Gesundheit digital
BDI initiativ

BDI-INITIATIVE GESUNDHEIT DIGITAL

Nutzung von Gesundheitsdaten: Brauchen wir ein Trust-Center?

Herausforderungen und Chancen aus Sicht der industriellen Gesundheitswirtschaft

Personenbezogene Gesundheitsdaten müssen für die Nutzung verfügbar gemacht werden.

Personenbezogene Gesundheitsdaten sind ein großes und bislang hauptsächlich ungenutztes Potenzial für die Gesundheitsversorgung. Aus rechtlichen, politischen und finanziellen Gründen ist der Großteil dieser Daten heute in Deutschland noch nicht für die Nutzung in der industriellen Gesundheitswirtschaft verfügbar. Durch die Nutzung können neue Erkenntnisse über die Gesundheit der Bevölkerung, unterschiedliche Erkrankungen und Behandlungsmethoden gewonnen werden.

Die industrielle Gesundheitswirtschaft spricht sich für die Implementierung eines bundesweiten Trust-Centers in Deutschland aus.

Ein Trust-Center verknüpft und verwaltet personenbezogene Gesundheitsdaten und macht sie nach einem Prozess der Verschlüsselung, Entschlüsselung und einer Datenzugriffsregelung in einer hohen Qualität verfügbar. Dies ermöglicht es der Wirtschaft und anderen forschenden Institutionen qualitativ hochwertige, strukturiert aufbereitete und aktuelle Gesundheitsdaten für die Forschung und Entwicklung zu nutzen.

Die industrielle Gesundheitswirtschaft ruft zur Zusammenarbeit mit der BDI-Initiative Gesundheit digital auf.

Die Datennutzung und die Implementierung eines bundesweiten Trust-Centers sind nur durch eine Zusammenarbeit der unterschiedlichen Akteure des Gesundheitssystems möglich. Deshalb lädt die iGW in der BDI-Initiative Gesundheit digital die Politik, Wirtschaft, Wissenschaft, Leistungserbringer, gesetzliche Krankenkassen und alle anderen interessierten Akteure ein, zusammen eine Lösungsskizze für die Implementierung eines bundesweiten Trust-Centers für die Datennutzung von personenbezogenen Gesundheitsdaten zu erarbeiten.

Ben Mayer | BDI-Initiative Gesundheit digital | T: +49 30 20281570 | b.mayer@ifg.bdi.eu | www.bdi-gesundheit-digital.eu

Inhaltsverzeichnis

Datennutzung

Personenbezogene Gesundheitsdaten sind ein großes und bislang hauptsächlich ungenutztes Potenzial für die Gesundheitsversorgung.[1,2] Die Nutzung von personenbezogenen Gesundheitsdaten aus der ambulanten und stationären Versorgung, von den gesetzlichen Krankenkassen und aus anderen Bereichen kann neue Erkenntnisse zu effizienten Behandlungsmethoden, einer optimierten Versorgung sowie innovativen Forschungshypothesen ermöglichen.[3,4]

Dennoch ist der Großteil dieser Daten aus rechtlichen, politischen und finanziellen Gründen heute in Deutschland noch nicht für die Nutzung in der industriellen Gesundheitswirtschaft verfügbar. Der Bereich „Datennutzung“ beleuchtet die notwendigen Voraussetzungen für die Nutzung von personenbezogenen Gesundheitsdaten. Der Problemaufriss hat das Ziel, die Probleme und offenen Fragen rund um die Datennutzung aus Sicht der industriellen Gesundheitswirtschaft aufzubereiten. Detaillierte technische Fragestellungen, wie zum Beispiel zur Interoperabilität und zu unterschiedlichen Standards zum Datenaustausch, sind nicht Teil dieses Problemaufrisses.

Dieser Problemaufriss wird das Themenfeld „Datennutzung“ anhand der Fallstudie eines Trust-Centers für Gesundheitsdaten veranschaulichen. In der Folge wird das Trust-Center für personenbezogene Gesundheitsdaten entlang von Best-Practice-Beispielen sowie strukturellen, rechtlichen und infrastrukturellen Umsetzungshürden und Fragestellungen dargestellt. Der Problemaufriss endet mit kurz- und mittelfristigen Lösungsempfehlungen an die Politik und andere Akteure des Gesundheitssystems.

Veranschaulichung der Datennutzung: Trust-Center

Was ist ein Trust-Center und warum ist es wichtig?

Ein Trust-Center bietet Leistungen zur Datenqualität, Datenverarbeitung und zum Datenmanagement von personenbezogenen Gesundheitsdaten und macht sie nach einem Prozess der Verschlüsselung, Entschlüsselung und einer Datenzugriffsregelung in einer hohen Qualität verfügbar. Dies ermöglicht es der Wirtschaft und anderen forschenden Institutionen, qualitativ hochwertige, strukturiert aufbereitete und aktuelle Gesundheitsdaten für die Forschung und Entwicklung zu nutzen.[5] Technologisch sind eine Vielfalt von Bereitstellungsmodellen und Plattformservices für die Implementierung eines Trust-Centers möglich: Beispielsweise können die personenbezogenen Daten entweder zentral oder dezentral mit einem Cloud-Dienst gespeichert werden. Ein Trust-Center verknüpft Gesundheitsdaten aus mehreren heterogenen und geographisch verteilten Datenquellen und bereitet sie strukturiert in große Datensätze auf. All dies ist heute im deutschen Gesundheitssystem aufgrund diverser Barrieren nicht möglich, obwohl es technologisch möglich wäre.

Fazit: Vor diesem Hintergrund spricht sich die iGW für die Implementierung eines solchen Trust-Centers – basierend auf innovativen und sicheren Technologien – in Deutschland aus.

