Übergreifendes Datenschutzkonzept der Medizininformatik-Initiative

Autoren: Taskforce Datenschutz der MII mit Vertretern der Konsortien DIFUTURE, HiGHmed, MIRACUM, SMITH, dem Sprecher der AG Datenschutz der TMF sowie Vertretern der TMF-Geschäftsstelle

Version: 1.0

Stand: 17.12.2021

Versionshistorie:

Version	Datum	SharePoint	Autor(en)	Änderung
0.1	20.11.2018		TMF & TF Datenschutz	Gliederung
0.5	22.03.2019		SMITH, Speer, Lowitsch	Kapitel 5
0.6	10.04.2019		H. Hund (HiGHmed) Schneider, TMF Drepper, TMF	Erster Aufschlag auf Basis der DS-Konzepte der Konsortien und des TMF Leitfadens Kommentierung J. Drepper HiGHmed, Herr Hund; Kap. 7.1.
0.8	24.11.2021		Drepper, Speer, Hund, Thasler, Kaulke, Gebhardt u. weitere Vertreter der TF Datenschutz	Umfangreiche Umstrukturierung, Überarbeitung und Fokussierung auf die Anwendungsszenarien Machbarkeitsanfragen, Verteilte Analysen und Daten-Herausgaben, dabei Umstellung von generischem Konzept für Konsortien und Standorte hin zu konkretem Konzept für übergreifende Aspekte
0.9	25.11.2021		Drepper	Abarbeitung von Kommentaren und Änderungsvorschlägen der TF Datenschutz, Komplettierung der Anhänge – zur Vorlage im NSG am 09.12.2021
1.0	17.12.2021		Drepper / Schepers	Berücksichtigung der Verbundvorhaben CORD, POLAR und ABIDE in Kap. 1.1 und 1.2. Umsetzung eines Vorschlags von Herrn Bahls zur Aufteilung von Geburtsdatum und bestimmten Adressangaben von Patienten auf IDAT und MDAT. Deutlichere Hervorhebung in Kap. 1.2 zur Notwendigkeit der Weiterentwicklung des Konzepts.

Inhalt

1. Einleitung

Um Daten aus Krankenversorgung und Forschung besser nutzbar zu machen, fördert das Bundesministerium für Bildung und Forschung (BMBF) die Medizininformatik-Initiative (MII) mit bislang rund 180 Millionen Euro. Die Fördermaßnahme soll die medizinische Forschung stärken und die Patientenversorgung verbessern. Derzeit arbeiten alle Universitätskliniken Deutschlands gemeinsam mit Forschungseinrichtungen, Unternehmen und Patientenvertretern daran, die Rahmenbedingungen zu entwickeln, damit Erkenntnisse aus der Forschung direkt den Patienten erreichen können. Die digitale Verfügbarkeit von Gesundheitsdaten ist dabei eine kritische Voraussetzung, um die Behandlung der Patienten zu verbessern und die Patientensicherheit zu erhöhen. Dadurch können etwa Diagnosen schneller und präziser gestellt und Doppeluntersuchungen vermieden oder unerwünschte Arzneimittelwirkungen verhindert werden. Zudem können Patienten mit Hilfe großer Datenmengen individueller charakterisiert werden. Dadurch gelingt es immer häufiger, den für den Patienten besten Behandlungsansatz bereits vor Therapiebeginn zu bestimmen. Diese maßgeschneiderten Therapien können zu mehr Behandlungserfolgen führen oder Nebenwirkungen reduzieren.

Zudem können routinemäßig im klinischen Alltag anfallende Versorgungsdaten in Deutschland bisher kaum für die Forschung genutzt werden. Die Verknüpfung von Datensätzen aus Forschung (z. B. Biobanken, Gendatenbanken, Daten aus Studien) und Patientenversorgung kann jedoch Zusammenhänge aufdecken, etwa zwischen einzelnen Genen, Lebensstilen und Erkrankungen oder Komplikationen. Die kombinierte Nutzung dieser Daten fördert Innovationen in Diagnostik, Therapie und Prävention. Zudem eröffnen große klinische Datensätze Chancen für die frühere Erkennung von seltenen Komplikationen, Risiken und Nebenwirkungen, etwa bei Arzneimitteltherapien. Auch würde zum Beispiel die Datenlage für die Erforschung seltener Erkrankungen verbessert.

Im Rahmen der MII werden medizinische Daten in den Universitätsklinika aufbereitet und für Anwendungsfälle der Forschung und Versorgung nutzbar gemacht. Zu diesem Zweck etablieren die beteiligten Universitätsklinika Datenintegrationszentren (DIZ), die Daten aus Forschung und Versorgung integriert nutzbar machen. Die Auswertung der Daten kann in verschiedenen Szenarien erfolgen, angefangen von der Auswertung von Daten eines einzelnen Universitätsklinikums bis hin zu Auswertungen von Daten aller beteiligten Standorte. Derzeit sind in vier Konsortien alle Standorte mit Universitätskliniken in Deutschland angeschlossen. Perspektivisch sollen auch nicht-universitäre Standorte und ggf. auch Versorgungseinrichtungen aus dem ambulanten Sektor in die Verfahren eingeschlossen werden. Die Bereitstellung der Daten soll sowohl im Sinne einer physischen Zusammenführung der Daten zum Zweck der Analyse („bring the data to the analysis“) als auch in Form einer verteilten Analyse am Standort des Dateneigners („bring the analysis to the data“) erfolgen.

1.1 Darstellung der Medizininformatik-Initiative

Die MII wurde vom BMBF im Jahr 2015 als neues Förderkonzept mit einem Antragsaufruf gestartet. Die Entwicklung dieser Förder-Initiative gliedert sich in mehrere, aufeinander aufbauende Phasen und begleitende Aktivitäten (s. Abb. 1).

Während in der vorgeschalteten Konzeptphase ab 2016 ein Ideenwettbewerb bei gleichzeitigem Aufbau einer koordinierenden Begleitstruktur stattfand, werden seit 2018 an den universitätsklinischen Standorten im Rahmen von vier Konsortien Infrastrukturen für die effiziente Integration von Versorgung und Forschung aufgebaut. Im Zentrum dieser Aufbauarbeiten stehen die neu geschaffenen

Datenintegrationszentren. In der ab 2023 folgenden nächsten Förderphase sollen die aktuell entwickelten Standards und Anwendungsfälle auch auf weitere Standorte und Stellen, was explizit auch den ambulanten Bereich einschließen soll, ausgerollt werden.

Abb. 1: Zeitliche Struktur der Medizininformatik-Initiative

Aktuell sind alle universitätsklinischen Standorte in Deutschland in der einen oder anderen Form an eines der vier geförderten Konsortien der MII angeschlossen (s. Abb. 2).

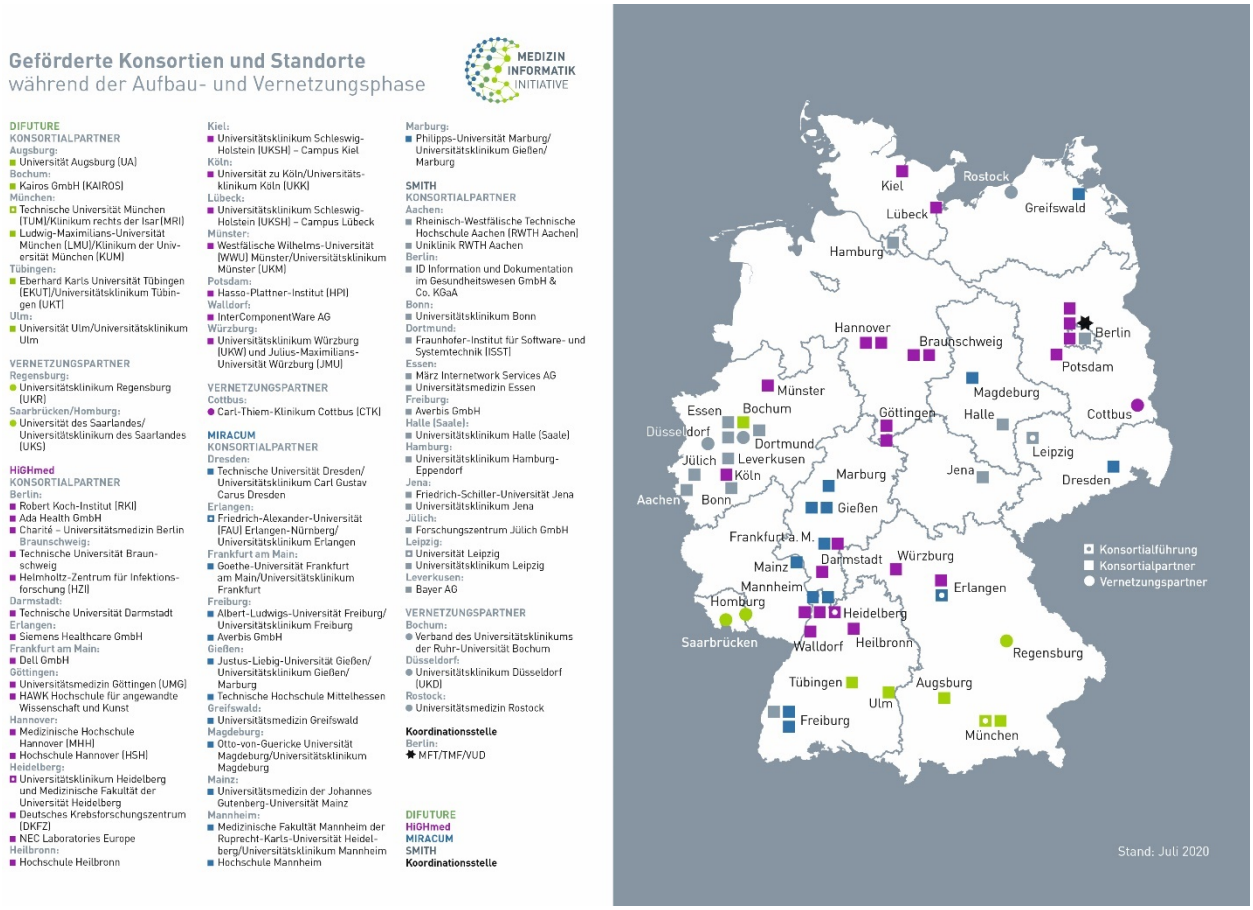

Abb. 2: Konsortien und Standorte der MII (während der Aufbau- und Vernetzungsphase)

In der Aufbau- und Vernetzungsphase fördert das BMBF die folgenden vier Konsortien:

- DIFUTURE: Data Integration for Future Medicine (www.difuture.de)
- HiGHmed: Heidelberg – Göttingen – Hannover Medical Informatics (www.highmed.org)
- MIRACUM: Medical Informatics in Research and Care in University Medicine – Medizininformatik in Forschung und Versorgung in der Universitätsmedizin (www.miracum.org)
- SMITH: Smart Medical Information Technology for Healthcare (www.smith.care)

Darüber hinaus fördert das BMBF in der Aufbau- und Vernetzungsphase seit 2020 sekundäre transkonsortiale Verbundvorhaben mit einer unterschiedlichen Anzahl von kooperierenden Verbundpartnern:

- POLAR-MI: POLypharmazie, Arzneimittelwechselwirkungen und Risiken (https://www.medizininformatik-initiative.de/index.php/de/POLAR)
- CORD-MI: Collaboration on Rare Diseases (https://www.medizininformatik-initiative.de/de/CORD)
- ABIDE-MI: Aligning Biobanking and DIC Efficiently (https://www.medizininformatik-initiative.de/de/use-cases-und-projekte/abidemi)

In den Konsortien und in den Verbundvorhaben haben sich Universitätskliniken mit weiteren Partnern wie Forschungsinstituten, Hochschulen, Unternehmen oder nicht-universitären Krankenhäusern zusammengeschlossen. Die Konsortien und Verbundvorhaben arbeiten gemeinsam daran, die Voraussetzungen zu schaffen, um Daten aus Forschung und Patientenversorgung untereinander austauschen zu können. Darüber hinaus entwickeln die Konsortien und Verbundvorhaben IT-Lösungen für spezifische Anwendungen („Use Cases“), für die der standortübergreifende Austausch von Forschungs- und Versorgungsdaten genutzt werden soll. Die Konsortien tragen außerdem dazu bei, die Medizininformatik in Deutschland zu stärken.

Das Nationale Steuerungsgremium (NSG) ist die übergeordnete Governance-Struktur der geförderten Konsortien d. h. es steuert die Entwicklung und Umsetzung konsortienübergreifender Standards in der MII. Begleitet wird das NSG vom Dialogforum, welches externe Partner in die strategische Planung und Entwicklung der Medizininformatik-Initiative einbindet. Ergänzend berät ein international besetztes Advisory Board das NSG (s. Abb. 3).

Die Koordinationsstelle organisiert und unterstützt die übergreifende Zusammenarbeit in der Medizininformatik-Initiative. Sie wird von der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung operativ betrieben. An der Geschäftsführung sind gemeinsam mit der TMF auch der Medizinische Fakultätentag (MFT) und der Verband der Universitätsklinika Deutschlands (VUD) beteiligt.

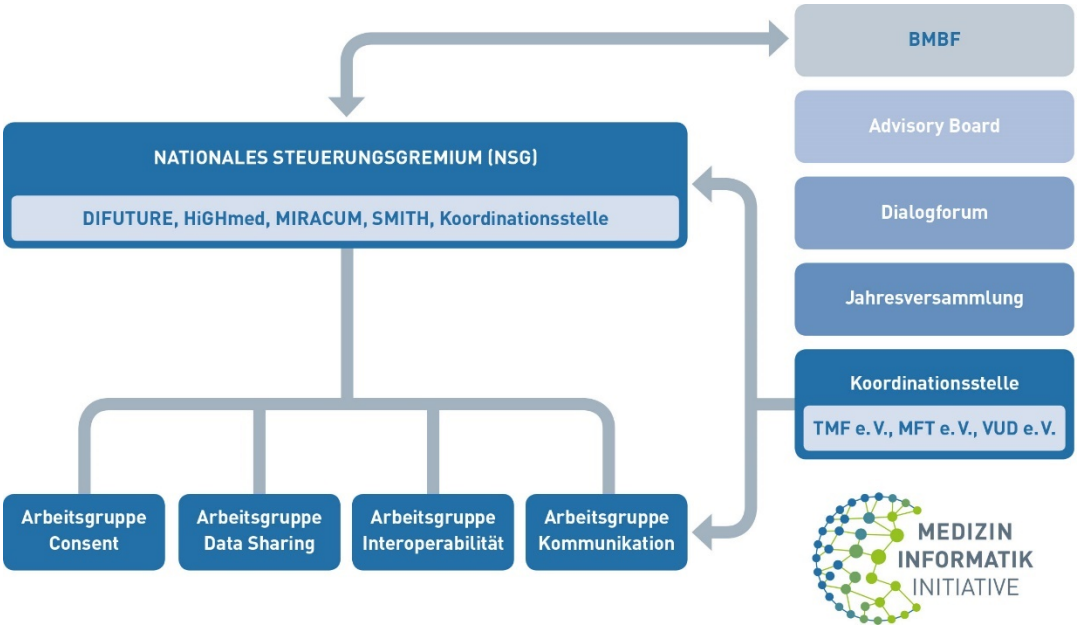

Abb. 3: Organisatorische Struktur der Medizininformatik-Initiative

Das NSG hat bislang vier inhaltlich orientierte Arbeitsgruppen initiiert, in denen die Konsortien gemeinsam daran arbeiten, die Voraussetzungen zu schaffen, um Daten aus Forschung und Patientenversorgung untereinander austauschen zu können. Darüber hinaus sollen die Arbeitsgruppen „Datenschutz“ und „IT-Infrastruktur und Qualitätsmanagement“ der TMF genutzt werden, wo es thematische Überschneidungen gibt. Das Nationale Steuerungsgremium hat in der Konzeptphase explizit entschieden, zu diesen übergeordneten Themenfeldern keine parallelen Arbeitsgruppen zu den bereits etablierten und bewährten Gremien der TMF zu schaffen. Entsprechend ist die AG Datenschutz der TMF auch in die Entwicklung des vorliegenden generischen Datenschutzkonzepts der MII eingebunden.

