und Anwendungsfelder **eindeutig zu unterscheiden und damit regulatorisch abzubilden**.¹
2. Deutschland hat in seiner föderalen Struktur mit teilweise mangelhaft aufeinander **abgestimmten Landesgesetzen** Schwierigkeiten, Nutzungskonzepte von Daten **national oder europäisch zu skalieren**, und erleidet so erhebliche Nachteile in der Qualität der Versorgung, der Effizienz des Einsatzes der knappen personellen und finanziellen Ressourcen sowie der Wettbewerbsfähigkeit der nationalen Gesundheitswirtschaft, nicht zuletzt auch im Hinblick auf die Resilienz, die verstärkt im Fokus steht.²

Um diese Leitgedanken umzusetzen, sollte das GDNG folgende Aspekte abdecken:

- Klare **Bezeichnung und Definition der Elemente** eines Datenraums zur Nutzung von Gesundheitsdaten. Dies ermöglicht auch die Strukturierung der politischen Debatte über die aktuelle und zukünftige Regulierung der Datennutzung.
- **Patientenzentrierte standardisierte Einwilligung** zur „Verschaltung“ beliebiger Nutzungsszenarien über einwilligungsfreie Forschung hinaus, sowohl durch Opt-in als auch Opt-out.
- Konkrete **Spezifikation der Prozesse, Strukturen** und (eventuell in Form von Durchführungsvorschriften) **Kriterien** für die vorgenannten Elemente der Datenverarbeitung. Dies begünstigt verantwortungsvolle Datennutzung im Sinne des Patienten durch regulatorische „Leitplanken“ und schafft Rechtssicherheit und Konsistenz bei der Auslegung durch einzelne Landesdatenschutzbehörden (insbesondere bei Nutzungsszenarien, die in der Praxis die Datennutzung behindern).
- **Harmonisierung** der Landesgesetze, insbesondere der Landeskrankenhausgesetze
- **Abstimmungsverfahren der Landesdatenschutzbehörden** für Unstimmigkeiten in konkreten Anwendungsfällen
- **Redaktionelle Anpassungen** einzelner Gesetze zur Erhöhung der Rechtssicherheit

¹ SVR v. 24. März 2021, „Digitalisierung für Gesundheit“, Empfehlung Nr. 23, S. 30

² Acatech v. 25. Februar 2021, „Resilienz und Leistungsfähigkeit des Gesundheitswesens in Krisenzeiten“

Inhaltsvorschläge

1. Definitionen

In der Diskussion über Gesundheitsdatenräume gibt es eine Vielzahl von Begriffen, die teilweise in nationalen oder EU-Rechtsnormen (manchmal auch uneinheitlich und widersprüchlich) definiert sind, teilweise aber auch sehr diffus der allgemeinen politischen Diskussion entstammen (wie beispielsweise „Datentreuhänder“). Aus diesem Grunde sollte im GDNG durch Verweise auf bestehende Rechtsnormen oder Definition neuer Elemente und Institutionen eine Struktur vorgegeben werden, die nicht nur für die Regelungen des GDNG hilfreich sind, sondern auch in den Prozessen, die das Gesetz aktuell oder zukünftig durch Erweiterungen und Rechtsnormen beschreiben soll, für Klarheit sorgen kann.