---

[1] Bundesministerium für Bildung und Forschung, „Digitalisierung in der Medizin - BMBF“, Bundesministerium für Bildung und Forschung - BMBF, zugegriffen 15. August 2018, https://www.bmbf.de/de/digitalisierung-in-der-medizin-2897.html.
[2] TMF e.V., „‚Eine stille Reserve für die medizinische Forschung und für die Steuerung im Gesundheitssystem‘ > TMF > News“, zugegriffen 15. August 2018, http://www.tmf-ev.de/News/articleType/ArticleView/articleId/4160.aspx.
[3] Bauanstalt für Arbeitsschutz und Arbeitsmedizin (baua), „Gutachten zum Einsatz von Sekundärdaten für die Forschung zu Arbeit und Gesundheit“, 2018, https://www.baua.de/DE/Angebote/Publikationen/Berichte/Gd93.pdf?__blob=publicationFile&v=7.
[4] Bundesministerium für Bildung und Forschung, „Digitalisierung in der Medizin - BMBF“.
[5] SNPC GmbH, „Von Big- über Smart-Data zur Personalisierten Medizin: Trust-Center/Datenintegrationszentren als Infrastruktur-Hub“, 2017, http://www.snpc.de/wp-content/uploads/2017/10/SNPC-Broschuere_Trust-Center-final-Web.pdf.

Durch die Nutzung von personenbezogenen Gesundheitsdaten können neue Erkenntnisse über die Gesundheit der Bevölkerung, unterschiedliche Erkrankungen und Behandlungsmethoden gewonnen werden. Ein Trust-Center kann viele verschiedene Formen annehmen, so dass ein einzigartiges Trust-Center nicht existiert. Die Implementierung eines entsprechenden Trust-Centers sollte dennoch die Richtlinien und Bedürfnisse des Wirtschaftsstandorts Deutschland widerspiegeln und gleichzeitig die Anlehnung an internationale Standards suchen. In diesem Problemaufriss werden ausschließlich die grundlegenden Eigenschaften und deren Umsetzungshürden beleuchtet. Beispielsweise ist offen, welche Organisation das Trust-Center verwalten soll und nach welchen Kriterien eine Prüfstelle Datennutzungsanträge prüft. Die detaillierte Ausgestaltung des Trust-Centers bleibt zu definieren.

Welche Umsetzungshürden gibt es heute in Deutschland für ein bundesweites Trust-Center?

Für ein bundesweites Trust-Center für Gesundheitsdaten in Deutschland bestehen diverse strukturelle, regulatorische und infrastrukturelle Umsetzungshürden.

Gesellschaftliche Akzeptanz

Die gesellschaftliche Akzeptanz in der breiten Bevölkerung für die Verarbeitung von personenbezogenen Gesundheitsdaten ist essenziell für die Umsetzung eines Trust-Centers in Deutschland. Eine Umfrage von TNS Infratest aus dem Jahre 2016 ergab, dass nur 42 Prozent aller Deutschen ihre medizinischen Daten anonymisiert zur Verfügung stellen würden. Dies steht den enormen Potenzialen der Digitalisierung des Gesundheitssystems gegenüber, die der deutschen Bevölkerung erhebliche Vorteile durch die Reduzierung von Gesundheits- und Versorgungskosten bietet.[6] Der Schutz der Privatsphäre und der Datenschutz sind – auch historisch bedingt – wichtige Anliegen für viele deutsche Bürger.[7] Grundlage für eine Akzeptanz ist ein besseres Verständnis von Verfahren, Abläufen, Sicherheitsvorkehrungen und Chancen eines Trust-Centers.

Fazit: Eine bundesweite Aufklärungskampagne der Bundeszentrale für gesundheitliche Aufklärung (BZgA) könnte die gesellschaftliche Akzeptanz für die Datennutzung im Gesundheitsbereich steigern. Darüber hinaus sollte die Digitalkompetenz frühzeitig in die Schulausbildung integriert werden.

---

[6] Digital McKinsey, „Digitalisierung im Gesundheitswesen, Oktober 2018, https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2018/2018-09-25-digitalisierung%20im%20gesundheitswesen/langfassung%20-%20digitalisierung%20im%20gesundheitswesen.ashx

[7] Tagesspiegel, „Therapie mit Daten“, *Der Tagesspiegel Online*, 17. Juli 2017, https://www.tagesspiegel.de/wissen/digitale-medizin-therapie-mit-daten/20067364.html.

Strukturelle Herausforderungen

Gewichtige strukturelle Probleme erschweren die Umsetzung eines bundesweiten Trust-Centers in Deutschland. Durch das föderale System liegt die Gesetzgebungskompetenz in diesem Bereich bei den 16 Bundesländern, die wiederum unterschiedliche sozioökonomische Interessen verfolgen. Neben dem Bundesdatenschutzgesetz (BDSG) verfügt jedes Bundesland über eigene Datenschutz- (LDSG) und Landeskrankenhausgesetze (LKG), welche von den entsprechenden Aufsichtsbehörden und Landesdatenschutzbeauftragten überwacht werden. Das hat zur Folge, dass bundesweite und tiefgreifende Projekte, die sensible Themen wie Gesundheitsdaten betreffen und bundesweite Koordination erfordern, schwer umzusetzen sind. Zusätzlich werden personenbezogene Gesundheitsdaten der Versicherten durch diese heterogene gesetzliche Landschaft unterschiedlich strikt geschützt. Dies hat zur Folge, dass der Datenschutz in diesem Fall vom Standort des Versicherten bzw. Patienten abhängt.[8]

Die teilweise sehr unterschiedlichen Anforderungen des BDSG, der LDS, der LKG und des SGBs sind eine der größten aktuellen Hindernisse für ein Trust-Center und in Textbox 1 veranschaulicht.[9]