1.2 Aktueller Status und Grenzen des vorliegenden Konzepts

Die aktuell vorliegende Version dieses Konzepts ist die erste mit dem NSG abgestimmte Version eines übergreifenden Datenschutzkonzepts der MII, die insbesondere die datenschutzrechtlichen Rahmenbedingungen des 6. Projectathons der MII abbilden und allen beteiligten Stellen die Durchführung einer Datenschutz-Folgenabschätzung anhand der in diesem Dokument enthaltenen, generischen Datenschutz-Folgenabschätzung zu übergreifenden Anwendungsszenarien ermöglichen soll. Da bislang noch nicht alle relevanten Verfahren, Schnittstellen und technischen Rahmenbedingungen final spezifiziert sind und die MII für weitere Spezifikationsschritte auch auf die Erfahrungen aus den Projectathons setzt, ist auch dieses Konzept notwendigerweise in weiteren Iterationsschritten an neue Erkenntnisse und Festlegungen anzupassen. Dies schließt auch die Erarbeitung von Vorgaben für die Authentifizierung und Autorisierung von Benutzern im Rahmen der hier adressierten Anwendungsszenarien ein.

Aktuell fokussiert dieses Dokument nur die folgenden drei übergreifenden Basis-Anwendungsszenarien:

- Machbarkeitsanfragen
- Daten-Nutzung im Sinne verteilter Analysen
- Daten-Nutzung im Sinne von Daten-Überlassung

Entsprechend werden die folgenden Anwendungsszenarien bzw. Use Cases im vorliegenden Dokument noch nicht behandelt:

- Überlassung von Bio-Proben (Biomaterial)
- spezifische Use Cases aus den Konsortien, ggf. auch Use Cases mit Versorgungsbezug (diese werden ggf. in übergreifenden Datenschutzkonzepten der Konsortien behandelt)
- Anwendungsfälle und Verarbeitungen die nur standortbezogen an einem DIZ-Standort ablaufen (hierzu wird auf die Datenschutzkonzepte der Standorte verwiesen)

Die schon in der Umsetzung befindlichen übergreifenden Use Cases der Verbundvorhaben zu seltenen Erkrankungen (Collaboration on Rare Diseases, CORD-MI) und Polypharmazie (Polypharmacy – Drug Interactions – Risks, POLAR-MI) können sich auf dieses Datenschutzkonzept beziehen, soweit sie die hier beschriebenen Basis-Anwendungsszenarien umsetzen. Abweichungen hiervon sind in eigenständigen Datenschutzkonzepten zu beschreiben. Dasselbe gilt für ggf. weitere übergreifende Use Cases in der MII.

Mit der Fokussierung auf die übergreifenden Basis-Anwendungsszenarien geht auch einher, dass diese Version des übergreifenden Datenschutzkonzepts der MII noch keine allgemeinen technischen und organisatorischen Mindeststandards für beteiligte Standorte enthält. Zudem fokussiert dieses Konzept auf den Umgang mit Patientendaten (s. Abschnitt 5.1), so dass die datenschutzrechtlich ebenfalls relevante Verarbeitung von personenbezogenen Daten von Antragstellern (s. Definition in Kap. 1.4.2) hier nicht behandelt wird. Diese wird zunächst in entsprechenden Dokumenten und Regelwerken des Forschungsdatenportals (vormals ZARS) beschrieben und festgelegt bzw. ist Teil vertraglicher Regelungen zwischen dem Forschungsdatenportal und den DIZ-Standorten.

Ebenfalls wird in dieser Version des Datenschutzkonzepts noch nicht die Methode der sicheren Mehrparteienberechnung (secure multi-party computation, SMPC) behandelt, auch wenn diese von einzelnen Akteuren der MII bereits mit Testdaten erprobt und die Anwendbarkeit intensiv erforscht wird.

Diese und voraussichtlich auch folgende Versionen dieses Datenschutzkonzepts verweisen bei der notwendigen Rechtsgrundlage für viele Verarbeitungsprozesse auf die Einwilligungsdokumente der MII und die hierfür in der zugehörigen Handreichung beschriebenen Rahmenbedingungen.[1] Die Nutzung alternativer Einwilligungsdokumente bzw. die Anpassung der Einwilligungsdokumente der MII über die in der Handreichung beschriebenen Grenzen hinaus wird in diesem Datenschutzkonzept nicht thematisiert. DIZ-Standorte, die mit solchen Alternativen arbeiten oder die Grenzen der Handreichung in begründeten Fällen umgehen, müssen insofern gesondert prüfen, ob entsprechende Teile dieses übergreifenden Datenschutzkonzepts auch für sie anwendbar sind.

Mit dem Verweis auf die aktuellen Einwilligungsdokumente der MII ist auch die Einschränkung verbunden, dass sich dieses Konzept, insoweit eine Einwilligung als Rechtsgrundlage vorausgesetzt wird, nur auf die Nutzung von Daten einwilligungsfähiger, erwachsener Patienten bezieht.

1.3 Weitere relevante Dokumente

- Übergreifende Nutzungsordnung der MII (NO) in der Version 1.1
  https://www.medizininformatik-initiative.de/de/nutzungsordnung

[1] alle Dokumente unter https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung

- Muster-Nutzungsvertrag der MII (NV), samt Allgemeinen Nutzungs- und Vertragsbedingungen (ANVB) sowie Nutzungsantragsformular und Handreichung jeweils in der Version 1.3 https://www.medizininformatik-initiative.de/de/nutzungsvertrag
- Einwilligungsdokumente der MII (Version 1.6d) samt Handreichung (Version 0.9d) und Positionspapieren der AG Consent der MII https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung
- Kerndatensatz der MII https://www.medizininformatik-initiative.de/de/der-kerndatensatz-der-medizininformatik-initiative

1.4 Begriffsbestimmungen

Für die Begriffsbestimmungen wird auf die Definitionen in Ziff. 1 der übergreifenden NO Bezug genommen. In Ergänzung zu den dort genannten Begriffsbestimmungen, bezeichnet der nachfolgende Begriff:

1.4.1 Nutzungsinteressent

die natürliche Person, die beim Forschungsdatenportal (vormals ZARS) registriert ist, und zu wissenschaftlichen Zwecken Machbarkeitsanfragen über das Forschungsdatenportal ausführt. Mit Einreichung eines Antrags auf Daten-Nutzung wird aus dem Nutzungsinteressent der Antragsteller.

1.4.2 Antragsteller

die natürliche oder juristische Person, die mit der Einreichung eines Nutzungsantrages (vgl. Ziff. 1.4 NO) zu einem geplanten Nutzer-Projekt (vgl. Ziff. 1.7. NO) den Abschluss eines Nutzungsvertrages auf Daten-Nutzung (vgl. Ziff. 1.6 NO) bezweckt. Mit Abschluss des Datennutzungsvertrages wird der Antragsteller Nutzer im Sinn von Ziff. 1.20 NO.

1.4.3 DIZ-Standort

die juristische Person, die in eigener Verantwortung ein Datenintegrationszentrum (vgl. Ziff. 1.12 NO) unterhält (vgl. Ziff. 1.19 NO).

1.4.4 Potentielle Geber

die DIZ-Standorte, die einen Nutzungsantrag geprüft und ihre grundsätzliche Bereitschaft erklärt haben, Geber im Rahmen eines Nutzungsvertrags auf Basis dieses Nutzungsantrags zu werden.

1.4.5 Übergreifende Treuhandstelle

eine in Ergänzung zu den Treuhandstellen der DIZ-Standorte nach Ziff. 1.14 NO in einem Nutzer-Projekt ggf. festgelegte Stelle, die dafür sorgt, dass in den einem Nutzer bereitgestellten Patientendaten von mehreren Gebern anhand einer eindeutigen pseudonymen Kennzeichnung möglichst erkennbar wird, welche Datensätze von unterschiedlichen Gebern zu ein und demselben Patienten gehören.

2. Anwendungsfälle und Zwecke der Datenverarbeitung

Die MII hat das übergreifende Ziel, medizinische Forschung und Versorgung mit Hilfe informatischer Methoden und Expertise zum Nutzen beider Anwendungsfelder stärker zu integrieren. Diese Ziele werden in der MII im Rahmen der konsortialen Use Cases, der übergreifenden Use Cases POLAR und CORD sowie vieler weiterer begleitender Aktivitäten und Projekte in vielfältiger Weise verfolgt. Dieses Datenschutzkonzept behandelt in der aktuellen Version jedoch nur die standortübergreifende Nutzung von klinischen Versorgungsdaten zu Zwecken der medizinischen Forschung. Der hauptsächliche Grund hierfür ist, dass die MII in der aktuellen Förderphase hinsichtlich der konsortienübergreifenden Standardisierung insbesondere diese Nachnutzung von Versorgungsdaten der beteiligten Standorte stark fokussiert hat. Zudem ist die Nachnutzung dieser Patientendaten aus datenschutzrechtlicher Sicht besonders sensibel.

Diese Nutzbarmachung von aus der klinischen Versorgung stammenden Routinedaten soll aus Sicht der MII tatsächlich vielfältige medizinische Forschungszwecke unterstützen. Insbesondere soll eine krankheitsübergreifende Nutzbarkeit der Daten gewährleistet werden. Eine ausführliche Erläuterung und Begründung dieses Ansatzes findet sich in einem Positionspapier der Arbeitsgruppe (AG) Consent der MII.[2]

Gleichzeitig sollen aber nicht schrankenlose Zwecke unterstützt werden. Auch der Begriff der medizinischen Forschung wird in den Einwilligungsdokumenten der MII nochmal einschränkender dahingehend definiert, dass darunter ausschließlich Forschung verstanden wird, die dazu dient, die Erkennung, Behandlung oder Vorbeugung von Krankheiten zu verbessern. Die Entwicklung biologischer Waffen oder diskriminierende Forschungsziele werden zudem explizit ausgeschlossen.

Diese breit formulierten Ziele sollen mit den drei im Folgenden ausführlicher beschriebenen Anwendungsszenarien verfolgt werden können.

2.1 Machbarkeitsanfragen

Mit Machbarkeitsanfragen wird ermittelt, ob für eine bestimmte wissenschaftliche Fragestellung ausreichend Datensätze in einer Datenbasis vorhanden sind. Hierzu wird die Anzahl bestimmter vorhandener Fälle (Fallzahl) in einer Datenbasis ermittelt, die einerseits nach bestimmten Kriterien wie etwa Alter, Geschlecht und Diagnose sowie andererseits nach dem Vorhandensein bestimmter Daten zu diesen Fällen ausgewählt sind. Die angefragte Datenbasis kann zentral oder wie in der MII verteilt (auf die Datenintegrationszentren) organisiert sein.

Für die von der Machbarkeitsanfrage zurückgegebene Fallzahl wird mit zusätzlichen Prüf- und ggf. Veränderungsmaßnahmen sichergestellt, dass in jedem Fall Anonymität gewährleistet wird. Zudem wird für die am Kerndatensatz der MII orientierte Auswahl der für Machbarkeitsanfragen verfügbaren Datenbasis sowie durch weitere mit den Standorten vereinbarte Sicherungsmaßnahmen gewährleistet, dass wirtschaftliche Interessen der Standorte bei Machbarkeitsanfragen ausreichend geschützt werden.

[2] s. https://www.medizininformatik-initiative.de/sites/default/files/2018-11/MII_AG-Consent_Begruendung-Krankheits%C3%BCbergreifender-Consent.pdf

2.2 Verteilte Analysen

Nach Ziffer 1.8 der übergreifenden Nutzungsordnung der MII sind verteilte Analysen ein Ansatz der Nutzung der in den Datenintegrationszentren der MII erhobenen Patientendaten in der Art, dass die sensiblen Patientendaten selbst nicht herausgegeben werden. Stattdessen werden die Analysemethoden vom Forscher über eine zentrale Plattform bereitgestellt und dann an die beteiligten Stellen verteilt, so dass sie die eigentliche Auswertung der Daten jeweils verteilt und lokal in den beteiligten Datenintegrationszentren stattfindet.

Für die rechtliche Betrachtung soll davon ausgegangen werden, dass die Ergebnisse dieser verteilten Analysen, die an den Forscher übermittelt werden, nach Ziffer 1.8 der übergreifenden Nutzungsordnung der MII keinen Personenbezug mehr aufweisen.

2.3 Daten-Herausgaben

In Ergänzung zur Methodik der verteilten Analysen sollen die im Rahmen der MII an den beteiligten Standorten mit einem DIZ gesammelten Daten auch für konkrete Forschungsprojekte herausgegeben werden können. In diesen Fällen erhalten externe Forscher die pseudonymisierten Individualdaten zwecks Durchführung ihrer Auswertungen. Da die Daten im Regelfall von mehreren Standorten kommen, werden sie vor der Herausgabe an die Forscher an einer Stelle zentral zusammengeführt und von dort zentral an den Forscher übergeben. Ggf. wird im Rahmen der Zusammenführung der Daten vor der Herausgabe auch noch ein Record Linkage durchgeführt, so dass für die Forscher erkennbar wird, welche Datensätze von verschiedenen Standorten zu ein und demselben Patienten gehört.

Derzeit ist die Herausgabe von Daten auf Forscher aus den Ländern der EU bzw. aus Ländern, für die die Europäische Kommission eine Angemessenheit des Datenschutzniveaus festgestellt hat, beschränkt.

3. Rechtsgrundlagen

Zunächst werden in diesem Abschnitt die wichtigsten Gesetze mit ihrem jeweiligen Anwendungsbereich beschrieben. Im Anschluss wird dargestellt, auf welche Rechtsgrundlagen bestimmte Verarbeitungsprozesse konkret gestützt werden können.

3.1 Anwendbares Recht

3.1.1 Europäische Datenschutz-Grundverordnung

Die Europäische Datenschutz-Grundverordnung (DSGVO) trat am 25.05.2016 in Kraft und gilt seit dem 25.05.2018 unmittelbar in den Mitgliedstaaten der Europäischen Union. Nationale Gesetze sind seit diesem Datum für datenschutzrechtliche Belange nur insoweit relevant, als dass sie sich auf entsprechende Öffnungsklauseln in der DSGVO stützen können. Da die DSGVO als Grundverordnung allerdings sehr weitgehende Öffnungsklauseln enthält, die den Nationalstaaten gerade auch im Umgang mit besonderen Kategorien personenbezogener Daten nach Art. 9 (1) DSGVO, wie etwa Gesundheitsdaten, eigenständige bzw. abweichende Regelungen erlauben, ist im Regelfall auch immer der nationale Rechtsrahmen ausführlich zu prüfen [1].

3.1.2 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) in seiner aktuell gültigen Fassung trat mit Geltungsbeginn der DSGVO am 25.05.2018 in Kraft. Das BDSG findet Anwendung bei öffentlichen Stellen des Bundes und Länder sowie bei nicht-öffentlichen Stellen. Die Anwendbarkeit bei öffentlichen Stellen der Länder ist jedoch nur dann gegeben, wenn keine Regelungen zum Datenschutz innerhalb der Landesgesetzgebung vorhanden sind oder die öffentlichen Stellen der Länder im Wettbewerb mit nicht-öffentlichen Stellen stehen und somit nach § 2 (5) BDSG als nicht-öffentliche Stellen im Sinne des BDSG gelten und entsprechende landesgesetzliche Regelungen die Anwendbarkeit des BDSG regeln.

Die von diesem übergreifenden Datenschutzkonzept der MII zunächst betroffenen Universitätsklinika Deutschlands sind bis auf die Klinika in Gießen und Marburg öffentliche Stellen der Länder. Die Klinika Gießen und Marburg sind in der Universitätsklinikum Gießen und Marburg GmbH als Teil der Rhön-Klinikum AG zusammengeschlossen. Für die Klinika als öffentliche Einrichtungen der Länder wird im Folgenden der Argumentation von Schneider gefolgt und eine Wettbewerbssituation sowohl bei den Versorgungsfällen [2, S. 152ff] als auch im Bereich von Forschungszuwendungen angenommen [3, S. 91f]. Insoweit wird auch für diese Klinika nach § 2 (5) BDSG und den entsprechenden Verweisen in den Landesdatenschutzgesetzen (z. B. § 2 (6) Berliner Datenschutzgesetz) von einer mindestens teilweisen Anwendbarkeit des BDSG ausgegangen. Für alternative Sichtweisen wird an entsprechenden Stellen dieses Konzepts auf die Konsequenzen hingewiesen.

Nach § 1 (2) BDSG gehen andere Rechtsvorschriften des Bundes zum Datenschutz dem BDSG immer vor. Das BDSG ist nur insoweit anzuwenden, als die spezifischeren Regelungen nicht oder nicht abschließend gelten. Insbesondere bleiben gesetzliche Geheimhaltungspflichten oder Berufsgeheimnisse von den Regelungen des BDSG unberührt. Insofern geht die insbesondere berufsrechtlich (vergl. § 9 der Musterberufsordnung (MBO) der Bundesärztekammer) und strafrechtlich (§ 203 StGB) geregelte ärztliche Schweigepflicht dem BDSG immer vor. Regelungen des BDSG können insoweit nicht als Offenbarungsbefugnisse interpretiert werden.