- **Forschung:** In Anlehnung an Erwägungsgrund 159 DSGVO sollte eine Definition der Forschung erfolgen, die sowohl private als auch öffentlich-rechtliche Forschung umfasst und auch die Entwicklung von Produkten und deren Weiterentwicklung einschließt.
- **Nutzungsfreigabestruktur:** Struktur zur Definition, welche Nutzergruppe welchen Datentyp in welchem klinischen Anwendungsbereich mit welchem Datenzugangsmodus und welchem Datenspeicherkriterium nutzen darf.
- **Datennutzergruppe:** Abstrakte Einteilung aller möglichen Datennutzer in gleichberechtigte Gruppen anhand objektiver Kriterien.
- **Datentyp:** Unterscheidung von Abrechnungs- und Sozialdaten, Bilddaten, klinischen Daten, Sensor- oder „Real-World-Daten“ und Biomaterialien und aus diesen abgeleiteten genetischen Daten. Innerhalb dieser Haupttypen gibt es weitere Unterscheidungen, wie beispielsweise Basisdaten und erweiterte Datensätze.
- **Klinischer Anwendungsbereich:** Unterscheidet wesentliche klinische Bereiche in einer auch für Patienten verständlichen Form.
- **Datenzugangsmodus:** Unterscheidet zwischen Abfrage aggregierter Daten, Zugang zu pseudonymisierten oder anonymisierten Daten, oder Übermittlung derselben.
- **Datenspeicherkriterium:** Die Speicherung kann nur für die Dauer der direkten Verarbeitung erfolgen, 90 Tage, 3 Jahre, oder 5 Jahre.
- **Zusätzliche Einwilligungskriterien:** Patienten können in eine Re-Kontaktierung über Fragebögen einwilligen oder den Zugang zu Daten der mentalen und sexuellen Gesundheit einschränken.
- **Pseudonymisierung:** Die identifizierenden Daten (IDAT) sind durch ein anderes Identifikationsmerkmal, ein Pseudonym (beispielsweise mit anerkannt sicheren Hash-Verfahren oder anerkannt sicheren Zufallsgeneratoren), ersetzt, um die Feststellung der Identität des Betroffenen auszuschließen. Nicht ausreichend sind hingegen Verfahren, welche nach gegenwärtigem Stand der Technik mit vertretbarem Zeitaufwand rückaufgelöst werden können und somit zum Zeitpunkt der Verwendung als reversibel gelten, wie etwa die Verfahren MD5 und SHA1.
- **Anonymisierung:** Daten können nur mit unverhältnismäßig großem Aufwand einer bestimmbar Person zugeordnet werden.
- **Zugangsstelle im Sinne des EHDS-VO-E:** Öffentliche Stelle, die gemäß Art. 36 ff EHDS-VO-E u.a. dafür zuständig ist, (i) Anträge von Datennutzern zu bearbeiten, (ii) elektronische Gesundheitsdaten zu speichern, zu verarbeiten und ggf. zu

pseudonymisieren sowie (iii) den tatsächlichen Zugang für die Sekundärnutzung zu gewähren. Diese Aufgaben sollten auf getrennte (ggf. private) Stellen verteilt werden:

- **Antragsstelle:** Einrichtung, welche die Anträge von Datennutzern für jede Form des Zugangs zu Gesundheitsdaten bearbeitet (d.h. abweichend von der „Zugangsstelle“ gemäß EHDS-VO-E speichert die Antragsstelle selbst keine elektronischen Gesundheitsdaten).
- **Registerstelle:** Datenregister zur Speicherung der Daten, die in der Nutzungsfreigabestruktur spezifiziert ist und ausschließlich Daten speichern darf, die durch die Pseudonymisierungsstelle pseudonymisiert wurden (d.h. abweichend von der „Zugangsstelle“ gemäß EHDS-VO-E bearbeitet die Registerstelle selbst keine Nutzungsanträge).
- **Pseudonymisierungsstelle:** Rechtlich, organisatorisch, und technisch von der verarbeitenden Stelle unabhängige Stelle zur Pseudonymisierung.
- **Datenintegrationszentrum:** Die aus der MII weiterentwickelte Struktur, um Daten innerhalb einer Gesundheitseinrichtung aus unterschiedlichen Datenquellen für die Sekundärnutzung zu aggregieren.
- **Datengenerierende Einrichtung:** Gesundheitseinrichtung, die Patientendaten erfasst.

2. Patientenzentrierte standardisierte Einwilligung

Im GDNG sollte spezifisch geregelt werden, wie Daten mit Einwilligung des Patienten genutzt werden können.

- Eine Nutzungsfreigabestruktur ist so zu definieren, dass sich jedes Nutzungsvorhaben eindeutig einem einwilligungsfreien oder einem einwilligungsbasierten Zugang zuordnen lässt.
- Für den Patienten muss transparent sein, unabhängig von der Art der erfassten digitalen Daten, welcher Datentyp von welcher Datennutzergruppe für welchen klinischen Anwendungsbereich in welchem Datenzugangsmodus und zu welchen Datenspeicherungskriterien einwilligungsfrei oder aufgrund einer Einwilligung des Patienten genutzt werden kann.
- Diese Transparenz muss auch abbilden, für welche Nutzungsszenarien eine Freigabe spezifisch erteilt werden muss (Opt-in) oder als erteilt gilt und konkret widerrufen werden muss (Opt-out). Die beschriebene Einwilligungsstruktur regelt die Verarbeitung ausschließlich, und Erweiterungen oder Einschränkungen einer Einwilligung sind nicht gestattet sind, da eine sinnvolle Verwaltung der Einwilligungsparameter sonst nicht möglich ist.