Textbox 1: Unterschiedliche Datenschutzgesetze

Der Schutz von personenbezogenen Patientendaten ist im jeweiligen Krankenhausgesetz der Bundesländer festgelegt. Allerdings ist derselbe Datenschutz in Nordrhein-Westfalen in einem eigenständigen Gesundheitsdatenschutzgesetz geregelt. Die Bestimmungen sind also nicht nur anders verortet, sondern unterscheiden sich auch inhaltlich. Beispielsweise besagt § 24 Abs. 8 des Landeskrankenhausgesetzes Berlin, dass Patientendaten nach Erfüllung der Aufgaben, für die sie erhoben worden sind, unverzüglich zu löschen sind. Andererseits sieht das Landeskrankenhausgesetz Mecklenburg-Vorpommern in § 19 Abs.1 die Sperrung der Patientendaten in Krankenunterlagen nach Abschluss der Behandlung und deren Löschung spätestens nach Ablauf von 30 Jahren vor.[10]

Fazit: Eine Harmonisierung der einzelnen Landesdatenschutzgesetze hin zu bundesweit einheitlichen Vorgaben ist aus Sicht der iGW zwingend notwendig. Hier sollte die Möglichkeit eines Bund-Länder-Staatsvertrages geprüft werden.

[8] SNPC GmbH, „Von Big- über Smart-Data zur Personalisierten Medizin: Trust-Center/Datenintegrationszentren als Infrastruktur-Hub“.
[9] BIO Deutschland, bitkom, bvitg, BVMed, Spectaris, VDGH, vfa, ZVEI, Hrsg., „Deutschland braucht ein nationales eHealth-Zielbild - für eine starke industrielle Gesundheitswirtschaft und eine qualitativ hochwertige medizinische Versorgung“, Juni 2018, https://www.bvitg.de/wp-content/uploads/Verb%C3%A4nde-bvitg_Co_Diskussionspapier-eHealth-Zielbild-20180625.pdf.
[10] BIO Deutschland, bitkom, bvitg, BVMed, Spectaris, VDGH, vfa, ZVEI.

Rechtliche & regulatorische Aspekte

Rechtliche und regulatorische Hürden und Aspekte erschweren die Umsetzung eines Trust-Centers in Deutschland. Diese rechtlichen Hürden haben ihre Wurzeln zum Teil in den bereits beschriebenen strukturellen Hürden des föderalen Systems in Deutschland. Andere rechtliche Problemstellungen reflektieren den tief verwurzelten Wunsch und die Notwendigkeit nach dem Schutz der Privatsphäre und persönlichen Daten. Laut des Bundesdatenschutzgesetzes und der Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO) sind Gesundheitsdaten Teil einer besonderen Kategorie von personenbezogenen Daten, die bei der Verarbeitung außerordentlichen Schutz erhalten.[11,12] Der hohe Datenschutz erschwert die Datenverarbeitung und verlangt eine genaue Abwägung der Risiken und des Nutzens.

a) **EU-DSGVO:** Die EU-DSGVO ist seit dem 25. Mai 2018 in Kraft. Die komplexen rechtlichen Anforderungen an die Industrie verdeutlichen, dass eine bundesweite einheitliche Umsetzung der EU-DSGVO und eine Harmonisierung der gesetzlichen Rahmenbedingungen zwingend notwendig sind. Das heißt, dass nicht nur eine bundesweit einheitliche Harmonisierung der Datenschutzgesetze – wie oben beschrieben – erforderlich ist, sondern auch eine EU-weite Vereinheitlichung des Datenschutzes. Eine internationale rechtliche Harmonisierung würde erreichen, dass die Verarbeitung von personenbezogenen Gesundheitsdaten erstens erfolgen kann und zweitens nicht standortabhängig ist.[13] Denn besonders im digitalen Gesundheitsbereich verändern sich die technischen Rahmenbedingungen rasant. Gleichzeitig droht der deutschen Industrie ein Rückstand im internationalen Innovationswettbewerb. Nur mit einem innovationsfreundlichen Rechtsrahmen, der die relevanten nationalen Gesetze harmonisiert und die einheitliche Umsetzung der EU-DSGVO beinhaltet, ist die Datenverarbeitung und ein Trust-Center möglich.[14] Der Standort Deutschland kann außerdem nur im internationalen Wettbewerb mit einem adäquaten Rechtsrahmen mithalten und führen.

b) **Informationelle Selbstbestimmung:** Das Recht jedes Bürgers auf Informationelle Selbstbestimmung ist ein wichtiger rechtlicher Aspekt bei der Umsetzung eines Trust-Centers.[15] Grundgedanke des Rechts ist es, dass die moderne Datenverarbeitung im digitalen Zeitalter die informationelle Selbstbestimmung der Bürger gefährdet, wenn nicht bekannt ist, welche persönlichen Daten für unterschiedliche Zwecke verarbeitet werden.[16] Hinsichtlich eines möglichen Trust-Centers muss geprüft werden, welche Daten aufgenommen werden können, wie die Verknüpfung von Gesundheitsdaten durch ein Trust-Center rechtskonform umgesetzt werden kann und in welchem Umfang verknüpfte Daten gemeinsam genutzt werden können. Ziel ist es, die Therapie und Versorgung des Versicherten zu verbessern und das Recht auf informationelle Selbstbestimmung zu schützen.

c) **Datenhoheit:** Grundsätzlich muss klar festgelegt werden, wem die Datenhoheit über personenbezogene Gesundheitsdaten in welchem Maße obliegt. Die industrielle Gesundheitswirtschaft begrüßt die Positionen von unterschiedlichen Akteuren des Gesundheitssystems, dass der Versicherte Herr seiner