3.1.3 Landesdatenschutzgesetze

Die Datenschutzgesetze der 16 Bundesländer wurden mittlerweile alle vollständig an die vorrangige Geltung der DSGVO angepasst und im Zuge dieser Anpassung z. T. auch modernisiert. Wie schon zum BDSG ausgeführt, können sich auch die Landesdatenschutzgesetze auf weitgehende Öffnungsklauseln der DSGVO stützen und so den Datenschutz landesspezifisch in den Grenzen der DSGVO ausgestalten.

Die Anwendbarkeit für öffentliche Stellen der Länder ist eingeschränkt, wenn für diese ein Wettbewerbsverhältnis mit nicht-öffentlichen Stellen angenommen werden muss. Insoweit ist auch die Anwendbarkeit für die hier im Fokus stehenden Universitätsklinika als öffentlichen Stellen der Länder (mit Ausnahme von Gießen und Marburg) eingeschränkt, da für diese von einem Wettbewerb mit privat getragenen bzw. nicht-öffentlichen Stellen sowohl um Versorgungsfälle als auch um Forschungszuwendungen auszugehen ist (s. o.).

Die Regelungen der ärztlichen Schweigepflicht werden in aller Regel von den Landesdatenschutzgesetzen ebenso wenig modifiziert wie vom BDSG. Im Einzelfall kann aber eine Erlaubnisnorm aus einem Landesdatenschutzgesetz sich ausreichend konkret auf das besonders geschützte Verhältnis von Arzt und Patient sowie die in diesem Rahmen erhobenen Daten beziehen, dass sie auch als Offenbarungsbefugnis angesehen werden kann.

3.1.4 Landeskrankenhausgesetze

In fast allen Bundesländern gibt es für den Bereich der stationären Versorgung Landeskrankenhausgesetze (in Nordrhein-Westfalen das analoge Gesundheitsdatenschutzgesetz). Die Anpassung an die DSGVO ist noch nicht in allen Ländern vollständig abgeschlossen. Auch vor der Anwendbarkeit der DSGVO verabschiedete Gesetze können allerdings anzuwenden sein, wenn ihre Geltung auf entsprechende Öffnungsklauseln der DSGVO gestützt werden kann. Im Regelfall ist von einer vorrangigen Geltung des Krankenhausrechts vor dem Landes- bzw. Bundesdatenschutzgesetz auszugehen, auch wenn dies für jedes Bundesland sowie für die spezifische Trägerschaft und Rechtsform eines Krankenhauses immer im Einzelfall zu prüfen ist. Eine ausführliche Analyse dieses spezifischen Rechtsrahmens in allen Bundesländern und für unterschiedliche getragene Krankenhäuser liegt leider nur aus der Zeit vor Einführung der DSGVO vor [3]. Die in der Analyse von Schneider genannten Kriterien der Anwendbarkeit bzw. des Vorrangs bestimmter Gesetze lassen sich jedoch grundsätzlich auch auf die heutige Situation anwenden.

3.1.5 Sozialgesetzbuch

Für die Verarbeitung von Daten, die auch im Rahmen der gesetzlichen Krankenversicherung (GKV) erhoben bzw. verwendet werden, sind die Regelungen der „Bücher des Sozialgesetzbuchs“ zu beachten. Das in § 35 SGB I i. V. m. §§ 67 ff. SGB X geregelte Sozialdatenschutzrecht sieht nach § 35 (2) Satz 1 SGB I explizit vor, dass die Regelungen des Sozialgesetzbuchs den Sozialdatenschutz abschließend regeln, allerdings nur insoweit die Regelungen der DSGVO nicht unmittelbar anzuwenden sind. Zu beachten ist dabei, dass viele Daten aus der klinischen Versorgung innerhalb mehrerer Kontexte Verwendung finden und somit mehrere gesetzliche Rahmenbedingungen Anwendung finden können. So wird eine Diagnose zwar auch zu Abrechnungszwecken weiterverarbeitet und unterfällt soweit dem Sozialrecht und dem zugehörigen Sozialdatenschutz. Primär dient die Dokumentation einer Diagnose beispielsweise aber auch der ärztlichen Dokumentationspflicht nach § 630f BGB (s. u.). Insofern wäre das Sozialdatenschutzrecht nur insoweit abschließend und in Ergänzung zur DSGVO anzuwenden, als es um den Kontext der

Verwendung einer Diagnose als Sozialdatum geht. Im Übrigen wären aber auch z. B. auch die Bestimmungen des Krankenhausrechts (s. o.) anzuwenden.

Im vorliegenden Kontext finden die Bestimmungen des Sozialgesetzbuchs insbesondere in Bezug auf die Verwendung von Daten der gesetzlichen Krankenkassen Beachtung. Eine aktuelle Darstellung der für die Nachnutzung von Sozialdaten für die Forschung relevanten Bestimmungen des SGB findet sich in [4].

Unklar ist noch, inwieweit die sehr neue Regelung aus § 287a SGB V zur einheitlichen Anwendung von § 27 BDSG bei länderübergreifenden Forschungsvorhaben, wie sie im Rahmen der MII eher die Regel als die Ausnahme darstellen dürften, zur Anwendung kommen kann.

3.1.6 Bürgerliches Gesetzbuch und Berufsordnungen

Die Dokumentationspflichten im Rahmen der Behandlung ergeben sich für Ärztinnen und Ärzte aus § 630f Bürgerliches Gesetzbuch (BGB). Zusätzlich sind die untergesetzlich, berufsrechtlich normierten Pflichten aus den Berufsordnungen zu beachten (vergl. § 10 MBO). Entsprechend sind auch unterschiedliche Rechtsgrundlagen für die Einsichtnahme in die ärztliche Dokumentation nach § 630g BGB einerseits und die datenschutzrechtlichen Auskunftsrechte nach Art. 15 DSGVO andererseits zu beachten (vergl. hierzu [5]).

3.2 Anwendungsfälle und Rechtsgrundlagen

3.2.1 Machbarkeitsanfragen

3.2.1.1 Zusammenfassende Darstellung der Rechtsgrundlage

Die lokale Verarbeitung personenbezogener Daten zur Unterstützung von Machbarkeitsanfragen, die anderen Zwecken als der Behandlung der von der Verarbeitung betroffenen Patientinnen und Patienten dient, kann als Rechtsgrundlage auf den Behandlungsvertrag bzw. die jeweils für die Erhebung der Daten lokal anwendbare Rechtsgrundlage gestützt werden. Die Weitergeltung dieser Rechtsgrundlage ergibt sich aus der Vereinbarkeit des Zwecks der Machbarkeitsanfrage mit dem ursprünglichen Erhebungs- und Verarbeitungszweck gemäß Art. 6 (4) DSGVO. Entsprechend Art. 5 (1) b in Verbindung mit dem Erwägungsgrund Nr. 50 DSGVO ist somit keine neue Rechtsgrundlage für die Verarbeitung zu Zwecken der Machbarkeitsanfragen notwendig.

Hilfsweise kann die Verarbeitung auch auf eine Interessensabwägung nach § 27 (1) BDSG gestützt werden, wobei von einem erheblichen Überwiegen des Interesses der verantwortlichen Einrichtungen an der Unterstützung von Forschungsprojekten durch Machbarkeitsanfragen gegenüber den Interessen der Betroffenen an einem Ausschluss ihres Datensatzes von einem reinen Zählvorgang ausgegangen werden kann. Für die Klinika als öffentliche Einrichtungen der Länder wird der Argumentation von Schneider [3, S. 91f] gefolgt und eine Wettbewerbssituation sowohl bei den Versorgungsfällen als auch im Bereich von Forschungszuwendungen angenommen. Insoweit wird nach § 2 (5) BDSG und den entsprechenden Verweisen in den Landesdatenschutzgesetzen (z. B. § 2 (6) Berliner Datenschutzgesetz) von einer Anwendbarkeit von § 27 BDSG ausgegangen. Alternativ wird auf die noch neue und hinsichtlich ihrer Anwendbarkeit noch nicht abschließend bewertbare Regelung in § 287a SGB V für länderübergreifende Forschungsprojekte verwiesen.

Im Fall einer Nicht-Anwendbarkeit von § 27 BDSG kann die Verarbeitung hilfsweise auf vergleichbare Regelungen im jeweils anwendbaren Krankenhausrecht (z. B. § 27 (4) Bayerisches Krankenhausgesetz

oder § 25 (1) Berliner Landeskrankenhausgesetz) oder Landesdatenschutzrecht (z. B. § 13 Niedersächsisches Datenschutzgesetz oder § 13 Landesdatenschutzgesetz Baden-Württemberg) gestützt werden. Da für die mit den Machbarkeitsanfragen angestrebten Zwecke nicht nur von einem relevanten Interesse der verantwortlichen Einrichtungen sondern auch von einem relevanten öffentlichen Interesse ausgegangen werden kann, spielt es für die Abwägung mit den vergleichsweise geringen Interessen der Betroffenen an einem Ausschluss ihrer Daten bei dieser Art der Verarbeitung keine Rolle, welches Abwägungsziel konkret in den jeweiligen Forschungsklauseln genannt wird.

3.2.1.2 Ausführliche Darstellung und Begründung zur Rechtsgrundlage

Da die von den Standorten an eine zentrale, die Anfrage koordinierende Stelle übermittelten Daten (Anzahlen gefundener Treffer, die den Anfragekriterien entsprechen) nach ggf. notwendiger Verrauschung oder Anwendung anderer Sicherheitsmaßnahmen keinen Personenbezug mehr aufweisen, handelt es sich bei dieser Übermittlung nicht um eine Übermittlung im datenschutzrechtlichen Sinne. Insofern ist für die Übermittlung auch keine datenschutzrechtliche Rechtsgrundlage notwendig. Zudem ist das lokale Zählen der Daten so auszugestalten, dass keine Offenbarung im Sinne der ärztlichen Schweigepflicht nach § 203 StGB oder § 9 MBO stattfindet. Insofern ist für die Unterstützung von Machbarkeitsanfragen auch keine entsprechende Offenbarungsbefugnis notwendig.

Die hierfür notwendige lokale Verarbeitung der Daten wird jedoch auf einer Datenbasis stattfinden, die selbst noch Personenbezug der Daten aufweist. Insofern wird heute überwiegend davon ausgegangen, dass für eine solche Verarbeitung gemäß Art. 4 Nr. 2 DSGVO eine Rechtsgrundlage vorliegen muss. Zu beachten ist dabei, dass das Zählen der Daten für die Machbarkeitsanfrage einer anderen Zwecksetzung als die Erhebung der Daten im Kontext der Versorgung folgt. Gemäß dem datenschutzrechtlichen Prinzip der Zweckbindung in Art. 5 (1) b in Verbindung mit Erwägungsgrund Nr. 50 Satz 2 DSGVO ist hierfür eine eigenständige Rechtsgrundlage erforderlich, es sei denn, der neue Verarbeitungszweck ist mit dem ursprünglichen Zweck vereinbar. Auch Art. 6 (4) DSGVO weist darauf hin, dass die Prüfung von Zwecken auf eine Vereinbarkeit nur zu erfolgen hat, wenn für die Verarbeitung zum neuen Zweck keine eigenständige Rechtsgrundlage im Sinne einer Einwilligung oder einer Rechtsvorschrift der Union oder der Mitgliedstaaten vorliegt.

Die Prüfung der Vereinbarkeit hat nach den in Art. 6 (4) DSGVO genannten Kriterien zu erfolgen:

- Zunächst ist nach Art. 6 (4) a zu prüfen, ob eine Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht. Wenn der Zweck der Weiterverarbeitung die medizinische Forschung in dem Sinne ist, dass Erkrankungen vermieden werden (Prävention) oder eine Verbesserung der Behandlung erreicht werden soll (Diagnostik und Therapie), so kann durchaus von einer Verbindung zur ursprünglichen Behandlung, zu deren Zweck die Daten erhoben wurden, ausgegangen werden. Voraussetzung hierfür ist, dass die Machbarkeitsanfragen tatsächlich auf die Prüfung solcher Forschungsprojekte begrenzt werden, die eine Verbesserung von Prävention, Diagnostik oder Therapie von Erkrankungen zum Ziel haben. Eine Verbindung der Zwecke wird auch dadurch nicht aufgehoben, dass die Forschung, zu deren Unterstützung die Machbarkeitsanfrage durchgeführt wird, möglicherweise auf eine andere Erkrankung abzielt, als die, an der ein von der Zählung seines Datensatzes betroffener Patient leidet. Möglicherweise wird in solchen Fällen die Verbindung allenfalls etwas weniger direkt sein, wobei darauf hinzuweisen ist, dass die aktuelle medizinische Forschung immer weitergehend dazu in der Lage ist, komplexe Zusammenhänge zwischen verschiedenen Erkrankungsgebieten aufzuzeigen. Die AG Consent der MII hat hierzu im Rahmen der

Begründung einer krankheitsübergreifenden Einwilligungserklärung („broad consent“) eine ausführliche Stellungnahme verfasst.[3] Auch dass die hier relevante Machbarkeitsanfrage selbst noch keine wissenschaftliche Fragestellung beantwortet, ist im Sinne der Verbindung der Zwecke nicht negativ zu bewerten. Gerade aus Sicht des Datenschutzes ist es von hohem Wert, wenn die sensiblen personenbeziehbaren Gesundheitsdaten der betroffenen Patientinnen und Patienten nur für die Forschung genutzt oder gar herausgegeben werden, wenn mit den Daten tatsächlich auch die gestellte Frage beantwortet werden kann. Hierfür sind Machbarkeits-Abschätzungen im Vorfeld häufig unverzichtbar.

- Nach Art. 6 (4) b DSGVO ist der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, zu berücksichtigen, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen. Diesbezüglich kann davon ausgegangen werden, dass zwischen den betroffenen Personen und der die Zählung durchführenden Stelle, also der behandelnden Einrichtung, ein besonderes Vertrauensverhältnis besteht. Dadurch, dass die Zählung gerade lokal in den behandelnden Einrichtungen erfolgt und hierfür die Daten nicht schon herausgegeben werden, kann gerade dieser hier zu prüfende Zusammenhang in hohem Maße gewährleistet werden. Hierfür ist es auch unschädlich, dass durch die standortübergreifende Abstimmungsnotwendigkeit zu den Möglichkeiten und Grenzen einer Machbarkeitsanfrage die das zentrale Portal betreibende Stelle nach Art. 26 DSGVO formal mit verantwortlich für die Durchführung von Machbarkeitsanfragen wird. Es kann davon ausgegangen werden, dass für die betroffenen Patienten besonders relevant ist, dass bei diesem Verfahren ihre Daten die behandelnde Einrichtung nicht verlassen.
- Nach Art. 6 (4) c ist die Art der personenbezogenen Daten zu berücksichtigen, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 (1) DSGVO verarbeitet werden. Tatsächlich sind von der Verarbeitung besondere Kategorien personenbezogener Daten gemäß Art. 9 (1) DSGVO betroffen, in diesem Falle Gesundheitsdaten. Insofern muss die Prüfung der übrigen Kriterien strenger erfolgen, als dies bei der Verarbeitung anderer Daten der Fall wäre.
- Nach Art. 6 (4) d DSGVO sind die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen zu prüfen. Da im Rahmen der Machbarkeitsanfragen nur temporär vollständig anonyme Fallzahlen erstellt und übermittelt werden, ist von keinerlei kritischen Folgen für die Betroffenen auszugehen. Hierfür muss allerdings sichergestellt sein, dass die lokale Verarbeitung tatsächlich auf die temporäre Erstellung vollständig anonymer Fallzahlen beschränkt bleibt.
- Nach Art. 6 (4) e ist schließlich das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann, zu berücksichtigen. Da die Anonymität grundsätzlich als aus Sicht des Datenschutzes beste Schutzmaßnahme und Garantie anzusehen ist, insbesondere als noch stärkere Schutzmaßnahme als die Pseudonymisierung oder Verschlüsselung, kann hier in jedem Falle von einer ausreichenden Garantie ausgegangen werden.

Zusammenfassend ist festzuhalten, dass von den fünf in Art. 6 (4) DSGVO genannten Prüfkriterien vier zu einem positiven oder sogar sehr positiven Ergebnis führen. Zum fünften Prüfkriterium, der Art der Daten, ist festzustellen, dass hier besondere Kategorien personenbezogener Daten verarbeitet werden. Insgesamt kann vor dem Hintergrund dieser ausführlichen Prüfung von einer Zweckvereinbarkeit ausgegangen werden. Zusätzlich ist auf die vom Gesetzgeber in Art. 5 (1) b DSGVO zum Ausdruck

[3] https://www.medizininformatik-initiative.de/sites/default/files/2018-11/MII_AG-Consent_Begruendung-Krankheits%C3%BCbergreifender-Consent.pdf

gebrachte Privilegierung wissenschaftlicher Forschungszwecke hinzuweisen, die im vorliegenden Fall ergänzend zu berücksichtigen ist.