3. Governance

Um das Vertrauen der Patienten in die Nutzung von Gesundheitsdaten zu erhöhen, sollten folgende „Leitplanken“ definiert werden:

- Strafen für den Versuch der Re-identifizierung pseudonymisierter oder anonymisierter Gesundheitsdaten
- Verbot von Exklusivitätsverträgen bzgl. des Datenzugangs

- Angemessenes (ggf. gedeckeltes) Entgelt für die Speicherung und Weitergabe von Daten
- Möglichkeit, die Datenzugangspflicht aus guten Gründen für bis zu 24 Monate einzuschränken
- Weitergabe von Daten außerhalb von Gesundheitseinrichtungen mindestens pseudonymisiert, wenn möglich aber anonymisiert
- Jede Form der Datennutzung muss den hier beschriebenen Prozess über die oben definierten (privaten) Stellen (Pseudonymisierungsstelle, Registerstelle, Antragsstelle) durchlaufen.
- Unternehmen, die Gesundheitsdaten nutzen wollen, müssen ein zertifiziertes Qualitätssicherungssystem unterhalten (und somit strukturierte Entwicklungs- und Schulungsprozesse nachweisen). Für eine Übergangszeit von 24 Monaten kann eine eidesstattliche Versicherung ausreichen, dass die Zertifizierung in Vorbereitung ist.
- Jede Sekundärnutzung von Biomaterialien und daraus resultierenden genetischen Daten ist nur nach einer Freigabe durch eine Ethikkommission möglich.

4. Datennutzergruppe

Im Rahmen einer Datenfreigabe sollten die auszuwählenden Datennutzer in Gruppen von Nutzern nach objektiven Kriterien unter einem Begriff zusammengefasst werden, um für die Patienten eine handhabbare Transparenz herzustellen. Dadurch bleibt einerseits die Komplexität der Nutzungsfreigabestruktur überschaubar, andererseits werden einzelne Nutzer nicht spezifisch privilegiert. Eine Nutzungsfreigabe kann beispielsweise nicht für ein einzelnes Unternehmen erfolgen, sondern z.B. nur für alle Medizinproduktehersteller der an der Behandlung des Patienten beteiligten Produkte.

Diese Zugehörigkeit spezifischer Nutzer zu bestimmten Gruppen kann auch von einer Antragsstelle bestätigt werden. Die Nutzer und deren Gruppenzugehörigkeit müssen dann auf der Website aller Registerstellen (inklusive der entsprechenden Kontaktdaten) aufgeführt werden.

5. Klinischer Anwendungsbereich

Sinnvollerweise enthält eine Nutzungsfreigabe keine Einschränkungen hinsichtlich des klinischen Bereichs, in dem mit den Daten geforscht werden darf, da sich so besser Zusammenhänge unterschiedlicher Erkrankungen analysieren lassen. In der Realität sind jedoch nicht alle Patienten bereit, Daten für jeden klinischen Anwendungsfall zu teilen. Diese Herausforderung ließe sich wie folgt lösen:

- Um Datentypen klar zu definieren, sollte das RKI jedem klinischen Anwendungsbereich eine oder mehrere Fachgesellschaften zuordnen. Diese Fachgesellschaften können dann einen Basisdatensatz von minimal erforderlichen Daten erarbeiten, die für Qualitätskontrolle und statistische Auswertungen in dem jeweiligen Bereich erforderlich sind und für alle Patienten zu erheben sind.
- Darüber hinaus spezifizieren diese einen erweiterten optionalen Datensatz, der möglichst international kompetitiv hinsichtlich Struktur, Granularität, und Format sein sollte.