---

[11] Datenschutzbeauftragter-Info, „Besondere Kategorien personenbezogener Daten nach der DSGVO“, Datenschutzbeauftragter, 28. Juli 2017, https://www.datenschutzbeauftragter-info.de/besondere-kategorien-personenbezogener-daten-nach-der-dsgvo/.
[12] „Art. 4 DSGVO – Begriffsbestimmungen“, *Datenschutz-Grundverordnung (DSGVO)* (blog), zugegriffen 14. August 2018, https://dsgvo-gesetz.de/art-4-dsgvo/.
[13] bvitg, „Datenschutz-Grundverordnung: bvitg regt Diskurs über Gestaltungs- und Interpretationsspielräume an“, BVITG, 17. Mai 2018, https://www.bvitg.de/datenschutz-grundverordnung-bvitg-regt-diskurs-ueber-gestaltungs-und-interpretationsspielraeume-an/.
[14] Christian Dierks, „Gastbeitrag zum EU-Datenschutz: Aufwind für Verarbeitung medizinischer Daten“, zugegriffen 17. August 2018, https://www.aerztezeitung.de/praxis_wirtschaft/datenschutz/article/964545/gastbeitrag-eu-datenschutz-aufwind-verarbeitung-medizinischer-daten.html.
[15] Kassenärztliche Bundesvereinigung, „Dabrock: Patient muss Souverän seiner Daten bleiben“, zugegriffen 2. August 2018, http://www.kbv.de/html/2017_32331.php.
[16] Bundeszentrale für politische Bildung, „informationelle Selbstbestimmung | bpb“, zugegriffen 14. August 2018, https://www.bpb.de/nachschlagen/lexika/recht-a-z/22392/informationelle-selbstbestimmung.

Daten sein sollte.[17,18,19] Im digitalen Zeitalter sollte das Recht auf informationelle Selbstbestimmung gewahrt und gefördert werden, damit der Nutzer zur Kontrolle über seine Daten befähigt wird. Der rechtliche Anspruch des Leistungserbringers, der die Gesundheitsdaten während der Behandlung erhebt, steht der vollen Datenhoheit beziehungsweise dem Dateneigentum des Versicherten entgegen. Zusätzlich zu der Festlegung der Datenhoheit des Versicherten bedarf es klarer Zugriffsrechte Dritter für die Verarbeitung von Gesundheitsdaten durch ein Trust-Center. Die Zugriffsrechte müssen die Sicherheit, Verfügbarkeit und Nutzbarkeit der personenbezogenen Gesundheitsdaten sicherstellen. Eine detaillierte Ausgestaltung der Zugriffsrechte für Dritte bei einem Trust-Center sollte die Bedürfnisse der industriellen Gesundheitswirtschaft berücksichtigen.

d) **Einwilligung:** Das Recht auf Informationelle Selbstbestimmung könnte möglicherweise ausreichend durch eine Einwilligung des Bürgers bzw. des Versicherten geschützt sein. Das ist allerdings von der genauen Ausgestaltung des Trust-Centers abhängig und wie die Verarbeitung der Daten gehandhabt wird. Die Einwilligung des Versicherten wirft jedoch Unklarheiten auf. Es ist nicht offensichtlich, ob und in welchem Umfang Versicherte ihre personenbezogenen Gesundheitsdaten für unbestimmte Forschungszwecke freigeben können. Der Umfang und die Reichweite der Einwilligung sind nicht nur für das Recht auf informationelle Selbstbestimmung wichtig, sondern werden sich auch auf die Verarbeiter der Gesundheitsdaten auswirken.

Einige Öffnungsklauseln sollten auf ihre Anwendbarkeit bezüglich der Einwilligung für die Nutzung von personenbezogenen Gesundheitsdaten geprüft werden. Beispielsweise sollte geprüft werden, inwiefern die Öffnungsklausel aus Art. 9 Abs. 2 Uabs. 2 lit. j) EU-DSGVO als Forschungsausnahme bei der Verarbeitung von personenbezogenen Gesundheitsdaten durch ein Trust-Center Anwendbarkeit finden kann. Zusätzlich decken Art. 6 Abs. 1. Uabs. 1 lit. c), e), Abs 2, 3 EU-DSGVO und Art. 9 Abs. 2. Lit. b), g), h), i), Abs. 4 EU-DSGVO einen großen Bereich der im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt in Erwägung kommende Datenverarbeitungsvorgänge ab. Eine weitere Möglichkeit für eine forschungs- und nutzungsfreundliche Ausgestaltung des Forschungstatbestands bietet § 287 Sozialgesetzbuch (SGB) V, der besonders hinsichtlich der zeitlichen Befristung und Beschränkungen auf bestimmte Forschungsvorhaben gelockert werden könnte.

e) **Widerrufsrecht:** Die Beantwortung dieser Unklarheiten wirkt sich auf andere Aspekte aus, zum Beispiel auf das Widerrufsrecht der Versicherten. Der Versicherte muss die Möglichkeit haben, seine Einwilligung zur Verarbeitung von personenbezogenen Gesundheitsdaten für zukünftige Zwecke zu widerrufen. Dennoch sollte festgestellt werden, dass entsprechend Art. 7 Abs. 3 Satz 2 EU-DSGVO ein rückwirkender Widerruf nicht erfolgen kann, da dieser nicht mit der Verarbeitung von Gesundheitsdaten in der industriellen Gesundheitswirtschaft vereinbar ist. Hinsichtlich eines Trust-Centers muss ebenfalls klar geregelt werden, wie sich ein Widerruf auswirkt. Deshalb ist eine Aufklärung dieser Fragen für die Datenverarbeitung und ein mögliches Trust-Center zwingend notwendig.

f) **Datenschutz:** Der Datenschutz steht bei der Datenverarbeitung an erster Stelle. Durch die hohe Sensibilität sind die Daten nicht nur für ihre Subjekte sensibel, sondern auch schützenswert vor Angriffen von Cyber-Kriminellen.[20] Deshalb müssen personenbezogene Gesundheitsdaten so verschlüsselt und entschlüsselt werden, so dass die personenbezogenen Gesundheitsdaten ausreichend technisch geschützt sind. Die Verschlüsselung beim Eingang der Daten in das Trust-Center und die Entschlüsselung haben einen maßgeblichen Einfluss auf die Datenverarbeitung. Aus Sicht der iGW müssen die personenbezogenen Gesundheitsdaten „at-rest“ und „in-transit“ verschlüsselt sein. Zusätzlich muss