Damit übereinstimmend kam auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in einem Positionspapier vom Juni 2020 zu dem Schluss, dass für anonymisierende Vorgänge – immer abhängig von der Prüfung im Einzelfall – grundsätzlich eine Zweckvereinbarkeit nach Art. 6 (4) DSGVO mit Weitergeltung der ursprünglich für die Erhebung der Daten geltenden Rechtsgrundlage nach Art. 5 (1) b in Verbindung mit Erwägungsgrund Nr. 50 DSGVO angenommen werden kann [6]. Dabei ist zu berücksichtigen, dass die Anonymisierung im datenschutzrechtlichen Sinne nur über das Ergebnis definiert ist, welches den Kriterien der Anonymität gemäß Erwägungsgrund 26 DSGVO entsprechen muss. Auf welche Art und Weise ein solches Ergebnis erreicht wird, also konkret über das Zählen der Datensätze, eine andere Form der Aggregation oder eine Vergröberung der Individualdaten in einer Form, die die Struktur der Daten erhält, ist datenschutzrechtlich nicht definiert und somit in Bezug auf die rechtliche Wertung nicht relevant. Insofern kann das im Rahmen der Machbarkeitsanfragen lokal stattfindende Zählen der Datensätze, welches – ggf. unter Anwendung zusätzlicher Schutzmaßnahmen – zu einem zweifelsfrei anonymen Ergebnis führt, auch als Anonymisieren im Sinne des Positionspapiers des BfDI verstanden werden.

Allerdings ist der in Erwägungsgrund Nr. 50 DSGVO sehr klar zum Ausdruck kommende Grundsatz, dass für die Verarbeitung zu vereinbaren Zwecken nach Art. 6 (4) DSGVO keine neue, eigenständige Rechtsgrundlage benötigt wird, sondern hierfür vielmehr die ursprüngliche Rechtsgrundlage weitergilt, in der Literatur immer noch etwas umstritten. Die Kritik fokussiert dabei stark auf eine vermeintlich eingeschränkte Aussagekraft von Erwägungsgrund Nr. 50 (vergl. etwa [7]) bzw. fordert dessen Anpassung [8, S. 34f]. Dabei wird übersehen, dass die Logik der möglichen Weitergeltung einer bisherigen Rechtsgrundlage weitergehend in der DSGVO verankert ist. Ohne dieses Prinzip würde die notwendige Prüfung auf Vereinbarkeit der Zwecke implizieren, dass unvereinbare Zwecke auch bei Bestehen einer ausreichenden Rechtsgrundlage nicht zulässig wären. Damit würde aus dem die Zweckbindung etwas erweiternden Prinzip der Zweckvereinbarkeit eine die möglichen Rechtsgrundlagen einschränkende Regelung. Dass das so vom Gesetzgeber gewollt oder in den Regelungen der Rechtsgrundlagen schon angelegt wäre, dafür gibt es weder in der DSGVO noch aus dem Gesetzgebungsverfahren Hinweise.

Für die Geltung der ursprünglichen Rechtsgrundlage für vereinbare Zwecke bei der Weiterverarbeitung personenbezogener Daten sprechen auch weitere, in der DSGVO angelegte Privilegierungen, die sich sonst kaum innerhalb des Prinzips der Rechtmäßigkeit nach Art. 6 (1) DSGVO abbilden ließen. Hierzu gehört die in Art. 5 (1) e DSGVO festgelegte Erlaubnis, dass Daten für bestimmte privilegierte Zwecke auch länger in personenbeziehbarer Form gespeichert werden dürfen. In eine ähnliche Richtung geht zudem die Privilegierung in Art. 17 (3) d DSGVO, die das Recht auf Löschung bei einer Verarbeitung für bestimmte Zwecke einschränkt. In beiden Fällen kann eigentlich sinnvollerweise nur die Weitergeltung der ursprünglichen Rechtsgrundlage angenommen werden, insbesondere wenn man vor dem Hintergrund der engen und abschließenden Formulierungen in Art. 6 (1) und Art. 9 (2) DSGVO davon absieht, dass Art. 5 (1) e und Art. 17 (3) d DSGVO eigenständige Rechtsgrundlagen darstellen könnten.

Falls trotz der ausführlichen Begründung dieser hier dargelegten Argumentation nicht gefolgt werden sollte, könnte hilfsweise die lokale Verarbeitung auch auf entsprechende Forschungsklauseln im jeweiligen Landeskrankenhausrecht oder im Datenschutzrecht gestützt werden, die als konkrete Umsetzungen der Öffnungsklausel in Art. 9 (2) j der DSGVO gewertet werden können. Insoweit für die beteiligten Universitätsklinika als im Wettbewerb stehende Einrichtungen eine Anwendbarkeit des BDSG

anzunehmen ist, kann die lokale Verarbeitung auf § 27 (1) BDSG gestützt werden [3, S. 91f]. Aufgrund des mit dem reinen Zählen eines Falls verbundenen minimalen Eingriffs in das Persönlichkeitsrecht der betroffenen Personen sowie des vergleichsweise leicht ausschließbaren Risikos einer Re-Identifizierung der betroffenen Personen anhand einer ggf. sogar noch verrauschten Gesamtzahl von Fällen, ist in dem Fall einer Machbarkeitsanfrage von einem erheblichen Überwiegen der Interessen des Verantwortlichen gegenüber den Interessen der Betroffenen auszugehen.

Der Vollständigkeit halber ist darauf hinzuweisen, dass eine Anwendbarkeit von § 27 BDSG (1) auch auf die Regelung in § 287a SGB V gestützt werden könnte, wenn die Machbarkeitsanfrage bundeslandübergreifend durchgeführt wird. Wie schon weiter oben ausgeführt, bestehen zur Anwendbarkeit der neuen und im Zuge der Pandemiegesetzgebung sehr kurzfristig eingeführten Regelung in § 287a SGB V allerdings noch einige Fragen.

Sollte im Einzelfall an einem Standort die Anwendbarkeit des § 27 (1) BDSG nicht nachvollzogen werden können, müsste hilfsweise überprüft werden, ob es im anwendbaren Krankenhausrecht (Landeskrankenhausgesetz oder Gesundheitsdatenschutzgesetz in NRW) oder im Landesdatenschutzrecht eine dem § 27 (1) BDSG vergleichbare Regelung bzw. Forschungsklausel gibt. Eine vollständige Listung ist an dieser Stelle nicht möglich, beispielsweise sei aber auf die Regelungen in § 27 (4) des Bayerischen Krankenhausgesetzes, § 25 (1) des Berliner Landeskrankenhausgesetzes, § 13 des Niedersächsischen Datenschutzgesetzes oder § 13 des Landesdatenschutzgesetzes Baden-Württemberg verwiesen. Teilweise ist das Interesse der Betroffenen anders als in § 27 (1) BDSG nicht gegen das Interesse des Verantwortlichen, sondern gegen ein öffentliches Interesse an der Durchführung eines Forschungsprojekts abzuwiegen. Für die von der MII als öffentlich geförderter Initiative unterstützten Forschungsprojekte mit Durchführung an den öffentlich getragenen Universitätsklinika in Deutschland kann grundsätzlich auch ein öffentliches Interesse an der Durchführung angenommen werden. Dieses Interesse kann sicherlich unterschiedlich groß ausfallen, dürfte aber im Regelfall immer das sehr geringe Interesse der Betroffenen von dem Ausschluss an einem reinen Zählvorgang erheblich überwiegen.

3.2.2 Verteilte Analysen

3.2.2.1 Zusammenfassende Darstellung der Rechtsgrundlage

Die lokale Verarbeitung personenbezogener Daten im Rahmen der Durchführung verteilter Analysen, die anderen Zwecken als denen der Behandlung der betroffenen Patientinnen und Patienten dient, kann als Rechtsgrundlage auf den Behandlungsvertrag bzw. die für die Erhebung der Daten anwendbare Rechtsgrundlage gestützt werden. Die Weitergeltung dieser Rechtsgrundlage ergibt sich aus der Vereinbarkeit des Zwecks der verteilten Analysen mit dem ursprünglichen Erhebungs- und Verarbeitungszweck gemäß Art. 6 (4) DSGVO. Entsprechend Art. 5 (1) b in Verbindung mit dem Erwägungsgrund Nr. 50 DSGVO ist somit keine neue Rechtsgrundlage für diesen Verarbeitungsschritt im Rahmen verteilter Analysen notwendig.

Hilfsweise kann die Verarbeitung auf eine Interessensabwägung nach § 27 (1) BDSG gestützt werden. Für die Klinika als öffentliche Einrichtungen der Länder wird der Argumentation von Schneider [3, S. 91f] gefolgt und eine Wettbewerbssituation sowohl bei den Versorgungsfällen als auch im Bereich von Forschungszuwendungen angenommen. Insoweit wird nach § 2 (5) BDSG und den entsprechenden Verweisen in den Landesdatenschutzgesetzen (z. B. § 2 (6) Berliner Datenschutzgesetz) von einer Anwendbarkeit von § 27 BDSG ausgegangen. Alternativ wird auf die noch neue und hinsichtlich ihrer

Anwendbarkeit noch nicht abschließend bewertbare Regelung in § 287a SGB V für länderübergreifende Forschungsprojekte verwiesen.

Bei Nicht-Anwendbarkeit von § 27 BDSG kann die Verarbeitung hilfsweise auf vergleichbare Regelungen im jeweils anwendbaren Krankenhausrecht oder Landesdatenschutzrecht gestützt werden. Hilfsweise kann auch auf eine vorliegende Einwilligung wie den Broad Consent der MII als Rechtsgrundlage verwiesen werden.

3.2.2.2 Ausführliche Darstellung und Begründung zur Rechtsgrundlage

Da die von den Standorten an eine zentrale, die verteilte Analyse koordinierende Stelle übermittelten Ergebnisdaten (aggregierte Ergebnisse der jeweiligen lokalen Analyse, also z. B. Mittelwerte und Streuungsmaße) keinen Personenbezug mehr aufweisen, handelt es sich bei dieser Übermittlung nicht um eine Übermittlung im datenschutzrechtlichen Sinne. Insofern ist für die Übermittlung auch keine datenschutzrechtliche Rechtsgrundlage notwendig. Zudem ist die lokale Analyse der Daten so auszugestalten, dass keine Offenbarung im Sinne der ärztlichen Schweigepflicht nach § 203 StGB oder § 9 MBO stattfindet. Insofern ist für die Unterstützung verteilter Analysen auch keine entsprechende Offenbarungsbefugnis notwendig.

Die hierfür notwendige lokale Verarbeitung der Daten wird jedoch auf einer Datenbasis stattfinden, die selbst noch Personenbezug aufweist. Insofern wird heute überwiegend davon ausgegangen, dass für eine solche Verarbeitung gemäß Art. 4 Nr. 2 DSGVO eine Rechtsgrundlage vorliegen muss. Zu beachten ist dabei, dass die Verarbeitung der Daten im Rahmen verteilter Analysen einer anderen Zwecksetzung als die Erhebung und Verarbeitung der Daten im Kontext der Versorgung folgt. Gemäß dem datenschutzrechtlichen Prinzip der Zweckbindung in Art. 5 (1) b in Verbindung mit Erwägungsgrund Nr. 50 Satz 2 DSGVO ist hierfür eine eigenständige Rechtsgrundlage erforderlich, es sei denn, der neue Verarbeitungszweck ist mit dem ursprünglichen Zweck vereinbar. Auch Art. 6 (4) DSGVO weist darauf hin, dass die Prüfung von Zwecken auf eine Vereinbarkeit nur zu erfolgen hat, wenn für die Verarbeitung zum neuen Zweck keine eigenständige Rechtsgrundlage im Sinne einer Einwilligung oder einer Rechtsvorschrift der Union oder der Mitgliedstaaten vorliegt.

Für die detaillierte Prüfung der Vereinbarkeit der Zwecke der verteilten Analysen mit denen der Diagnostik und Behandlung der betroffenen Patienten wird auf Abschnitt 3.2.1.2 mit der Analyse der Zweckvereinbarkeit bei der Durchführung von Machbarkeitsanfragen verwiesen. Im Folgenden werden daher nur noch die für diese Analogie notwendigen Prämissen betrachtet und begründet.

Zunächst ist hierzu festzustellen, dass die Machbarkeitsanfrage einen vorbereitenden Schritt für die Durchführung einer verteilten Analyse darstellt und damit grundsätzlich von einer Zweckidentität beider Verfahren ausgegangen werden kann. Auch wenn nicht alle Machbarkeitsanfragen zu einer Durchführung verteilter Analysen oder gar von Daten-Herausgaben führen, spricht das nicht gegen die Verfolgung identischer Zwecke mit beiden Verfahren. Dass die Machbarkeitsanfrage als lediglich vorbereitender Schritt von der Zweckerreichung weiter entfernt ist als die verteilte Analyse, spricht nicht gegen die Identität der verfolgten Zwecke.

Wenn hier von einer Identität der Zwecke ausgegangen werden kann, ist aber ergänzend auch zu klären, ob die Verarbeitung der personenbezogenen Daten selbst aus datenschutzrechtlicher Perspektive bei beiden Verfahren gleich zu bewerten ist. Da die Prüfung der Vereinbarkeit der Zwecke nach Art. 6 (4) DSGVO insbesondere auch auf die mit der Verarbeitung verbundenen Risiken in Bezug auf die Rechte und

Freiheiten der Betroffenen abhebt, ist diesbezüglich besonders genau zu prüfen, ob von einer Vergleichbarkeit von Machbarkeitsanfragen und verteilten Analysen ausgegangen werden kann.

Während Machbarkeitsanfragen grundlegend auf dem Zählen von Datensätzen nach einer Auswahl anhand bestimmter Kriterien basiert, können im Rahmen verteilter Analysen auch andere Aggregatfunktionen zur Anwendung kommen, wie etwa eine Mittelwertbildung oder die Ermittlung von Streuungsmaßen. Auch bei den verteilten Analysen findet allerdings zuvor eine Auswahl der Daten statt, idealerweise dieselbe wie in einer zuvor vorbereitend durchgeführten Machbarkeitsanfrage. Die Auswahl der Daten ist allerdings bei der verteilten Analyse ein von der eigentlichen Analyse abgetrennter und vorbereitender Schritt, währen diese Auswahl bei der Machbarkeitsanalyse integrativ mit dem Zählschritt verbunden ist. Damit ist festzustellen, dass im Rahmen beider Verfahren eine vergleichbare Auswahl oder Filterung von Daten erfolgt und zudem eine Aggregatfunktion auf die ausgewählten Daten angewandt wird. Somit bleibt zu überprüfen, ob auch diese Aggregatfunktionen als vergleichbar angesehen werden können, wenn man diesbezüglich alleine die datenschutzrechtlichen Risiken berücksichtigt.

Während die Machbarkeitsanfragen immer zu einem Zählen der personenbezogenen Datensätze führen, können im Rahmen verteilter Analysen sehr unterschiedliche Rechenoperationen auf den Daten durchgeführt werden. Diese haben jedoch auch immer Aggregat-Charakter in dem Sinne, dass das Ergebnis der Rechenoperation nur noch etwas über eine Gruppe von Daten und nicht mehr über einzelne Datensätze aussagt. Nach den Festlegungen in der Nutzungsordnung der MII (Ziffer 1.8) ist davon auszugehen, dass die Ergebnisse der Aggregatfunktionen immer anonym im datenschutzrechtlichen Sinne sind. Beispielsweise kann hier von der Ermittlung einer zentralen Tendenz (z. B. Mittelwert oder Median) oder von Streuungsmaßen ausgegangen werden. Wenn aber die unterschiedlichen Rechenoperationen bei Machbarkeitsanfragen einerseits und verteilten Analysen andererseits immer im Ergebnis zu anonymen Größen bzw. Daten führen und zudem die Berechnung selbst in beiden Fällen automatisiert und ohne eine zusätzliche Kenntnisnahme personenbezogener Daten erfolgt, kann aus datenschutzrechtlicher Perspektive eine Vergleichbarkeit der Vorgänge angenommen werden.

Vor diesem Hintergrund wird von einer Vergleichbarkeit der Anwendungsfälle der verteilten Analyse einerseits und der Machbarkeitsanfragen andererseits hinsichtlich der datenschutzrechtlichen Einordnung ausgegangen. Entsprechend kann für die Analyse der Rechtsgrundlagen von verteilten Analysen auf die detaillierte Analyse der Rechtsgrundlagen von Machbarkeitsanfragen in Abschnitt 3.2.1.2 verwiesen werden.