- Der erweiterte Datensatz kann auch diagnostische und pathologische Bilddaten, Sensordaten und andere „Real-World-Daten“, sowie vom Patienten in Form von PROMS erhobene Daten enthalten.
- Beide Datensätze, der Basisdatensatz und der erweiterte Datensatz, können auch Elemente anderer Erkrankungen erhalten, wie beispielsweise Diabetes oder Demenz, soweit sie für die Behandlungsentscheidung, Prognose, oder Beurteilung des Ergebnisses der Behandlung und eventueller Nebenwirkungen oder Komplikationen nachgewiesenermaßen (Evidenzstufe 1) relevant sind.
- Diese Datensätze werden in FHIR-Format spezifiziert und auf der Website des RKI sowohl als technisches Format als auch in für Patienten verständlicher Form veröffentlicht. Diese Seite wird dann mit der Informationsseite der Antragsstellen verlinkt.

6. Pseudonymisierungsstelle

In § 9 IRegG ist der Prozess einer Pseudonymisierungsstelle bereits sinnvoll beschrieben. Die Ausgestaltung sollte wie folgt erweitert werden:

- Neben dem RKI können auch weitere Pseudonymisierungsstellen entstehen, die zur Erhöhung des Datenschutzniveaus organisatorisch, räumlich, rechtlich, und technisch von Registerstellen und datengenerierenden Einrichtungen getrennt sein müssen
- Die Einwilligung in die Pseudonymisierung sollte im Regelfall eine Migration der Pseudonymisierungsstelle zu einer anderen Pseudonymisierungsstelle abdecken
- Nicht erlaubt sein sollten Pseudonyme, die in rechnerischem Zusammenhang mit den tatsächlichen, patientenidentifizierenden Daten stehen
- Bei der Datenübermittlung an die Pseudonymisierungsstelle sollten die letztendlich für die Registerstelle bestimmten elektronischen Gesundheitsdaten zur Erhöhung des Datenschutzniveaus nicht Bestandteil des Datenpaketes sein, auch wenn sie gesondert verschlüsselt wären
- Die Pseudonymisierungsstelle soll eine Rückauflösung der Pseudonymisierung zum Zweck der Datenerfassung und Qualitätssicherung (Überprüfung / Ergänzung der zuvor übermittelten Gesundheitsdaten), zur Unterstützung bei der Umsetzung der Rechte betroffener Personen (Löschung, Einschränkung der Verarbeitung, Korrektur und Einsichtnahme), zur Kontaktierung der Patienten (beispielsweise für prä- oder post-operative Online-Befragungen oder für die Modifikation von Einwilligungen, soweit der Patient dazu eingewilligt hat), sowie zur Rückübertragung von Daten an die behandelnde Gesundheitseinrichtung ermöglichen
- Perspektivisch sollte eine multinationale EU-Stelle etabliert werden
- Pseudonymisierungsstellen ab 1. Million Patienten sollten zur multinationalen EU-Stelle migrieren müssen
- Es sollte ein Regelwerk sowie ein Registrierungs- bzw. Auditregime für Pseudonymisierungsstellen definiert werden

7. Anonymität

Es gibt bei der Beurteilung von Anonymität sehr unterschiedliche Auslegungen, insbesondere bei der Verwendung von Bilddaten. Folgende Klarstellungen sollen Rechtsicherheit schaffen:

- Daten, auch Bilddaten, gelten als anonym, wenn sie mithilfe von öffentlich zugänglichen weiteren Daten nicht einer Person zugeordnet werden können
- 3D Bilddaten, die auch das Gesicht der Patienten erfassen, können nur dann als anonymisiert gelten, wenn sie so verfremdet wurden, dass sie auch mit biometrischen Verfahren nicht der Person zugeordnet werden können (beispielsweise online zugänglichen Bildern der jeweiligen Person).
- Aggregierte Daten gelten dann als anonym, wenn die Daten aus mindestens 100 Einzeldatensätzen aggregiert wurden
- Einzeldatensätze gelten als anonym, wenn die spezifischen Datenfelder des Datensatzes so gewählt wurden, dass mindestens 100 Patienten einer Abfrage dieselben Daten liefern