---

[17] BIO Deutschland, bitkom, bvitg, BVMed, Spectaris, VDGH, vfa, ZVEI, „Deutschland braucht ein nationales eHealth-Zielbild - für eine starke industrielle Gesundheitswirtschaft und eine qualitativ hochwertige medizinische Versorgung“.
[18] Deutscher Ethikrat, „Big Data und Gesundheit“, Informationen und Nachrichten aus dem Deutschen Ethikrat, Januar 2018, https://www.ethikrat.org/fileadmin/Publikationen/Infobrief/Infobrief_01-18_Web.pdf.
[19] Techniker Krankenkasse, „Homo Digivitalis: TK-Studie zur Digitalen Gesundheitskompetenz“, April 2018, https://www.tk.de/centaurus/servlet/contentblob/981906/Datei/91738/TK-Studienband-Digitale-Gesundheitskompetenz-Homo-Digivitalis-2018.pdf.
[20] DGQ, „Datenschutz und die EU-DSGVO im Gesundheitswesen“, *DGQ Blog* (blog), 18. Oktober 2017, http://blog.dgq.de/datenschutz-und-die-eu-dsgvo-im-gesundheitswesen/.

geklärt werden, auf welche Art und Weise der Personenbezug in den Daten durch einen Prozess der Anonymisierung oder Pseudonymisierung unkenntlich gemacht wird. Es existieren verschiedene Ansätze, die Daten entweder zu pseudonymisieren oder zu anonymisieren. Der Health Insurance Portability and Accountability Act (HIPAA) in den USA ist ein Beispiel für mehrere Methoden, personenbezogene Gesundheitsdaten zu pseudonymisieren.[21] Zwar handelt es sich beim HIPAA um einen amerikanischen Ansatz zur Pseudonymisierung, doch es verdeutlicht dennoch, dass eine klare Einigung in diesem Bereich möglich ist. Die Entscheidung für eine bestimmte Methode hängt davon ab, in welchem Umfang Daten für die Verarbeitung benötigt werden und in welchem Maße sie für die Verarbeitung erkennbar sein müssen. Hier sollte der Gesetzgeber eine einheitliche Regelung schaffen, um die Planungssicherheit und den Datenschutz zu gewährleisten.[22]

g) **Datensicherheit:** Zusätzlich ist die Datensicherheit von entschlüsselten Gesundheitsdaten nicht vollständig geklärt. Ein Trust-Center muss die Sicherheit von Gesundheitsdaten gewährleisten können, wenn sie in das Trust-Center eingefügt werden und wenn es Anwendern den Zugriff auf die verschlüsselten Gesundheitsdaten ermöglicht. Hier bedarf es Richtlinien, wie diese Daten vor, während und nach der Nutzung gehandhabt werden sollen. Die Zugriffsrechte für Anwender müssen ebenfalls geklärt werden. In Verbindung mit der Verschlüsselung und Entschlüsselung von personenbezogenen Gesundheitsdaten benötigen die Anwender zukunftsorientierte und eindeutige Zugriffsrechte. So kann ein sicherer und ethischer Datenumgang von Anwendern wie der industriellen Gesundheitswirtschaft gewährleistet werden.

h) **Zweckbindung:** Der Art. 5 lit. b EU-DSGVO und das deutsche Datenschutzgesetz definieren eine strenge Zweckbindung für die Verarbeitung von personenbezogenen Gesundheitsdaten, die der Datenverarbeitung aktuell im Wege steht. Gekoppelt mit der Datensparsamkeit ist die enge Zweckbindung nicht mehr zeitgemäß im digitalen Zeitalter und nicht vereinbar mit dem Ziel, neue Erkenntnisse aus der Datenverarbeitung zugewinnen.[23] Gleichzeitig bietet die EU-DSGVO den nationalen Gesetzgebern in Art. 9 Abs. 2 reichlich Gestaltungsspielraum, um die Datenverarbeitung für wissenschaftliche Forschung zu ermöglichen. Diese Handlungsmöglichkeiten sollte der deutsche Gesetzgeber in jedem Fall nutzen, um die Potenziale der Datenverarbeitung zu nutzen. Eine Bedingung dafür ist, dass der Gesetzgeber rechtliche Unklarheiten ausräumt und klare Maßnahmen für die Verschlüsselung und Entschlüsselung der Gesundheitsdaten festlegt. Eine innovationsoffenere Zweckbindung ist deshalb notwendig für ein Trust-Center.

Fazit: Ein innovationsoffener und klarer Rechtsrahmen ist dringend benötigt, um diese wichtigen Fragen zu beantworten und der industriellen Gesundheitswirtschaft die notwendige Rechtssicherheit zu verschaffen, um personenbezogene Gesundheitsdaten sicher und verantwortungsvoll zu verarbeiten. Der Gesetzgeber muss hier seiner Verantwortung nachkommen.

---

[21] Office for Civil Rights (OCR), „Methods for De-Identification of PHI“, Text, HHS.gov, 7. September 2012, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.
[22] bvitg, „Datenschutz-Grundverordnung“.
[23] BIO Deutschland, bitkom, bvitg, BVMed, Spectaris, VDGH, vfa, ZVEI, „Deutschland braucht ein nationales eHealth-Zielbild - für eine starke industrielle Gesundheitswirtschaft und eine qualitativ hochwertige medizinische Versorgung“.