Hilfsweise kann die Verarbeitung auf eine Interessensabwägung nach § 27 (1) BDSG gestützt werden, wobei von einem erheblichen Überwiegen des Interesses der verantwortlichen Einrichtungen an der Unterstützung von Forschungsprojekten durch verteilte Analysen gegenüber den Interessen der Betroffenen an einem Ausschluss ihres Datensatzes von einem lokalen Auswertungs- und Aggregierungsvorgang – hinsichtlich der datenschutzrechtlichen Relevanz mit einem Anonymisierungs- oder Zählvorgang vergleichbar – ausgegangen werden kann. Für die Klinika als öffentliche Einrichtungen der Länder wird der Argumentation von Schneider [3, S. 91f] gefolgt und eine Wettbewerbssituation sowohl bei den Versorgungsfällen als auch im Bereich von Forschungszuwendungen angenommen. Insoweit wird nach § 2 (5) BDSG und den entsprechenden Verweisen in den Landesdatenschutzgesetzen (z. B. § 2 (6) Berliner Datenschutzgesetz) von einer Anwendbarkeit von § 27 BDSG ausgegangen. Alternativ wird auf die noch neue und hinsichtlich ihrer Anwendbarkeit noch nicht abschließend bewertbare Regelung in § 287a SGB V für länderübergreifende Forschungsprojekte verwiesen.

Bei Nicht-Anwendbarkeit von § 27 BDSG kann die Verarbeitung hilfsweise auf vergleichbare Regelungen im jeweils anwendbaren Krankenhausrecht (z. B. § 27 (4) Bayerisches Krankenhausgesetz oder § 25 (1) Berliner Landeskrankenhausgesetz) oder Landesdatenschutzrecht (z. B. § 13 Niedersächsisches Datenschutzgesetz oder § 13 Landesdatenschutzgesetz Baden-Württemberg) gestützt werden. Da für die mit den verteilten Analysen angestrebten Zwecke nicht nur von einem relevanten Interesse der verantwortlichen Einrichtungen sondern auch von einem relevanten öffentlichen Interesse ausgegangen werden kann, spielt es für die Abwägung mit den vergleichsweise geringen Interessen der Betroffenen an einem Ausschluss ihrer Daten bei dieser Art der Verarbeitung keine Rolle, welches Abwägungsziel konkret in den jeweiligen Forschungsklauseln genannt wird. Hilfsweise kann auch auf eine vorliegende Einwilligung wie den Broad Consent der MII als Rechtsgrundlage nach Art. 6 (1) a und Art. 9 (2) a verwiesen werden.

3.2.3 Daten-Herausgaben

3.2.3.1 Zusammenfassende Darstellung der Rechtsgrundlage

Rechtsgrundlage für solche Datenherausgaben ist eine informierte Einwilligung nach Art. 6 (1) a DSGVO, die sich zudem explizit auf Gesundheitsdaten bezieht und insofern nach Art. 9 (2) a als ausdrückliche Einwilligung ausgestaltet sein muss. Hierfür kommt insbesondere die von der AG Consent entwickelte Mustervorlage für eine Einwilligung in die Nutzung von Behandlungsdaten für breit beschriebene Forschungszwecke in der Version 1.6d in Frage, auf die im Weiteren näher eingegangen wird.[4]

Einzelne Landeskrankenhausgesetze enthalten Erlaubnisse für die Herausgabe von pseudonymen Patientendaten aus der Behandlung für Forschungszwecke unter ganz bestimmten Voraussetzungen (z. B. § 25 (3) Berliner Landeskrankenhausgesetz). Ob und in welchen Fällen solche Erlaubnisse im Einzelfall auch als ausreichend für den hier beschriebenen Anwendungsfall angesehen werden können, wird im Weiteren nicht geprüft und entsprechend auch nicht ausgeschlossen.

3.2.3.2 Ausführliche Darstellung und Begründung zur Rechtsgrundlage

Für personenbezogene Daten legt Art. 6 (1) a DSGVO fest, dass betroffene Personen in die Verarbeitung ihrer Daten für einen oder mehrere bestimmte Zwecke einwilligen können. Der vorliegend beschriebene Anwendungsfall beruht allerdings auf der Annahme, dass zum Zeitpunkt der Einwilligung regelmäßig die späteren Forschungsfragestellungen und damit auch die spezifischen Zwecke noch nicht bekannt sein können. Insofern ist zu fragen, ob sich der Begriff „festgelegte Zwecke“ aus der DSGVO auch so auslegen lässt, dass damit ein Korridor zulässiger Zwecke beschrieben wird. Damit wäre initial zum Zeitpunkt der Einwilligung die Festlegung und Beschreibung eines Korridors erlaubter Zwecke möglich, innerhalb dessen dann zu einem späteren Zeitpunkt die Daten für konkrete und enger formulierte Zwecke verarbeitet werden dürften. Ein deutlicher Hinweis auf diese mögliche Auslegung ist in Erwägungsgrund Nr. 33 DSGVO enthalten, der genau den beschriebenen Umstand, dass gerade in der wissenschaftlichen Forschung oftmals die Zwecke zu Zeitpunkt der Erhebung nicht vollständig angegeben werden können, reflektiert. Insofern soll demnach auch die Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung gelten können, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht.

[4] https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung

Da es vorliegend allerdings um die Verarbeitung von Gesundheitsdaten geht, die zu den besonderen Kategorien personenbezogener Daten zählen, ist zu fragen, ob sich diese auf Erwägungsgrund Nr. 33 DSGVO gestützte Interpretation auch auf die Verarbeitung solcher besonders sensiblen Daten übertragen lässt. Dies wird in der Kommentierung weitgehend befürwortet (z. B. Schiff in [9], Art. 9 Rn. 34; Weichert in [10], Art. 9 Rn. 51a; Kampert in [11], Art. 9 Rn. 13). Auch der ähnliche Wortlaut in den Einwilligungsnormen für allgemein personenbezogene Daten in Art. 6 (1) a „bestimmte Zwecke“ und für besondere Kategorien personenbezogener Daten in Art. 9 (2) a „festgelegte Zwecke“ lässt nicht vermuten, dass der Gesetzgeber hier eine systematische Unterscheidung intendiert hat. In der englischen Fassung ist von „specific purposes“ und „specified purposes“ die Rede, was hinsichtlich eines eindeutigen systematischen Unterschieds auch nicht weiterführt.

Die in der Datenschutzkonferenz zusammengeschlossenen Aufsichtsbehörden in Deutschland haben angesichts der nicht ganz einfachen Auslegbarkeit von Erwägungsgrund Nr. 33 DSGVO hierzu eine Auslegungshilfe formuliert, die sich im engeren Sinne zwar nicht direkt mit der Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ befasst, immerhin aber Rahmenbedingungen definiert, die eingehalten werden sollen, wenn man sich auf diese weitere Auslegung der Zweckfestlegung beruft [12]. Zum einen werden in dieser Auslegungshilfe besondere Kategorien personenbezogener Daten an keiner Stelle ausgeschlossen und zum anderen deutet der darin enthaltene Hinweis auf ein positives Votum eines Ethikgremiums als mögliche Sicherungsmaßnahme zur Vertrauensbildung darauf hin, dass das medizinische Umfeld mit seinen Daten doch mindestens implizit beim Schreiben der Auslegungshilfe mit bedacht wurde.

Vor dem Hintergrund der von der Datenschutzkonferenz festgelegten, notwendigen Rahmenbedingungen für den Einsatz eines Broad Consent ist weiter zu prüfen, ob die MII diese in ausreichender Weise erfüllt. Da diese Prüfung von der Datenschutzkonferenz anhand der Version 1.6d der Einwilligungsdokumente der MII zusammen mit der Version 0.9d der Handreichung selber mit positivem Ergebnis durchgeführt wurde, kann an dieser Stelle auf eine ausführliche Darlegung verzichtet werden.[5]

[5] https://www.datenschutzkonferenz-online.de/media/pm/20200427_Einwilligungsdokumente_der_Medizininformatik-Initiative.pdf

4. Verantwortlichkeiten und Zuständigkeiten

Die Aufgabenverteilung der beteiligten Stellen im Rahmen eines jeweiligen Anwendungsfalls ist in der Nutzungsordnung der MII detailliert beschrieben. Im Folgenden werden die datenschutzrechtliche Verantwortlichkeit und die sich daraus ergebenden Zuständigkeiten für speziell datenschutzrechtlich relevante Aufgabenstellungen beschrieben.

4.1 Machbarkeitsanfragen

Für die Durchführung von Machbarkeitsanfragen, insoweit diese personenbezogene Patientendaten der DIZ-Standorte betreffen und gemäß den Vorgaben der NO durchgeführt werden, ist jeweils der an der Durchführung beteiligte DIZ-Standort und das Forschungsdatenportal der MII gemeinsam nach Art. 26 DSGVO verantwortlich. Dem jeweiligen DIZ-Standort obliegt daher die Prüfung, ob für die Durchführung einer Machbarkeitsanfrage auf den eigenen Daten eine ausreichende Rechtsgrundlage besteht (vergl. Abschnitt 3.2.1). Dem Forschungsdatenportal muss das Vorliegen einer ausreichenden Rechtsgrundlage entsprechend zugesichert werden.

Weiter obliegen dem jeweiligen DIZ-Standort in Bezug auf die Betroffenen, von denen sie Daten im Rahmen von Machbarkeitsanfragen verarbeiten, die folgenden Pflichten:

- Information der Betroffenen nach den Vorgaben von Art. 12–14 DSGVO
- Umsetzung von Betroffenenrechten nach Art. 15–21 DSGVO
- Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO; Meldepflichten nach Art. 33 gelten in gleichem Umfang auch gegenüber dem Forschungsdatenportal

4.2 Verteilte Analysen

Die Identifikation, Auswahl und Zusammenstellung der für einen Nutzungsvertrag bereitzustellenden Patientendaten durch einen Geber sowie die in bestimmten Fällen notwendige Übermittlung personenbezogener Daten an eine übergreifende Treuhandstelle finden in alleiniger Verantwortung des jeweiligen Gebers statt.

Die Verarbeitung der von einem Geber bereitgestellten Daten mit Hilfe der vom Nutzer bereitgestellten Analysemethoden am Standort des jeweiligen Gebers findet in gemeinsamer Verantwortlichkeit vom jeweiligen Geber mit dem Nutzer statt. Dem jeweiligen Geber obliegt daher die Prüfung, ob für die Durchführung der verteilten Analyse auf den eigenen Daten eine ausreichende Rechtsgrundlage besteht (vergl. Abschnitt 3.2.2). Dem Nutzer muss das Vorliegen einer ausreichenden Rechtsgrundlage entsprechend zugesichert werden.

Weiter obliegen dem jeweiligen Geber in Bezug auf die Betroffenen, von denen sie Daten im Rahmen von verteilten Analysen verarbeiten, die folgenden Pflichten:

- Information der Betroffenen nach den Vorgaben von Art. 12–14 DSGVO
- Umsetzung von Betroffenenrechten nach Art. 15–21 DSGVO
- Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO; Meldepflichten nach Art. 33 gelten in gleichem Umfang auch gegenüber dem Forschungsdatenportal

Wird im Rahmen verteilter Analysen eine übergreifende Treuhandstelle eingebunden, so findet die Verarbeitung personenbezogener Daten in der übergreifenden Treuhandstelle in gemeinsamer Verantwortlichkeit aller Geber und der übergreifenden Treuhandstelle und die Übermittlung von Daten

von der übergreifenden Treuhandstelle an die Geber in gemeinsamer Verantwortlichkeit der jeweiligen Geber und der übergreifenden Treuhandstelle statt. Den Gebern obliegt es dann, für die genannten Verarbeitungsschritte zu prüfen, ob eine ausreichende Rechtsgrundlage hierfür besteht und dies der übergreifenden Treuhandstelle zuzusichern.

Dem jeweiligen Geber obliegen in Bezug auf die Betroffenen, von denen sie Daten im Rahmen von verteilten Analysen verarbeiten, weiterhin die folgenden Pflichten

- Information der Betroffenen nach Art. 12–14 DSGVO
- Umsetzung von Betroffenenrechten nach Art. 15–21 DSGVO
- Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO; Meldepflichten nach Art. 33 gelten in gleichem Umfang auch gegenüber dem Forschungsdatenportal

Die übergreifende Treuhandstelle ist verpflichtet, ihr bekannt gewordene und für die Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO relevante Vorfälle unverzüglich den Gebern im notwendigen Umfang zu melden, damit diese ihren Pflichten nach Art. 33 und 34 DSGVO nachkommen können.

4.3 Daten-Herausgaben

Die Identifikation, Auswahl und Zusammenstellung der für einen NV bereitzustellenden Patientendaten sowie die Übermittlung dieser Patientendaten an eine Datenmanagementstelle und an eine übergreifende Treuhandstelle durch die Geber findet in alleiniger Verantwortung der Geber statt.

Die Verarbeitung von Patientendaten in der Datenmanagementstelle, die Übermittlung von Patientendaten von der Datenmanagementstelle an den Nutzer, die Entgegennahme von abgeleiteten Daten vom Nutzer durch die Datenmanagementstelle, die Verarbeitung von abgeleiteten Daten nach Ziff. 1.11 NO in der Datenmanagementstelle sowie die Archivierung der Patientendaten und abgeleiteten Daten in der Datenmanagementstelle nach Ziff. 2.8 (4) NO finden in gemeinsamer Verantwortlichkeit aller Geber und der Datenmanagementstelle statt. Die Übermittlung abgeleiteter Daten von der Datenmanagementstelle an die jeweiligen Geber geschieht in gemeinsamer Verantwortlichkeit der Datenmanagementstelle mit dem jeweiligen Geber. Insoweit müssen die Geber der Datenmanagementstelle zusichern, dass für die genannten Verarbeitungen jeweils ausreichende Rechtsgrundlagen bestehen. Die Zuständigkeiten sind wie folgt geregelt:

- Die Informierung der Betroffenen nach Art. 12–14 DSGVO übernehmen die Geber für die Betroffenen, von denen sie Patientendaten im Rahmen eines NV bereitstellen bzw. als abgeleitete Daten erhalten.
- Die Umsetzung von Betroffenenrechten nach Art. 15–21 übernehmen die Geber für die Betroffenen, von denen sie Patientendaten im Rahmen eines NV bereitstellen bzw. abgeleitete Daten erhalten. Die Datenmanagementstelle ist verpflichtet, auf Anforderung durch den Geber, an der Umsetzung der Betroffenenrechte mitzuwirken.
- Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO übernehmen die Geber für die Betroffenen, von denen sie Patientendaten im Rahmen eines NV bereitstellen bzw. abgeleitete Daten erhalten. Die Datenmanagementstelle ist verpflichtet, ihr bekannt gewordene und hierfür relevante Vorfälle unverzüglich den Gebern im notwendigen Umfang zu melden, damit diese ihren Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO nachkommen können.

- Die Archivierung der Patientendaten nach Ziff. 2.8 (4) NO übernimmt die Datenmanagementstelle. Nach Ablauf der für die Archivierung in einem NV geregelten Frist löscht die Datenmanagementstelle die archivierten Daten und informiert darüber die an dem jeweiligen Nutzer-Projekt beteiligten Geber, das Forschungsdatenportal und eine ggf. eingebundene übergreifende Treuhandstelle.

Wird im Rahmen der Daten-Herausgabe eine übergreifende Treuhandstelle eingebunden, so findet die Verarbeitung personenbezogener Daten in der übergreifenden Treuhandstelle sowie die Übermittlung von Daten von der übergreifenden Treuhandstelle an die Datenmanagementstelle oder an die Geber in gemeinsamer Verantwortlichkeit der Geber, der Datenmanagementstelle und der übergreifenden Treuhandstelle statt. Insoweit müssen die Geber zusichern, dass für die genannten Verarbeitungsschritte jeweils ausreichende Rechtsgrundlagen bestehen.

Dem jeweiligen Geber obliegen in Bezug auf die Betroffenen, von denen sie Daten im Rahmen von verteilten Analysen verarbeiten, weiterhin die folgenden Pflichten

- Die Informierung der Betroffenen nach Art. 12–14 DSGVO
- Die Umsetzung von Betroffenenrechten nach Art. 15–21; die übergreifende Treuhandstelle ist verpflichtet, auf Anforderung durch den Geber, an der Umsetzung der Betroffenenrechte mitzuwirken.
- Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO; die übergreifende Treuhandstelle ist verpflichtet, ihr bekannt gewordene und hierfür relevante Vorfälle unverzüglich den Gebern im notwendigen Umfang zu melden, damit diese ihren Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO nachkommen können.