8. Antragsstelle

Es sollte ein regulatorischer Rahmen für das Entstehen mehrerer, eventuell regionaler, Antragsstellen (in den bisherigen Rechtsnormen auch als Zugangsstelle bezeichnet) geschaffen werden. Das sollte folgende Kriterien umfassen:

- Registrierungs- und Zertifizierungsprozesse (beispielsweise unabhängig und „not-for-profit“), ähnlich wie für benannte Stellen für CE-Zertifizierungen. Die im Rahmen der Medizin-Information-Initiative (MII) geleistete konzeptionelle Vorarbeit sollte miteinfließen und das Konzept weiterentwickelt werden.
- Die Antragsstelle sollte digitale (zeitliche begrenzte) Zertifikate ausstellen. Das kann im Rahmen eines Antrags erfolgen, oder bestimmte Aspekte separat abbilden, wie beispielsweise die Zugehörigkeit einer bestimmte Nutzergruppe, die dann nicht immer wieder erneut geprüft werden muss.
- Zu regeln sind die erforderlichen Elemente eines Antrags und Kriterien zur eventuell notwendigen Interessensabwägung.
- Eine Zielvorstellung wäre das Entstehen von 5-6 nationalen Antragsstellen (beispielsweise an der Universität Greifswald, Charité, Universitätsklinik Essen, dem Leibnitz-Rechenzentrum in München).
- Die Antragsbearbeitung erfolgt grundsätzlich gegen angemessene Gebühr, sollte aber im GDNG für zumindest die ersten 5 Jahre für KMUs und klinische Fachgesellschaften kostenfrei sein.
- Die genehmigten Nutzungsanträge müssen inklusiver der Details der Nutzungsfreigabestruktur auf der Website der Registerstelle inklusive der genehmigenden Antragsstelle aufgeführt werden.

9. Cloud-Datenspeicherung

Pseudonymisierte und verschlüsselte Daten gelten nicht als personenbezogen, und dürfen von den datenerhebenden Gesundheitseinrichtungen auch in Cloud-Lösungen Nicht-EU-basierter Hyperscaler gespeichert werden, soweit die Server in der EU stehen. Soweit also eine Verarbeitung von pseudonymisierten und verschlüsselten Daten durch die behandelnde Klinik erlaubt ist, darf dies auch Cloud-basiert erfolgen, soweit die Partition unter der Kontrolle dieser Gesundheitseinrichtung ist. Auch eine Verarbeitung anonymisierter Daten durch einen externen Cloudservice ist ohne zusätzliche Einwilligung möglich, soweit die Verarbeitung

selbst erlaubt ist, vorausgesetzt die Daten werden vom externen Anbieter über die Verarbeitung hinaus nicht gespeichert.

10. Einwilligungsfreie Nutzung

Im GDNG sollte die Verarbeitung und Speicherung in bestimmten Datennutzungsszenarien geregelt werden, die auch ohne Einwilligung erfolgen kann, teilweise an bestimmte, näher spezifiziert Einschränkungen geknüpft:

- Übertragung aller bereits innerhalb der letzten 24h erhobenen Daten der ambulanten Erstversorger an die Notaufnahme einer stationären Gesundheitseinrichtung
- Erfassung, Verarbeitung, und Speicherung aller Gesundheitsdaten durch die behandelnde stationären Gesundheitseinrichtung, mit einer auf 90 Tage nach der Entlassung begrenzten Speicherdauer
- Nutzung traumatologischer und Intensivmedizinischer Basisdaten durch die klinischen Fachgesellschaften im jeweiligen Bereich (beispielsweise für Register), insbesondere inklusive der Daten von Patienten, die aufgrund ihres Gesundheitszustandes keine entsprechende Einwilligung abgeben können
- Basisdaten für Register von Implantaten (entsprechend dem IRegG)
- Zugang (für beliebige Nutzergruppen) zu aggregierten Basisdaten aus den jeweils während der letzten fünf Jahre erfassten Gesundheitsdaten, soweit sie für die Qualitätsbewertung stationärer Gesundheitseinrichtungen nötig sind (ggf. in einer ministeriellen Verordnung im Einzelnen festzulegen)
- Zugang für Gesundheitsämter und RKI zu aggregierten Daten aus den jeweils während der letzten drei Jahre erfassten Gesundheitsdaten, soweit sie für die Beurteilung und Kontrolle von Pandemien nötig sind (ggf. in einer ministeriellen Verordnung im Einzelnen festzulegen)