Infrastruktur

Eine IT-Infrastruktur, die große Datenmengen sicher und schnell für Anwender verfügbar machen kann, gibt es noch nicht in Deutschland. Allerdings wird die Telematikinfrastruktur (TI) in Deutschland implementiert, die das Gesundheitssystem in Deutschland für den Austausch bundesweit verbinden wird. Die für die Umsetzung der TI und der elektronischen Gesundheitskarte verantwortliche Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) gibt an, dass neben den bestehenden Anwendungen wie den Versichertenstammdaten auf der elektronischen Gesundheitskarte zukünftig auch weitere Anwendungen durch die TI ausgerollt werden können.[24]

In Anbetracht des erheblichen zeitlichen und finanziellen Aufwandes der bisherigen Implementierung der TI sollten parallele Infrastrukturen bezüglich eines möglichen Trust-Centers vermieden werden. Zusätzlich verfügt die bestehende TI durch die Informationssicherheitsmechanismen, das geschlossene Netz und die kryptographischen Verfahren über eine belastbare Sicherheitsstruktur, die regelmäßig vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüft wird. Daraus folgt, dass die TI in vielerlei Hinsicht die passendste Infrastruktur für ein Trust-Center sein könnte. Die optimale Wahl der unterschiedlichen Infrastrukturkomponenten sollte basierend auf den detaillierten Bedürfnissen der unterschiedlichen Akteure und Anwender erfolgen. Die Interoperabilität zwischen verschiedenen Komponenten ist mittels verschiedener Standards möglich und dringend geboten. Daher besteht im Bereich der Infrastruktur viel Flexibilität zur Ausgestaltung des Trust-Centers.

Fazit: Die Möglichkeit, ein Trust-Center in die TI zu integrieren, sollte deshalb geprüft werden.

---

[24] gematik, „Telematikinfrastruktur“, zugegriffen 15. August 2018, https://www.gematik.de/telematikinfrastruktur/.

Best-Practice-Beispiele für Trust-Center

Andere Länder verfügen schon heute über ein Trust-Center und auch in Deutschland gibt es regionale und sektorale Ansätze für ein Trust-Center. Bei allen Beispielen ist zu beachten, dass sie nur begrenzt als Vorbilder dienen können.[25] Diverse Unterschiede bedeuten, dass sie nicht einfach in Deutschland adaptiert werden können. Trotzdem offenbaren sie mögliche Lösungsansätze für ein Trust-Center.

Textbox 2: Beispiel Australien: Population Health Research Network (PHRN)

Das Population Health Research Network (PHRN) ist ein Trust-Center, das eine Forschungsinfrastruktur im Gesundheitsbereich für Forscher, Wirtschaft und andere Anwender zur Verfügung stellt. Im Jahre 2008/2009 von der australischen Regierung gegründet, ist es für zehn Jahre bis 2027/2028 mit AUS$ 1,5 Milliarden finanziert.[26] Das PHRN verknüpft bestehende regionale Datenverknüpfungsstellen aus Bundesstaaten. Dadurch entsteht ein Trust-Center für Gesundheitsdaten aus allen Regionen des Landes. Die Datenverknüpfungsstellen forschen selbst nicht, sondern fungieren lediglich als Knotenpunkte für den Datenaustausch.[27]

Das PHRN verdeutlicht, wie wichtig infrastrukturelle Voraussetzungen sind, besonders in einem föderalen Land. Wenn ein Trust-Center in Deutschland etabliert werden sollte, wäre es erstrebenswert, die bestehenden Datenaustauschstellen zu integrieren. Zweitens verdeutlicht die Finanzierung des PHRN, dass die australische Regierung umfangreiche und weitsichtige Investitionen getätigt hat. Dies ist auch wichtig für ein Trust-Center in Deutschland, da sich die medizinische Forschung und Entwicklung in vielen Bereichen durch große Innovationszyklen auszeichnet.

Auch in Deutschland gibt es bereits erste Schritte in Richtung eines Trust-Centers im Gesundheitsbereich. In Textbox 3 und 4 ist die Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung (BMBF) dargestellt.

Textbox 3: Beispiel Deutschland: Medizininformatik-Initiative (BMBF)

Das BMBF hat 2017 das Förderkonzept Medizininformatik und die dazugehörige Medizininformatik-Initiative vorgestellt.[28] Ziel des Konzepts und der Initiative ist es, die Forschungsmöglichkeiten und die Patientenversorgung in den Universitätskliniken zu verbessern. Zentral für dieses Ziel sind Datenintegrationszentren, die relevante Gesundheitsdaten aus mehreren Universitätskliniken und anderen Einrichtungen für Forschungszwecke verfügbar machen.[29] Zusätzlich soll der Austausch und die Verfügbarkeit von Gesundheitsdaten für IT-Lösungen und Anwendungen genutzt werden. Das Förderkonzept finanziert aktuell vier Datenintegrationszentren und verfügt über ein Budget von € 150 Millionen für den Zeitraum 2017 – 2025.

Textbox 4: MIRACUM-Konsortium der Medizininformatik-Initiative (BMBF)

Aktuell sind vier Konsortien der Medizininformatik-Initiative in der Projektphase, wie zum Beispiel das MIRACUM-Konsortium, das mit acht Universitäten aus fünf Bundesländern, zwei Hochschulen und einem Industrie-Partner zahlreiche Forscher und Infrastrukturen für Forschungszwecke vereint.[30] Drei weitere Konsortien,

[25] SNPC GmbH, „Von Big- über Smart-Data zur Personalisierten Medizin: Trust-Center/Datenintegrationszentren als Infrastruktur-Hub“.
[26] Population Health Research Network, „PHRN - About Us“, zugegriffen 2. August 2018, http://www.phrn.org.au/about-us/overview/.
[27] Population Health Research Network, Overview, http://www.phrn.org.au/about-us/overview/
[28] Bundesministerium für Bildung und Forschung, „Medizininformatik - BMBF“, Bundesministerium für Bildung und Forschung - BMBF, zugegriffen 13. August 2018, https://www.bmbf.de/de/medizininformatik-3342.html.
[29] Bundesministerium für Bildung und Forschung, „Förderkonzept Medizininformatik: Daten vernetzen - Gesundheit verbessern“, Förderkonzept (Bundesministerium für Bildung und Forschung, 2017), https://www.bmbf.de/pub/Medizininformatik.pdf.
[30] Universität Magdeburg, „Medizinische Fakultät/Universitätsklinikum Magdeburg A. ö. R. - Bundesweite Medizininformatik-Initiative mit Beteiligung der UMMD erfolgreich gestartet“, zugegriffen 15. August 2018,