5. Beschreibung der Daten und Datenkategorien

5.1 Patientendaten

Patientendaten sind zunächst alle Informationen zu einem Patienten, die anlässlich der Untersuchung und Behandlung genutzt werden. Beispiele für Patientendaten sind: Daten aus Arztbriefen, die Krankengeschichte oder Befunde und Daten aus medizinischen Untersuchungen wie Blutdruckmessungen oder Röntgenbildern; ebenso zählen die Ergebnisse von Laboruntersuchungen dazu, einschließlich Untersuchungen der Erbsubstanz (z. B. auf angeborene genetisch bedingte Erkrankungen oder erworbene genetische Veränderungen, unter anderem auch von Tumoren). Damit unterfallen Patientendaten grundsätzlich den besonderen Kategorien personenbezogener Daten nach Art. 9 (1) DSGVO.

Im Rahmen der Medizininformatik-Initiative wurde durch die Arbeitsgruppe Interoperabilität des Nationalen Steuerungsgremiums ein Kerndatensatz definiert. Dieser Kerndatensatz definiert, in welcher Zusammenstellung und Form die Daten für die übergreifenden Anwendungsfälle bereitzustellen sind. Der Kerndatensatz ist in Module unterteilt und besteht aus Basis- und Erweiterungsmodulen. Die Basismodule sind fachlich übergreifend definiert. Die Erweiterungsmodule bilden Daten spezifischer Anwendungs- bzw. Fachgebiete ab und können je nach Forschungsfragestellung in Datenabfragen einbezogen werden. Der Kerndatensatz unterliegt einer kontinuierlichen Weiterentwicklung, die bedarfsgerecht, nachhaltig und international abgestimmt erfolgt.

In seiner jeweils aktuellen Version[6] definiert der Kerndatensatz damit immer auch den aktuellen Umfang der für die hier beschriebenen Anwendungsfälle relevanten Patientendaten. Eine Übersicht gibt Abb. 4.

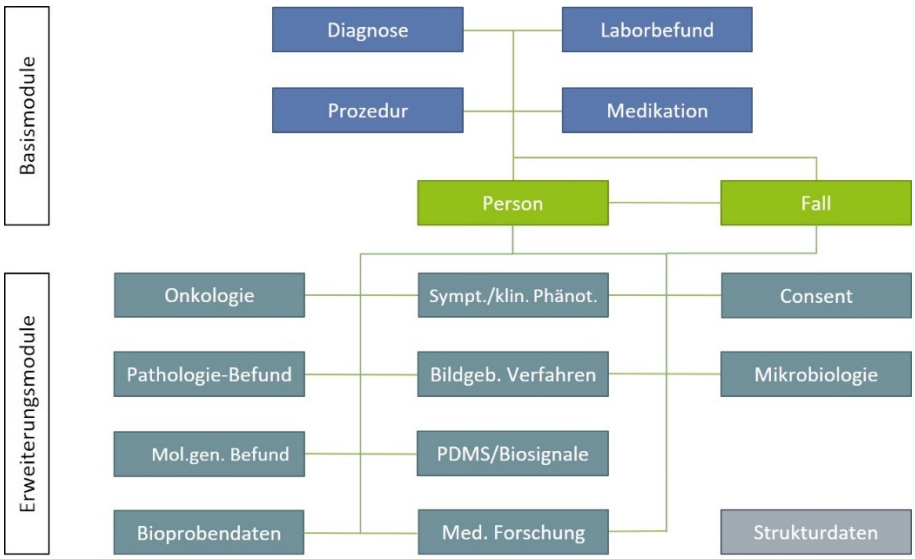

Abb. 4: Der modulare Kerndatensatz der Medizininformatik-Initiative

Die einzelnen Module des Kerndatensatzes werden im Rahmen der MII und abgestimmt mit HL7 als FHIR-Ressourcen profiliert. Zu jedem Modul wird zudem ein Implementation Guide erstellt und abgestimmt. Sofern für einzelne Felder nicht allein durch die Profilierung auf technischer Ebene sichergestellt werden

[6] siehe https://www.medizininformatik-initiative.de/de/der-kerndatensatz-der-medizininformatik-initiative

kann, dass nur bestimmungsgemäße und im jeweiligen Implementation Guide festgelegte Inhalte enthalten sind bzw. kommuniziert werden, geht das vorliegende Datenschutzkonzept davon aus, dass die bestimmungsgemäße Befüllung in der Verantwortlichkeit der DIZ-Standorte erfolgt und vorausgesetzt werden kann.

5.1.1 Medizinische Daten (MDAT)

Medizinische Daten stellen den Teil der Patientendaten dar, die tatsächlich medizinische Sachverhalte beschreiben, bzw. als Gesundheitsdaten anzusehen sind. Dies sind die Daten aller Module des Kerndatensatzes bis auf die Daten der Module Person und Strukturdaten. Aus dem Modul Person werden allerdings das Geburtsdatum auf das Quartal und Jahr vergröbert, das Geschlecht und die Postleitzahl (PLZ) auf die ersten beiden Ziffern vergröbert im Sinne von Klassifikatoren sowohl den IDAT als auch den MDAT zugeordnet.

5.1.2 Identifizierende Daten (IDAT)

Direkt die betroffenen Patienten identifizierende Daten werden in den hier beschriebenen übergreifenden Anwendungsfällen in aller Regel nicht verarbeitet. Sie sind jedoch an den DIZ-Standorten vorhanden und werden dort in aller Regel getrennt von den Patientendaten gespeichert und verarbeitet. In bestimmten Fällen können identifizierende Daten jedoch dafür verwendet werden, mit Hilfe einer übergreifenden Treuhandstelle zu klären, welche Datensätze aus verschiedenen Standorten zu ein und demselben Patienten gehören, wenn dies nicht mit anderen Mitteln eindeutig geklärt werden kann. Der Vollständigkeit halber werden sie daher hier beschrieben.

Die identifizierenden Daten sind in dem Modul „Person“ des Kerndatensatzes[7] definiert und umfassen

- IDs (Versicherten-Nummern, Patienten-ID aus dem Krankenhausinformationssystem),
- Namensangaben (incl. Geburtsname),
- Angaben zum Geschlecht,
- Geburtsdatum,
- Angabe, ob der Patient verstorben ist,
- Adressangaben.

Bei entsprechender Notwendigkeit aufgrund der wissenschaftlichen Fragestellung können in Einzelfällen und auf Antrag auch Angaben zum Geburtsdatum, die genauer sind als die Angabe von Geburtsjahr und Quartal, sowie Angaben zur Postleitzahl oder Gemeindekennziffer der Patientenadresse mit den beantragten MDAT zusammengeführt im Rahmen einer Daten-Nutzung bereitgestellt oder herausgegeben werden. Die Herausgabe oder Bereitstellung dieser Angaben unterliegt dann einer besonderen Prüfung (siehe Kap. 6.2.6.3).

5.2 Pseudonyme

Es ist eine besondere Eigenschaft der Datenschutz-Architektur der Medizininformatik-Initiative, dass dauerhaft verwendete Pseudonyme für die Patientendaten nur in den behandelnden Einrichtungen bzw. DIZ-Standorten erzeugt und verarbeitet werden. Für alle standortübergreifenden Verarbeitungen werden zusätzliche Pseudonyme erzeugt und verwendet, die spezifisch für diese Verarbeitung sind und entsprechend nach Abschluss der Verarbeitung auch wieder gelöscht werden. Insbesondere werden für

[7] siehe https://www.medizininformatik-initiative.de/Kerndatensatz/Modul_Person/Patient.html

Daten-Nutzungen jeweils spezifische Pseudonyme erstellt und im Fall einer Herausgabe der Daten auch mit herausgegeben. Insofern finden Pseudonyme mit den folgenden Eigenschaften Verwendung:

- $\text{Pseudonym}_{\text{DIZ}}$: im DIZ dauerhaft verwendetes Pseudonym zu den MDAT eines Patienten
- $\text{Pseudonym}_{\text{DIZ-Projekt}}$: für die MDAT eines Patienten in einem bestimmten Nutzer-Projekt vom DIZ temporär erzeugtes Pseudonym, welches nach Ablauf des Projekts (eine Archivierungsfrist nach Guter Wissenschaftlicher Praxis eingeschlossen) gelöscht wird
- $\text{IDAT}_{\text{Kodiert}}$: eine jeweils eindeutige Kodierung relevanter IDAT, um für Patienten eine eindeutige Kennung zu erhalten, aus der jedoch nicht auf die Identität des Patienten geschlossen werden kann (im Regelfall werden hierfür Bloom-Filter verwendet)
- $\text{Pseudonym}_{\text{Nutzer-Projekt}}$: für die MDAT eines Patienten in einem bestimmten Nutzer-Projekt von einer übergreifenden Treuhandstelle oder (bei Verfahren ohne vorgeschaltetes Record Linkage) der Datenmanagementstelle erzeugtes, standortübergreifend eindeutiges Pseudonym für die Übermittlung von Daten an einen Nutzer

Im Einzelfall können ergänzend noch Verschlüsselungsparameter oder temporäre Token für die Zuordnung von Datensätzen im Rahmen der Anwendungsfälle entstehen und genutzt werden, die hier aufgrund ihrer geringen Zuordenbarkeit zu den Patientendaten nicht mit aufgeführt werden. Eine ausführliche Darstellung der Generierung und Verwendung der einzelnen Pseudonyme ist in Kap. 6.2.6.2 zu finden.

An den DIZ-Standorten oder anderen beteiligten Stellen (übergreifende Treuhandstelle, Datenmanagementstelle) bzw. in den an der MII beteiligten Konsortien können diese Pseudonyme jeweils anders und jeweils unterschiedlich benannt sein. Insofern wird in diesem Konzept ein möglichst generisches und einfach verständliches Benennungsschema verwendet. Im Regelfall sollte ein Mapping der hier verwendeten Begriffe auf die jeweiligen Bezeichner einzelner beteiligter Stellen einfach möglich sein.

5.3 Übersichtsmatrix und Schutzstufen

Eine Übersicht der verschiedenen Datenkategorien mit den jeweiligen Zugriffsmöglichkeiten unterschiedlicher Stellen in der MII findet sich in Tabelle 1. Zu jeder Datenkategorie ist zudem die Schutzstufe nach dem Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen [13] vermerkt.

Tab. 1 Übersicht der Stellen und ihrer Zugriffsmöglichkeiten auf Datenkategorien mit den jeweiligen Schutzstufen

Datenkategorie (Schutzstufe[1])	DIZ-Standort	übergreifende Treuhandstelle	Datenmanagement-stelle	Nutzer	Forschungs-datenportal
IDAT (C[2])	X	(X)[3]	(X)[4]	(X)[4]	
MDAT (D-E[5])	X		X[6]	X[6]	
$Pseudonym_{DIZ}$ (B)	X				
$IDAT_{Kodiert}$ (B)	X	X			
$Pseudonym_{DIZ\text{-}Projekt}$ (B)	X	X	(X)[6]		
$Pseudonym_{Nutzer\text{-}Projekt}$ (B)	(X)[8]	X	X	X	(X)[9]

[1] nach dem Schutzstufenkonzept der LfD Niedersachsen [13]
[2] je nach Zuordnungsmöglichkeit zu den Patientendaten ggf. auch höher
[3] nur in Einzelfällen, in denen eine Zuordnung der Datensätze anhand $IDAT_{Kodiert}$ nicht ausreichend sicher möglich ist
[4] nur Alters- und Adressangaben (nur PLZ oder Gemeindekennziffer) im jeweils nach wissenschaftlicher Notwendigkeit zu begründenden und zu prüfenden Detailgrad
[5] je nach Umfang und Sensibilität der Daten, psychiatrische Diagnosen mit Diskriminierungspotential sind ggf. anders einzuordnen als ein grippaler Infekt
[6] je Projekt werden nur die für eine wiss. Fragestellung notwendigen Teile der MDAT und ggf. auch nur in der notwendigen Detailliertheit (z. B. beim Geburtsdatum oder der PLZ) herausgegeben
[7] nur bei Daten-Herausgabe ohne eingebundene Treuhandstelle und ohne Record Linkage
[8] je nach Architekturmodell
[9] nur bei der Koordinierung von Widerrufen durch das Forschungsdatenportal

6. Datenschutz-Folgenabschätzung

Dieses Kapitel dokumentiert integriert in ein umfassenderes Datenschutzkonzept eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. Insofern sind im Folgenden die notwendigen Inhalte einer Datenschutz-Folgenabschätzung nach Art. 35 (7) a-d DSGVO beschrieben.

6.1 Bewertung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung

Die Notwendigkeit der Verarbeitungsprozesse ergibt sich zunächst aus den sowohl gesetzlich privilegierten als auch im öffentlichen Interesse verankerten wissenschaftlichen Forschungszwecken, die im Rahmen der hier behandelten Anwendungsszenarien verfolgt werden (vergl. Kap. 2). In Bezug auf die Notwendigkeit ist zudem auf die detaillierte Beschreibung der Maßnahmen zur Beschränkung auf notwendige Verarbeitungen in Kap. 6.2.2 zu verweisen. Die Verhältnismäßigkeit der hier beschriebenen Datenverarbeitungen ergibt sich demgegenüber aus der Vielzahl an Maßnahmen zur effektiven Reduktion der Risiken für die von der Verarbeitung betroffenen Patienten. Insbesondere ist hier auf die in Kap. 6.2.6 beschriebenen Maßnahmen zur Datenminimierung zu verweisen. Vor diesem Hintergrund und unter Berücksichtigung des in Kap. 6.4 beschriebenen Ergebnisses der Datenschutz-Folgenabschätzung wird von einer Sicherstellung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung ausgegangen.

6.2 Technische und Organisatorische Maßnahmen

6.2.1 Vertragliche Regelung aller Verarbeitungen

Jegliche Verarbeitung sensibler Patientendaten unterliegt immer einer entsprechenden vertraglichen Regelung, einschließlich der relevanten datenschutzrechtlichen Zuständigkeiten der einzelnen Verantwortlichen (siehe Kap. 4). Für die Machbarkeitsanfragen ist dies ein Teilnahmevertrag,[8] der gemeinsam von allen DIZ-Standorten und dem Forschungsdatenportal geschlossen wird. Dieser Teilnahmevertrag regelt auch die Zuständigkeiten bei mehreren verantwortlichen Stellen für einzelne Datenverarbeitungen innerhalb der MII im Rahmen von Daten-Nutzungen wie verteilten Analysen oder auch Daten-Herausgaben. Zudem wird mit diesem Teilnahmevertrag die Nutzungsordnung der MII (NO)[9] als verbindliche Rahmenregelung von allen beteiligten Stellen anerkannt. Daten-Nutzungen werden im Außenverhältnis mit einem Nutzer durch den Nutzungsvertrag der MII (NV) geregelt.[10]

6.2.2 Beschränkung auf notwendige Verarbeitungen

6.2.2.1 Vorgeschaltete Machbarkeitsanfragen

Zunächst schafft die MII mit dem Angebot von Machbarkeitsanfragen (s. Kap. 2.1) die Voraussetzung dafür, dass vor jeder Daten-Nutzung, die mit weitergehenden Risiken für die informationelle Selbstbestimmung der betroffenen Patienten einhergeht, sichergestellt werden kann, dass grundsätzlich auch eine ausreichende Datenbasis zur Verfügung steht. Insofern können mit dem Instrument der Machbarkeitsanfragen Daten-Nutzungen verhindert werden, die mit bestimmten Risiken für die von der

[8] derzeit noch in Abstimmung
[9] https://www.medizininformatik-initiative.de/de/nutzungsordnung
[10] https://www.medizininformatik-initiative.de/de/nutzungsvertrag

Datenverarbeitung betroffenen Patienten verbunden sind, aber mangels ausreichender Datenbasis nicht zu hilfreichen wissenschaftlichen Ergebnissen führen.

6.2.2.2 Beratung und positive Bewertung durch eine unabhängige Ethikkommission

Einem Nutzungsantrag ist gemäß Ziffer 1.4 der NO immer ein zustimmendes Votum bzw. eine Kurzbescheinigung der Nicht-Zuständigkeit (Waiver) von einer den Antragsteller beratenden und nach Landesrecht gebildeten Ethikkommission als Anlage anzufügen. Damit sind die Vorgaben der MII für nicht-interventionelle und ohne zusätzliche Datenerhebungen auskommende Studien strenger als die rein berufsrechtlichen Vorgaben, die bei Nutzung personenbeziehbarer Daten im Regelfall lediglich fordern, dass eine Beratung durch eine Ethikkommission stattgefunden hat und dies unabhängig vom Ergebnis der Beratung dokumentiert wurde. Insofern ist sichergestellt, dass jedes Forschungsprojekt, welches eine Daten-Nutzung mit personenbeziehbaren Daten in der MII einschließt, zuvor durch eine unabhängige Ethikkommission geprüft und positiv bewertet wird.