11. Nicht erlaubte Nutzung

Die Nutzungsfreigabestruktur kann auch die Szenarien abdecken, die nicht erlaubt sein sollen, um den Patienten vor der Abgabe einer Einwilligung zu schützen, die eventuell gegen dessen Interessen ist und deren Folgen er nicht vollständig überblicken kann. Insbesondere folgende Szenarien sind nicht erlaubt, entsprechende Einwilligungen wären ungültig (und auch eine einwilligungsfreie Nutzung wäre konsequenterweise nicht möglich):

- Speicherung der für Sekundärnutzung übermittelten Einzeldatensätze genetischer Daten über eine Speicherdauer von 90 Tagen hinaus
- Zugang zu Einzeldatensätzen für Nutzer, die auch Daten für Profilbildung erheben (insbesondere durch Suchmaschinenabfragen, Sprachverarbeitung, und Positionsdaten) und diese über eine Frist von 90 Tagen hinaus speichern

12. Vereinheitlichung der Landesrechte / Kompetenzen

Langfristig sollten die unterschiedlichen Vorgaben der Bundesländer für die Forschung angeglichen und einheitliche Kompetenzen geschaffen werden. Dies erfordert gemeinsame Anstrengungen von Bund und Ländern und wird mit dem ersten Entwurf des Gesundheitsdaten-Nutzungsgesetzes vielleicht nicht zu erreichen sein. Allerdings können

bereits bestehende Regelungen ins GDNG überführt werden, insbesondere § 287a SGB V. So ließen sich die Zweifel der Datenschutzbehörden an der Anwendbarkeit aufgrund der bisherigen Lokalisierung im Sozialgesetzbuch überwinden.

- Zusätzlich müsste der Auftrag aus dem Koalitionsvertrag in Angriff genommen werden, die Entscheidungskompetenz der Datenschutzkonferenz zu stärken, damit die analoge Anwendung der Art. 56, 60 DSGVO auch im GDNG zur Abbildung kommen kann. Dies erfordert einen intensiveren Blick auf die Gesetzgebungskompetenz des Bundes. Hierzu liefern wir gern im Laufe des Januars weitere Überlegungen.
- Möglicherweise könnte die Bund-Länder-Arbeitsgruppe durch einen Formulierungsvorschlag für Regelungen zur Forschung in den Landesdatenschutz- / Landeskrankenhaus- / Landeskrebsregistergesetzen die Basis für eine Konsolidierung schaffen.
- Für die länderübergreifenden Vorhaben der Gesundheits- und Versorgungsforschung könnte erstmalig probatorisch im Gesetz die Möglichkeit geschaffen werden, von einer Behörde eine verbindliche Auskunft für ein Forschungsvorhaben einholen zu können.

13. Aufhebung der Unterscheidung zwischen privat und öffentlich finanzierter Forschung

Die Benachteiligungen der privatwirtschaftlichen Forschung sollten aufgehoben werden, um ihr einen gleichberechtigten Rahmen zu geben und das Forschungspotenzial zu heben, insbesondere:

- §§ 64e Abs. 11, 303e SGB V
 - Erweiterung der Nutzungsberechtigten auch auf private Einrichtungen und Personen
 - Definition und Präzisierung der Anforderungen an einen Antrag
 - Überarbeitung/Überführung weiterer Verweismormen, z.B. § 8 Datentransparenz-Verordnung
- § 363 SGB V
 - Klarstellung in Abs. 8 SGB V: „bestimmte Zwecke oder Arten von Zwecken“
 - Ergänzung der Freigabe an Datenvermittlungsdienste (der Begriff des „Datentreuhänders“ ist gesetzlich nicht definiert, wird uneinheitlich verwendet und sollte daher vermieden werden)
 - Klarstellung Anforderungen an „Informiertheit“
- § 27 BDSG
 - Streichung „erhebliches“ Überwiegen des Forschungsinteresses (unbestimmter Rechtsbegriff, der nicht ausgefüllt werden kann) zugleich Klarstellung, dass Überwiegen dann anzunehmen ist, wenn Re-identifikation nahezu ausgeschlossen ist, vergleiche Erwägungsgrund 26 DSGVO).
- § 203 StGB
 - Ausnahme gem. Abs. 3 ergänzen, dass zulässige Forschung (nach § 27 BDSG oder GDNG) keine Strafbarkeit nach § 203 StGB begründet