HiGHmed, DIFUTURE und SMITH beschäftigen sich ebenfalls mit Wegen zur gemeinsamen Datennutzung für die Verbesserung der Gesundheitsversorgung. Beispielsweise verknüpft das MIRACUM-Konsortium klinische Befunde, bildgebende Diagnostik und genetische und molekulare Untersuchungen für eine zielgerichtete Behandlung. Das MIRACUM-Konsortium und die weiteren Konsortien in der Projektphase veranschaulichen, dass schon heutzutage in Deutschland verschiedene personenbezogene Gesundheitsdaten über Bundesländer hinweg für die Gesundheitsversorgung und Forschung verknüpft werden.[31]

Die Medizininformatik-Initiative des BMBF ist ein positives Signal für die Datenverarbeitung und ein Trust-Center in Deutschland. Dennoch fließen noch keine Daten aus Arztpraxen, die Routinedaten von Sozialversicherungsträgern oder der gesetzlichen Krankenversicherungen in die Datenintegrationszentren der geförderten Projekte. Das mögliche Bayerische Gesundheitsdatenzentrum ist ein zweites positives Signal. Eine Machbarkeitsstudie der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF) zu der Möglichkeit eines Gesundheitsdatenzentrums in Bayern wurde für den Zeitraum 2015 – 2016 beauftragt.[32]

Fazit: Es sollte geprüft werden, ob die Medizininformatik-Initiative als ein bundesweites Trust-Center fungieren könnte. In diesem Zusammenhang hat das BMBF auch bereits den Ausbau der TI in Verbindung gebracht.[33] Dem sollte eine detaillierte Prüfung folgen, ob die TI auch eine Trust-Center-Funktion ausfüllen könnte.

---

https://www.med.uni-magdeburg.de/Presse/Pressemitteilungen/Bundesweite+Medizininformatik_Initiative-p-15562.html.

[31] Universität Magdeburg.

[32] Sebastian Claudius Semler, „Machbarkeitsstudie zur Gesundheitsdatennutzung in Bayern“ (7. Juli 2017), https://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=30909&PortalId=0.

[33] Bundesministerium für Bildung und Forschung, „Förderkonzept Medizininformatik: Daten vernetzen - Gesundheit verbessern“.

Lösungsvorschläge

Kurzfristige Lösungsvorschläge – bis Ende der Legislaturperiode

1. Eine bundesweite Aufklärungskampagne der Bundeszentrale für gesundheitliche Aufklärung (BZgA) sowie die Förderung von Digitalkompetenzen in der Schulbildung wäre zielführend, um die gesellschaftliche Akzeptanz für die Datenverarbeitung zu steigern.

2. Die Finanzierung der BMBF-Medizininformatik-Initiative sollte für den Zeitraum nach 2025 gesichert und ausgebaut werden. Die Medizininformatik-Initiative liefert vielversprechende Forschungsergebnisse und treibt die Forschung und Entwicklung durch die Verknüpfung von Gesundheitsdaten weiter voran. Zusätzlich sollte geprüft werden, ob die Medizininformatik-Initiative in der Zukunft als ein bundesweites Trust-Center fungieren könnte.

3. Für die Prüfung der Weiterentwicklung der Medizininformatik-Initiative zu einem bundesweiten Trust-Center ruft die iGW alle weiteren Akteure im deutschen Gesundheitssystem sowie alle Interessierten dazu auf, gemeinsam eine Lösungsskizze mit der BDI-Initiative Gesundheit digital zu erarbeiten.

4. Die Telematikinfrastruktur sollte für die Funktion eines bundesweiten Trust-Centers mittels einer Machbarkeitsstudie geprüft werden. Als Infrastruktur für den Datenaustausch innerhalb des Gesundheitssystems bietet sich die TI als mögliche „Datenautobahn“ eines Trust-Centers an.

Mittelfristige Lösungsvorschläge – in den nächsten 5 – 10 Jahren

1. Die einheitliche Umsetzung der EU-DSGVO auf Länderebene sollte vorangetrieben werden und Handlungsspielräume in bestehenden nationalen Normen durch die EU-DSGVO genutzt werden. Die EU-DSGVO bietet vor allem in Hinblick auf den Forschungstatbestand hinsichtlich der zeitlichen Befristung und Beschränkungen auf bestimmte Forschungsvorhaben Gestaltungsspielraum.

Quellenverzeichnis

„Art. 4 DSGVO – Begriffsbestimmungen“. *Datenschutz-Grundverordnung (DSGVO)* (blog). Zugegriffen 14. August 2018. https://dsgvo-gesetz.de/art-4-dsgvo/.

Bauanstalt für Arbeitsschutz und Arbeitsmedizin (baua). „Gutachten zum Einsatz von Sekundärdaten für die Forschung zu Arbeit und Gesundheit“, 2018. https://www.baua.de/DE/Angebote/Publikationen/Berichte/Gd93.pdf?__blob=publicationFile&v=7.

BIO Deutschland, bitkom, bvitg, BVMed, Spectaris, VDGH, vfa, ZVEI, Hrsg. „Deutschland braucht ein nationales eHealth-Zielbild - für eine starke industrielle Gesundheitswirtschaft und eine qualitativ hochwertige medizinische Versorgung“, Juni 2018. https://www.bvitg.de/wp-content/uploads/Verb%C3%A4nde-bvitg_Co_Diskussionspapier-eHealth-Zielbild-20180625.pdf.