6.2.2.3 Prüfung und Genehmigung durch Use & Access Committees an allen DIZ-Standorten

Jeder Nutzungsantrag in der MII wird durch Use & Access Committees (UAC) an allen DIZ-Standorten geprüft. Nur bei einem positiven Votum eines UAC, kann ein DIZ-Standort durch Teilnahme an einem Nutzungsvertrag auch Geber im Sinne des Nutzungsvertrags werden. Die Zusammensetzung eines UAC sowie die Verfahrensweisen und Prüfungskriterien werden in lokalen Geschäfts- oder Nutzungsordnungen der DIZ-Standorte geregelt. Mindestvorgaben bzw. Empfehlungen, insbesondere mit Blick auf die Zusammensetzung, sind in der NO in Ziff. 1.13 festgehalten.

6.2.2.4 Priorisierung von verteilten Analysen

Durch die Schaffung einer Infrastruktur für verteilte Analysen kann die MII perspektivisch Datenverarbeitungen verhindern, die mit einer Offenlegung umfangreicher pseudonymer Datensätze an Forscher einhergehen, wenn diese Offenlegung für die wissenschaftlichen Zwecke der Daten-Nutzung nicht notwendig ist. Dadurch, dass im Falle verteilter Analysen die sensiblen Patientendaten in der Hoheit der Geber verbleiben, wird eine unnötige und mit bestimmten Risiken für die Rechte und Freiheiten der betroffenen Patienten einhergehende Verarbeitung direkt beim Forscher vermieden. Kriterien für die Beurteilung, ob eine bestimmte Daten-Nutzung auch als verteilte Analyse organisiert werden kann, werden derzeit von der Taskforce für verteilte Analysen in der MII entwickelt. Diese Kriterien sind allerdings stark davon abhängig, welche Auswertungsmöglichkeiten eine Infrastruktur für verteilte Analysen bietet. Insofern sind diese Kriterien parallel zum Ausbau einer Infrastruktur für verteilte Analysen in der MII weiterzuentwickeln.

6.2.2.5 Verhinderung der langfristigen Archivierung von Patientendaten bei Forschern

Nach den Leitlinien der Deutschen Forschungsgemeinschaft (DFG) zur Sicherung guter wissenschaftlicher Praxis[11] müssen die Daten, auf denen ein publiziertes Auswertungsergebnis beruht, für 10 Jahre aufbewahrt werden, um die Nachvollziehbarkeit der Forschungsergebnisse abzusichern. Häufig führt diese Anforderung dazu, dass sensible Rohdaten unter wenig regulierten Bedingungen von Forschern

11 https://www.dfg.de/download/pdf/foerderung/rechtliche_rahmenbedingungen/gute_wissenschaftliche_praxis/kodex_gwp.pdf

aufbewahrt werden. Dadurch, dass seitens der MII im NV geregelt wird, dass diese Archivierung der Patientendaten von der Infrastruktur der MII übernommen wird, wird eine schwer zu regulierende Speicherung der Daten für einen vergleichsweise langen Zeitraum bei den Forschern verhindert. Den Forschern wird im Gegenzug vertraglich garantiert, dass die Daten zu Zwecken der Nachvollziehbarkeit innerhalb der Frist von 10 Jahren in unveränderter Form zur Verfügung gestellt werden können.

6.2.3 Schaffung geeigneter Rahmenbedingungen für die informierte Einwilligung

Viele Datenverarbeitungen in der MII werden voraussichtlich auf der Rechtsgrundlage einer informierten Einwilligung aufbauen. Dies gilt insbesondere für Daten-Nutzungen im Sinne von Daten-Herausgaben (vergl. Kap. 3.2.3), die immer mit etwas höheren Risiken für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Patienten einhergehen. Insofern ist es von besonderer Bedeutung, wie die Rahmenbedingungen der Einholung einer informierten Einwilligung in der MII gestaltet sind.

Diese Rahmenbedingungen sind für die Nutzung der Einwilligungsdokumente der MII in der ergänzenden Handreichung dargestellt und geregelt.[12] Demnach müssen gesondert geschulte Mitarbeiter die Aufklärung der Patienten im Rahmen eines Einwilligungsprozesses übernehmen. Eine Aufklärung durch ärztliches Personal ist hingegen nicht notwendig, da mit der Einwilligung in die Datennutzung keine medizinischen Risiken verbunden sind. Zudem müssen an jedem DIZ-Standort, der die Einwilligungsdokumente einsetzt, klar definierte, ethisch und klinisch angemessene Prozesse zum Umgang mit Zusatzbefunden etabliert werden. Dadurch sollen Risiken für die betroffenen Patienten vermindert werden, die mit der unkontrollierten Rückmeldung von möglicherweise sehr belastenden Zusatzbefunden einhergehen können. Weitere in der Handreichung beschriebene und festgelegte Rahmenbedingungen beziehen sich auf die notwendige Umsetzung von Betroffenenrechten (vergl. Kap. 7), die Schaffung notwendiger Transparenz gegenüber den Betroffenen (vergl. Kap. 6.2.5) sowie die notwendige Sicherheit der Verarbeitung (vergl. Kap. 6.2.7).

Da die oft längeren Texte in Patienteninformationen und Einwilligungserklärungen von vielen Patienten nicht vollständig gelesen bzw. verstanden werden (z. B. [14]), ist es der MII ein großes Anliegen, die Aushändigung der Dokumente mit niedrigschwelligen Informationsangeboten zu ergänzen. Hierzu wurden animierte Videos erstellt und breit abgestimmt, die mit oder ohne Ton (und Untertiteln) z. B. in Aufnahmesettings in den beteiligten Krankenhäusern abgespielt werden können.[13] Diese erklären den Umfang einer Einwilligung, die Konsequenzen, den Nutzen und auch die Risiken in einfacher und mit passenden Bildern untersetzter Sprache. Ergänzend werden Flyer und Poster für die DIZ-Standorte angeboten, die ggf. ergänzend für die Aufklärung der Patienten genutzt werden können. So können z. B. ambulant behandelte Patienten einen Flyer mit nach Hause nehmen und sich so über die Einwilligungsmöglichkeiten in der MII schon vor einem stationären Aufenthalt informieren. Für Patienten mit eingeschränkten Fähigkeiten, längere und komplexe Texte zu verstehen, entwickelt die MII derzeit zudem eine Fassung der Einwilligungsdokumente in einfacher Sprache.

[12] https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Handreichung_v0.9d.pdf
[13] einsehbar unter https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung

Mit all diesen Hilfsmitteln kann einerseits das Verständnis der Patienten gefördert und andererseits das aufklärende Personal, welches ansonsten alle notwendigen Informationen im Aufklärungsgespräch vermitteln muss, entlastet werden.

Auch wenn längere Texte erfahrungsgemäß von vielen Patienten – zumal in einem klinischen Setting – nicht ausführlich und konzentriert gelesen werden, muss doch eine Möglichkeit für interessierte Patienten geschaffen werden, sich umfangreich über alle Rahmenbedingungen und Konsequenzen einer Einwilligung zu informieren. Entsprechend enthält die Patienteninformation der MII umfangreiche und ausführlich mit den Datenschutzbehörden abgestimmte Risikohinweise in Bezug auf die Verarbeitung personenbezogener Gesundheitsdaten. Besonders umfangreiche Informationen bietet die MII ergänzend zu dem komplexen Thema der Forschung mit genetischen Daten an. Um den Text der Patienteninformation diesbezüglich jedoch nicht noch weiter zu verlängern, enthält diese hierzu nur die wichtigsten Hinweise. Ergänzend wird eine Website mit ausführlicheren Informationen in der Patienteninformation verlinkt.[14]

6.2.4 Umsetzung von Betroffenenrechten

Die Umsetzung von Betroffenenrechten erfordert technische und organisatorische Maßnahmen, um die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen zu garantieren. Insofern ist dieses Thema auch in diesem Abschnitt zu den allgemeinen technischen und organisatorischen Maßnahmen referenziert. Auf Grund der umfangreichen gesetzlichen Regelung und nötiger eigenständiger Maßnahmen, wird die Umsetzung der Betroffenenrechte jedoch im separaten Kapitel 7 beschrieben.

6.2.5 Transparenz der Verarbeitungen

Auch wenn die basalen Informationspflichten nach Art. 12–14 DSGVO die DIZ-Standorte als die behandelnden Einrichtungen der betroffenen Patienten treffen und insofern von diesen umgesetzt werden müssen (vergl. Kap. 4), gibt es in der MII doch eine Reihe ergänzender und übergreifender Maßnahmen zur Sicherstellung einer umfangreichen Transparenz der Datenverarbeitung für die Betroffenen, die in diesem Abschnitt dargestellt werden.

Alle vertraglich abgesicherten Daten-Nutzungen in der MII, die als Rechtsgrundlage auf der informierten Einwilligung unter Verwendung der Einwilligungsdokumente der MII beruhen, werden in einem zentralen und öffentlich zugänglichen Studienregister transparent gemacht.[15] Im Rahmen der Abstimmung der Einwilligungsdokumente der MII hatten einige Datenschutzbehörden zunächst gefordert, dass in diesem Register jeder Patient einsehen können sollte, in welchen Studien genau seine Daten verwendet wurden. Aus guten und letztlich auch die Datenschutzbehörden überzeugenden Gründen wird in der MII jedoch auf eine solche patientenindividuelle Nutzungstransparenz verzichtet.[16] Insofern können interessierte Patienten nur verfolgen, welche Studien überhaupt durchgeführt werden, nicht aber, in welchen Studien ihre eigenen Daten tatsächlich Verwendung finden.

Das Studienregister verfügt ergänzend über eine Registrierungsfunktion für einen E-Mail-Verteiler, mit dessen Hilfe kurzfristig über alle neu registrierten Studien informiert wird. Eine Daten-Überlassung oder

[14] siehe www.vernetzen-forschen-heilen.de/genetische-daten
[15] www.medizininformatik-initiative.de/datennutzung
[16] Begründung in einem Positionspapier der AG Consent unter https://www.medizininformatik-initiative.de/sites/default/files/2019-09/MII_AG-Consent_Stellungnahme-Consent-Modelle_v05.pdf

eine Daten-Bereitstellung im Sinne verteilter Analysen darf gemäß den Rahmenbedingungen der Einwilligungsdokumente der MII immer erst eine Woche nach der öffentlich einsehbaren Registrierung des Projekts samt Informierung über den E-Mail-Verteiler erfolgen. Zu den öffentlich verfügbar zu machenden Angaben im Register gehören insbesondere die folgenden Angaben in allgemeinverständlicher Sprache:

- zu den verantwortlichen Forschern bzw. Stellen,
- zum Zweck des Forschungsprojekts,
- zu den Ergebnissen des Forschungsprojekts (nach dessen Durchführung) sowie
- zur Finanzierung des Forschungsprojekts.

In den Einwilligungsdokumenten, der zugehörigen Handreichung und der NO (Ziff. 2.10 Abs. 3 u. 4) der MII ist zudem geregelt, dass in begründeten Einzelfällen das Recht auf Löschung der Daten bei einem Widerruf der Patienten nach Art. 17 (3) d DSGVO eingeschränkt sein kann. Hierzu müssen Nutzer einen begründeten Antrag auf Ausnahme von der Pflicht zur Datenlöschung stellen, der zusammen mit der Entscheidung des für die betroffene Person zuständigen UAC ebenfalls im zentralen Register in anonymer Form öffentlich einsehbar zu dokumentieren ist.

Im Sinne der Transparenz für die Betroffenen ist es zudem von zentraler Bedeutung, dass die Verfahren zur Nutzung der Daten möglichst transparent gemacht werden. So fordern auch die deutschen Datenschutzbehörden, dass bei Verwendung einer Einwilligung in breite Forschungszwecke unter Berufung auf Erwägungsgrund Nr. 33 DSGVO eine Nutzungsordnung für die Betroffenen transparent gemacht wird [12]. Dementsprechend sind sowohl die übergreifende Nutzungsordnung als auch der Nutzungsvertrag samt den ergänzenden Allgemeinen Nutzungs- und Vertragsbedingungen der MII öffentlich einsehbar auf der Website der MII hinterlegt.[17]

6.2.6 Datenminimierung

6.2.6.1 Anonymisierung

Eine Anonymisierung von Daten findet zum einen bei der Durchführung von Machbarkeitsanfragen statt, bevor die dann anonymisierten Fallzahlen einzelner Standorte an das zentrale Forschungsdatenportal geschickt werden. Zum anderen gilt die Anforderung der Anonymität für die Analyse-Ergebnisse einzelner Standorte im Rahmen verteilter Analysen. Und abschließend kann eine Anonymisierung von Daten eine Löschung der Daten ersetzen, wenn die Rechtsgrundlage für die weitere Aufbewahrung der Daten entfallen ist [6]. In letzterem Fall gelten besondere Anforderungen an die Anonymisierung der Daten, die in den jeweiligen lokalen Datenschutzkonzepten beschrieben sind.

Für die Durchführung von Machbarkeitsanfragen ist festgelegt, dass von den einzelnen DIZ-Standorten alle Fallzahlen vor der Rückmeldung an das Forschungsdatenportal zu verrauschen sind, in dem zu einer Fallzahl vor der Übermittlung ein jeweils neu ermittelter Zufallswert aus dem Wertebereich von -5 bis +5 addiert wird. Dadurch, dass alle Fallzahlen verrauscht werden, kann die Ermittlung kleiner und ggf. einzelne Fälle identifizierender Fallzahlen durch Differenzbildung verhindert werden. Verrauschte Fallzahlen kleiner 5 werden zudem nicht übermittelt, um so für jeden zurückübermittelten Wert den vollständigen Unsicherheitsbereich von -5 bis +5 gewährleisten zu können.

[17] https://www.medizininformatik-initiative.de/de/ueber-die-initiative/ergebnisse

Bei dieser Art der Verrauschung kann durch eine große Zahl identischer oder sehr ähnlicher Anfragen in kurzer Zeit und mit Hilfe statistischer Mittelung doch der exakte mittlere Wert einer Fallzahl ermittelt werden. Um dies zu verhindern, stellt das Forschungsdatenportal durch technische und ggf. organisatorische Maßnahmen sicher, dass identische oder ähnliche Machbarkeitsanfragen nicht in kurzer Zeit (< 1 Minute) zu häufig (> 3) hintereinander ausgeführt werden können.

Die Art der Anonymisierung von Ergebnissen verteilter Analysen an den einzelnen DIZ-Standorten hängt stark von der Verwendung der jeweiligen Plattform oder Infrastruktur für die verteilten Analysen ab. Da hierfür bislang noch keine einheitliche Plattform oder Infrastruktur etabliert wurde, können in dieser Version des Datenschutzkonzepts dazu auch noch keine Feststellungen getroffen werden. Insofern müssen die diesbezüglichen Maßnahmen in ggf. bereits durchzuführenden verteilten Analysen im Einzelfall beschrieben und geprüft werden.

6.2.6.2 Pseudonymisierung

Lokale Pseudonymisierung an den DIZ-Standorten

In der NO der MII (Ziff. 1.14) ist der Einsatz von Treuhandstellen an den DIZ-Standorten in rudimentärer Form beschrieben. Die genaue technische und organisatorische Umsetzung einer Treuhandstelle an einem DIZ-Standort ist im jeweiligen lokalen Datenschutzkonzept beschrieben und wird hier dementsprechend nicht in gleicher Ausführlichkeit behandelt.

Festzuhalten ist an dieser Stelle lediglich, dass zumindest eine personelle, technische und häufig auch organisatorische – in bestimmten Fällen sogar auch rechtliche – Unabhängigkeit der Treuhandstelle von dem Teil eines DIZ (wenn nicht vom gesamten DIZ) gewährleistet wird, der sich mit der Verwaltung der medizinischen Daten (MDAT, vergl. Kap. 5.1.1) im DIZ befasst. Dem Prinzip der informationellen Gewaltenteilung folgend, ist die Treuhandstelle entsprechend mit der Verwaltung der einen Patienten identifizierenden Daten (IDAT, vergl. Kap. 5.1.2) befasst und generiert und verwaltet zu diesen lokal gültige Pseudonyme ($Pseudonym_{DIZ}$, vergl. Kap. 5.2). Die Generierung und Verwaltung eindeutiger Patientenidentitäten und deren korrekte Zuordnung zu den Datensätzen eines Patienten über verschiedene Behandlungsfälle und Dokumentationssysteme hinweg liegt in der Verantwortung der lokalen Treuhandstellen. Fehler an dieser Stelle können in aller Regel bei standortübergreifenden Verfahren des Record Linkage nicht mehr kompensiert werden.