14. Interoperabilität

Das Recht auf Einsichtnahme in die Patientenakte sollte um einen Datentransferanspruch in einem interoperablen, international anerkannten Format (z.B. FIHR) erweitert werden (sichert Transparenz der Sekundärdatennutzung und Informiertheit der Einwilligung)

- Öffentlich-rechtliche und privatwirtschaftliche Vorhaben der Datennutzung müssen im Grundsatz Interoperabilität mit international anerkannten Formaten sicherstellen.
- Formate für Datenübertragung können staatlich (gematik) definiert werden, Übertragungsmodalitäten und Auswahl von Hardware wie z.B. Konnektoren auf der Basis dieser Standards, können von den Beteiligten frei gewählt werden.

15. Umsetzung des Data Governance Acts

Die Definition des Datenvermittlungsdiensts ist ergänzungsbedürftig. Sie sollte konkreter fassen, was unter einem solchen Dienst zu verstehen ist.

- Es bedarf auch der Definition von Maßnahmen, wie bei einem Datenvermittlungsdienst der Interessenskonflikt zwischen Datenvermittlung und Datenforschung verhindert werden kann (zusätzliche Anforderungen, Antragsstellen, Abhängigkeit von Datenarten, insb. als Alternative zur im DGA dargestellten rechtlichen Trennung von Datenvermittlung und Datenforschung)

16. Kritikpunkte zu dem EHDS-Entwurf

Hierzu möchten wir auf unseren Kommentar zum EHDS-VO-E verweisen. Problematisch sind insbesondere folgende Punkte:

- eine einwilligungsfreie Sekundärnutzung von Gesundheitsdaten, die einem Kontrollverlust der Betroffenen gleichkommt,
- die Anwendbarkeit der Offenlegungspflicht auf alle, auch durch private Akteure kostenintensiv gesammelten elektronischen Gesundheitsdaten,
- die völlige staatliche Kontrolle des Zuganges zu elektronischen Gesundheitsdaten, welche auch die Gefahr der Zusammenführung mit anderen Daten birgt, sowie
- die Zerstörung der Motivation für die Wirtschaft und Forschung, durch gut strukturiert erhobene Daten einen Vorsprung zu erhalten.

EHDS im Übrigen:

- Einschlägigkeit Art. 14 Abs. 3: „allgemeine Software, die im Gesundheitswesen verwendet wird“ in Art. 14 Abs. 2 ist zu weit gefasst; Hersteller von Medizinprodukten, die geltend machen, dass sie mit EHR-Systemen interoperabel sind, müssen nach Art. 14 Abs. 3 die Einhaltung der Anforderungen an die Interoperabilität gemäß Anhang II Abschnitt 2 der VO nachweisen. Unklar ist hier, was unter „geltend machen“ zu verstehen ist. Naheliegender wäre, dass die Vorgaben zumindest dann nicht gelten sollen, wenn man nicht mit der Interoperabilität wirbt. Idealerweise sollte klargestellt werden, dass die bloße Interoperabilität den Anwendungsbereich der Normen noch nicht eröffnen soll. In diesem Zuge wäre auch klarzustellen, wann sonstige Dritte, deren Systeme bereits interoperabel sind, den Vorgaben der Art. 14 ff. unterfallen.
- Eine einwilligungsfreie Verarbeitung von elektronischen Gesundheitsdaten sollte ausschließlich dann gestattet sein, wenn diese Daten dergestalt anonymisiert sind, dass sie auch unter Einsatz jeglicher denkbaren Mittel nicht rückaufgelöst werden können.
- Auf zahlreiche weitere Punkte des EHDS-VO-E, wie das Verhältnis zum Datenbankherstellerrecht (§ 87c I Nr. 2 UrhG), gehen wir derzeit noch nicht ein, da wir davon ausgehen, dass im Verordnungsentwurf noch Änderungen vorgenommen werden.