Bundesministerium für Bildung und Forschung. „Digitalisierung in der Medizin - BMBF“. Bundesministerium für Bildung und Forschung - BMBF. Zugegriffen 15. August 2018. https://www.bmbf.de/de/digitalisierung-in-der-medizin-2897.html.

Bundesministerium für Bildung und Forschung. „Förderkonzept Medizininformatik: Daten vernetzen - Gesundheit verbessern“. Förderkonzept. Bundesministerium für Bildung und Forschung, 2017. https://www.bmbf.de/pub/Medizininformatik.pdf.

Bundesministerium für Bildung und Forschung. „Medizininformatik - BMBF“. Bundesministerium für Bildung und Forschung - BMBF. Zugegriffen 13. August 2018. https://www.bmbf.de/de/medizininformatik-3342.html.

Bundeszentrale für politische Bildung. „informationelle Selbstbestimmung | bpb“. Zugegriffen 14. August 2018. https://www.bpb.de/nachschlagen/lexika/recht-a-z/22392/informationelle-selbstbestimmung.

bvitg. „Datenschutz-Grundverordnung: bvitg regt Diskurs über Gestaltungs- und Interpretationsspielräume an“. BVITG, 17. Mai 2018. https://www.bvitg.de/datenschutz-grundverordnung-bvitg-regt-diskurs-ueber-gestaltungs-und-interpretationsspielraeume-an/.

Datenschutzbeauftragter-Info. „Besondere Kategorien personenbezogener Daten nach der DSGVO“. Datenschutzbeauftragter, 28. Juli 2017. https://www.datenschutzbeauftragter-info.de/besondere-kategorien-personenbezogener-daten-nach-der-dsgvo/.

Deutscher Ethikrat. „Big Data und Gesundheit“. Informationen und Nachrichten aus dem Deutschen Ethikrat, Januar 2018. https://www.ethikrat.org/fileadmin/Publikationen/Infobrief/Infobrief_01-18_Web.pdf.

DGQ. „Datenschutz und die EU-DSGVO im Gesundheitswesen“. *DGQ Blog* (blog), 18. Oktober 2017. http://blog.dgq.de/datenschutz-und-die-eu-dsgvo-im-gesundheitswesen/.

Digital McKinsey, „Digitalisierung im Gesundheitswesen, Oktober 2018, https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2018/2018-09-25-digitalisierung%20im%20gesundheitswesen/langfassung%20-%20digitalisierung%20im%20gesundheitswesen.ashx.

Dierks, Christian. „Gastbeitrag zum EU-Datenschutz: Aufwind für Verarbeitung medizinischer Daten“. Zugegriffen 17. August 2018. https://www.aerztezeitung.de/praxis_wirtschaft/datenschutz/article/964545/gastbeitrag-eu-datenschutz-aufwind-verarbeitung-medizinischer-daten.html.

gematik. „Telematikinfrastruktur“. Zugegriffen 15. August 2018. https://www.gematik.de/telematikinfrastruktur/.

Kassenärztliche Bundesvereinigung. „Dabrock: Patient muss Souverän seiner Daten bleiben“. Zugegriffen 2. August 2018. http://www.kbv.de/html/2017_32331.php.

Population Health Research Network. „PHRN - About Us“. Zugegriffen 2. August 2018. http://www.phrn.org.au/about-us/overview/.

Rights (OCR), Office for Civil. „Methods for De-Identification of PHI“. Text. HHS.gov, 7. September 2012. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

Sebastian Claudius Semler. „Machbarkeitsstudie zur Gesundheitsdatenverarbeitung in Bayern“. Berlin, 7. Juli 2017. https://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=30909&PortalId=0.

SNPC GmbH. „Von Big- über Smart-Data zur Personalisierten Medizin: Trust-Center/Datenintegrationszentren als Infrastruktur-Hub“, 2017. http://www.snpc.de/wp-content/uploads/2017/10/SNPC-Broschuere_Trust-Center-final-Web.pdf.

Tagesspiegel. „Therapie mit Daten“. *Der Tagesspiegel Online*, 17. Juli 2017. https://www.tagesspiegel.de/wissen/digitale-medizin-therapie-mit-daten/20067364.html.

Techniker Krankenkasse. „Homo Digivitalis: TK-Studie zur Digitalen Gesundheitskompetenz“, April 2018. https://www.tk.de/centaurus/servlet/contentblob/981906/Datei/91738/TK-Studienband-Digitale-Gesundheitskompetenz-Homo-Digivitalis-2018.pdf.

TMF e.V. „‚Eine stille Reserve für die medizinische Forschung und für die Steuerung im Gesundheitssystem‘ > TMF > News“. Zugegriffen 15. August 2018. http://www.tmf-ev.de/News/articleType/ArticleView/articleId/4160.aspx.

Universität Magdeburg. „Medizinische Fakultät/Universitätsklinikum Magdeburg A. ö. R. - Bundesweite Medizininformatik-Initiative mit Beteiligung der UMMD erfolgreich gestartet“. Zugegriffen 15. August 2018. https://www.med.uni-magdeburg.de/Presse/Pressemitteilungen/Bundesweite+Medizininformatik_Initiative-p-15562.html.

Notizen

Impressum

BDI-Initiative Gesundheit digital (Industrie-Förderung Gesellschaft mbH)
c/o Breite Straße 29, 10178 Berlin
www.bdi-gesundheit-digital.de
T: +49 30 2028-1570

Redaktion

Herr Ben Mayer
BDI-Initiative Gesundheit digital (IFG)
T: +49 30 2028-1570
b.mayer@ifg.bdi.eu

Frau Katharina Altenburg
ZVEI - Zentralverband Elektrotechnik und Elektronikindustrie e. V.
altenburg@zvei.org

Frau Sabine Hoffmann
Pfizer Deutschland GmbH
sabine.hoffmann@pfizer.com

Mit Unterstützung von

Herr Michael Kahnert
BIO Deutschland e.V.
kahnert@biodeutschland.org