DIZ-Architekturen können sich zwischen den Standorten durchaus deutlich unterscheiden. So ist für die Unterstützung von Anwendungsfällen der Versorgung auch eine gemeinsame Speicherung und Verwaltung von IDAT und MDAT im DIZ in bestimmten Fällen denkbar und an einigen Standorten auch umgesetzt. Die langfristige, einzelne Krankenhausaufenthalte von Patienten überspannende und forschungsorientierte Aufbewahrung wird jedoch an allen Standorten pseudonym umgesetzt. Die genauen Sicherheitsmaßnahmen einer lokalen Treuhandstelle sind dem jeweiligen lokalen Datenschutzkonzept zu entnehmen.

Standortübergreifende Pseudonymisierung ohne Record Linkage

Bei Daten-Herausgaben muss immer rückverfolgbar sein, welcher Datensatz bei einem Nutzer einem bestimmten Datensatz bei einem der Geber entspricht. Wenn Daten-Herausgaben als datenschutzrechtliche Grundlage auf einer informierten Einwilligung beruhen, muss diese Einwilligung auch widerrufbar sein, was regelmäßig mit der Anforderung einhergeht, dass auch Nutzer über den

Widerruf informiert werden und gemäß NV der MII verpflichtet sind, die betreffenden Daten dann auch zu löschen. Dieses Beispiel macht klar, warum ein eindeutiges Mapping zwischen den Datensätzen beim Geber, bei der Datenmanagementstelle und beim Nutzer existieren muss.

Die einzelnen Geber können jedoch ohne weitere Hilfsmittel, wie etwa eine übergreifende Treuhandstelle, keine standortübergreifend eineindeutigen Pseudonyme erzeugen, es sei denn, man würde in dem Pseudonym auch eine ID für den Geber mit kodieren, was aus Datensparsamkeitsgründen jedoch nicht empfehlenswert erscheint. Insofern erstellen die Geber in solchen Fällen von Daten-Herausgaben ohne Record Linkage und damit ohne Einbindung einer übergreifenden Treuhandstelle zunächst projektspezifische Pseudonyme ($Pseudonym_{DIZ\text{-}Projekt}$) für die herauszugebenden Datensätze, die dann an die Datenmanagementstelle übermittelt werden. Diese erstellt dann für alle Datensätze aller Geber eine eineindeutige und wiederum projektspezifische Liste von Pseudonymen, die an den Nutzer mit den MDAT herausgegeben werden ($Pseudonym_{Nutzer\text{-}Projekt}$). Das Mapping zwischen den geberspezifischen Pseudonymen ($Pseudonym_{DIZ\text{-}Projekt}$) und den an den Nutzer herausgegebenen Pseudonymen ($Pseudonym_{Nutzer\text{-}Projekt}$) wird in der Datenmanagementstelle zusammen mit den MDAT für den Nutzungszeitraum und den sich anschließenden Archivierungszeitraum sicher aufbewahrt (siehe Abb. 5).

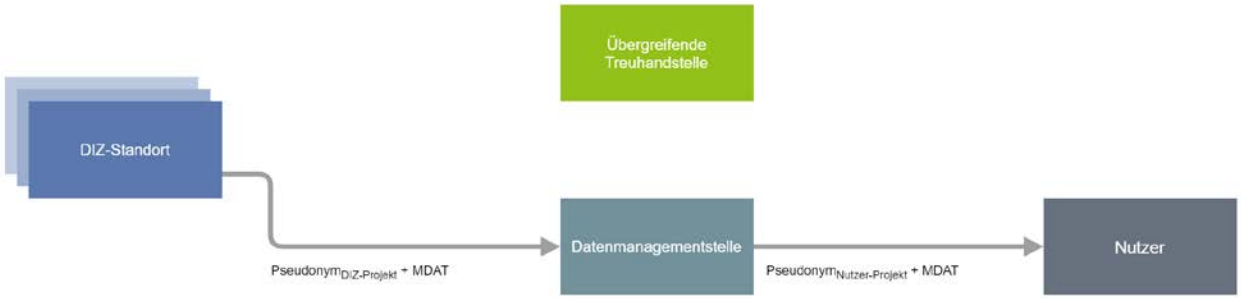

Abb. 5 Erstellung standortübergreifender Pseudonyme durch die Datenmanagementstelle bei Daten-Herausgaben ohne Record Linkage

Alternativ kann auch bei einer standortübergreifenden Pseudonymisierung ohne vorgeschaltetes Record Linkage eine übergreifende Treuhandstelle eingebunden werden, die zentral und projektspezifisch standortübergreifend eindeutige Pseudonyme generiert und zur Verfügung stellt. Zudem kann das Mapping zwischen den an den Nutzer herausgegebenen Pseudonymen und den Pseudonymen an den DIZ-Standorten kryptografisch gespeichert werden, so dass die Information des datenliefernden Standorts und eines standortspezifischen Pseudonyms ($Pseudonym_{DIZ\text{-}Projekt}$) in einem standortübergreifend eindeutigen Pseudonym ($Pseudonym_{Nutzer\text{-}Projekt}$) in verschlüsselter Form enthalten sind. Die Zuordnung der Pseudonyme ($Pseudonym_{DIZ\text{-}Projekt}$ und $Pseudonym_{Nutzer\text{-}Projekt}$) wird von der übergreifenden Treuhandstelle für den Nutzungszeitraum und den sich anschließenden Archivierungszeitraum sicher aufbewahrt.

Die verschiedenen Varianten der Einbindung einer übergreifenden Treuhandstelle sind am Ende des folgenden Abschnitts zur Pseudonymisierung mit Record Linkage aufgeführt und gelten ebenso für die Pseudonymisierung ohne Record Linkage, wenn eine übergreifende Treuhandstelle hierfür eingebunden wird (siehe auch Abb. 6-8).

Standortübergreifende Pseudonymisierung mit Record Linkage

Es existieren Fragestellungen bzw. Anwendungsfälle, in denen es wesentlich ist zu wissen, ob, wie viele oder welche Personen eines Teildatensatzes A in einem Teildatensatz B ebenfalls und ggf. mit leicht abweichenden Schreibweisen oder anderen Details der IDAT vorhanden sind. Die Erzeugung fragestellungs- oder aufgabenbezogener Verbunddatensätze aus Teildatensätzen mehrerer DIZ erfordert das Record Linkage über die Teildatenbestände der Standorte hinweg mit dem Ziel, alle MDAT im Verbunddatensatz so zusammenzuführen, dass Teildatensätze jeder Personenidentität unter einem einzigen, jedoch projektspezifischen Identifikator ($Pseudonym_{Nutzer\text{-}Projekt}$) im Verbunddatensatz vorliegen. Insofern gehören Record Linkage und Pseudonymisierung zusammen, das Record Linkage ist der Pseudonymgenerierung und -zuordnung vorgeschaltet.

Allerdings wird eine solche standortübergreifende Pseudonymisierung nur durchgeführt, wenn diese für die einer Daten-Nutzung zugrundeliegende wissenschaftliche Fragestellung und angesichts der Datenlage auch wirklich notwendig ist. Diese Prüfung ist auch Teil des grundsätzlich zweistufigen Prüfungsverfahrens für Daten-Nutzungen in der MII. So ist zum einen schon eine positive Bewertung einer unabhängigen Ethikkommission mit einem Nutzungsantrag in der MII einzureichen und zum anderen wird die Notwendigkeit auch Teil der Prüfung durch die UACs an den DIZ-Standorten sein.

Record Linkage bezeichnet eine Gruppe von Verfahren, die (Teil-) Datensätze anhand ihrer Zugehörigkeit zu Personen zusammenfassen können. Aufgrund von Tippfehlern, verschiedenen Schreibweisen bei Umlauten, Doppelnamen, Namensänderungen durch Heirat usw. ist es als Normalfall in zeitlich kumulierten und über verschiedene Teildatensätze verteilten Datensammlungen hinzunehmen, dass einer tatsächlichen Person verschiedene technische Personenidentitäten zugehörig sind. Die möglichst korrekte und vollständige Determinierung der zuzuordnenden Person auf Basis der verschiedenen technischen Personenidentitäten ist somit ursächlich für die Güte des (föderierten) Record Linkage. Direkte Matching-Algorithmen („exakter String-Vergleich“) sind in klinischen Systemen oftmals die Realität. Wahrscheinlichkeitsbasierte Ansätze können hier mehr leisten, bergen aber genauso das Risiko sowohl von falsch positiven wie auch falsch negativen Zuordnungen. Im Ergebnis kann daher, abhängig von den Anforderungen an Genauigkeit und statistische Signifikanz bezogen auf eine konkrete Fragestellung, eine manuelle Nacharbeit erforderlich sein.

Grundsätzlich erfolgt das standortübergreifende Record Linkage nur auf der Basis kodierter Identitätsdaten ($IDAT_{Kodiert}$, vergl. Kap. 5.2). Diese werden an den DIZ-Standorten und hier von den lokalen Treuhandstellen anhand projektspezifischer Parameter und Vorgaben erzeugt und zusammen mit projektspezifisch erzeugten, eindeutigen IDs ($Pseudonym_{DIZ\text{-}Projekt}$) an die übergreifende Treuhandstelle übermittelt. Damit verlassen keine IDAT im Klartext die behandelnden Einrichtungen, das Verfahren entspricht insofern den Vorgaben des Privacy Preserving Record Linkage (PPRL). Die $IDAT_{Kodiert}$ sind so beschaffen, dass Ähnlichkeiten bzw. Distanzen zwischen verschiedenen Ausgangsdatensätzen (IDAT) auf ihnen bestimmt werden können. Die übergreifende Treuhandstelle kann anhand von $IDAT_{Kodiert}$ immer nur Personen-Kandidaten für potenzielle Duplikate finden und diese anhand von hinreichenden Übereinstimmungen in Form von unterschiedlichen Schreibweisen (z. B. durch Tippfehler) als Personenidentitäten einer Person zuordnen. Definierte Schwellenwerte legen hierbei fest, ab welcher Übereinstimmung zwei Personen-Kandidaten einer Person zugeordnet oder als getrennte Personen definiert werden sollen. Entsprechend wird ein einziges Pseudonym ($Pseudonym_{Nutzer\text{-}Projekt}$) generiert und den beiden Personen-Kandidaten zugeordnet oder es werden zwei Pseudonyme ($Pseudonym_{Nutzer\text{-}Projekt}$) generiert und zugeordnet.

Wenn bei dem beschriebenen Verfahren auf Basis des Abgleichs von $IDAT_{Kodiert}$ der Schwellenwert für die Identität von zwei Datensätzen nicht erreicht wird, andererseits aber auch nicht mit hinreichender Sicherheit die Identität ausgeschlossen werden kann und zudem für die wissenschaftliche Fragestellung eine möglichst genaue Zuordnung von Datensätzen über Standorte hinweg notwendig ist, kann für diese Datensätze ergänzend auch ein Abgleich auf IDAT erfolgen, die die Treuhandstelle dann von den beteiligten DIZ-Standorten anfordert und für einen Abgleich zur temporären Verarbeitung erhält. In diesen Fällen erfolgt in der übergreifenden Treuhandstelle ein manueller Abgleich der hierfür notwendigen IDAT. Zu beachten ist, dass für diese Art des Record Linkage eine für die Herausgabe von IDAT im Klartext durch den DIZ-Standort ausreichende Rechtsgrundlage, wie etwa eine informierte Einwilligung auf Basis der Einwilligungsdokumente der MII, besteht.

Für die Einbindung einer übergreifenden Treuhandstelle können in der MII zwei unterschiedliche Verfahren implementiert werden.

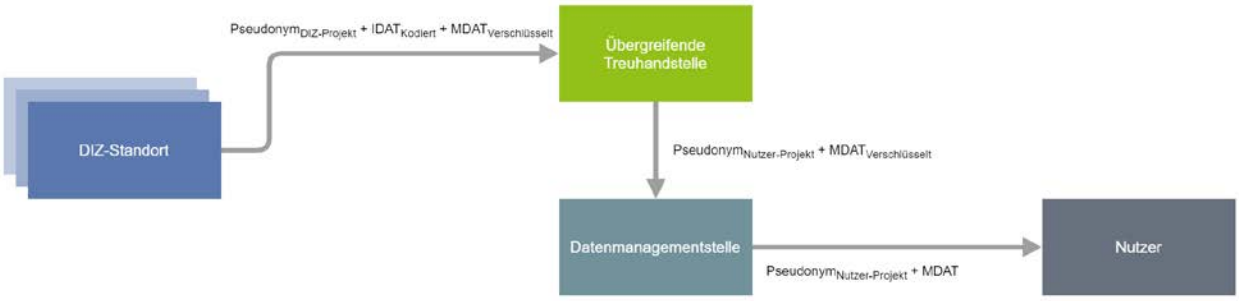

Abb. 6 Einbindung einer übergreifenden Treuhandstelle beim Record Linkage mit verschlüsselter Durchleitung von MDAT

Das erste Modell sieht eine Verortung der übergreifenden Treuhandstelle zwischen den Gebern und der Datenmanagementstelle vor. In diesen Fällen übermittelt die übergreifende Treuhandstelle die ermittelten eindeutigen Pseudonyme ($Pseudonym_{Nutzer\text{-}Projekt}$) nicht zurück an die Geber, sondern weiter an die Datenmanagementstelle. Die MDAT werden dann entweder so verschlüsselt, dass die übergreifende Treuhandstelle diese nicht entziffern kann. Die übergreifende Treuhandstelle leitet diese dann unverändert an die Datenmanagementstelle weiter (siehe Abb. 6). Alternativ kann ein temporäres Token oder Zugriffsticket verwendet werden, um die Pseudonyme ($Pseudonym_{Nutzer\text{-}Projekt}$) und MDAT in der Datenmanagementstelle wieder korrekt einander zuzuordnen, obwohl erstere von der übergreifenden Treuhandstelle und letztere von den Gebern übermittelt wurden (siehe Abb. 7). Das Durchleiten der MDAT in verschlüsselter Form und die Methode der Zuordnung anhand eines Tokens oder Zugriffstickets sind aus Sicht des Datenschutzes grundsätzlich als gleichwertig zu betrachten [15, S. 111].

Nach dem zweiten Modell der Einbindung einer übergreifenden Treuhandstelle besteht hingegen zwischen dieser und der Datenmanagementstelle keine Verbindung. Die von der übergreifenden Treuhandstelle ermittelten Pseudonyme werden dann zunächst an die Geber zurück übermittelt und im Falle von Daten-Herausgaben mit den MDAT von den Gebern an die Datenmanagementstelle übermittelt (siehe Abb. 8).

Für eine Daten-Nutzung im Sinne einer verteilten Analyse kommt nur Modell 2 in Betracht, da in diesen Fällen keine Zusammenführung von MDAT in einer Datenmanagementstelle erfolgt und die übergreifend erstellten und eindeutigen Pseudonyme in den DIZ für die verteilte Analyse benötigt werden. Für Daten-

Herausgaben können hingegen beide Modelle umgesetzt und grundsätzlich als gleichwertig angesehen werden. Allerdings kann die Information, welche MDAT von welchem DIZ-Standort stammen, nur in Modell 1 mit Hilfe bestimmter Implementierungsvorgaben vor der Datenmanagementstelle verborgen werden.

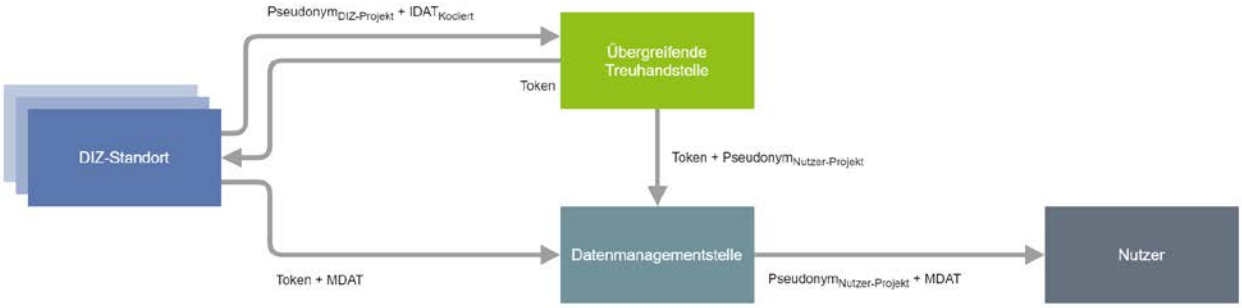

Abb. 7 Einbindung einer übergreifenden Treuhandstelle beim Record Linkage mit direkter Übermittlung der MDAT an die Datenmanagementstelle

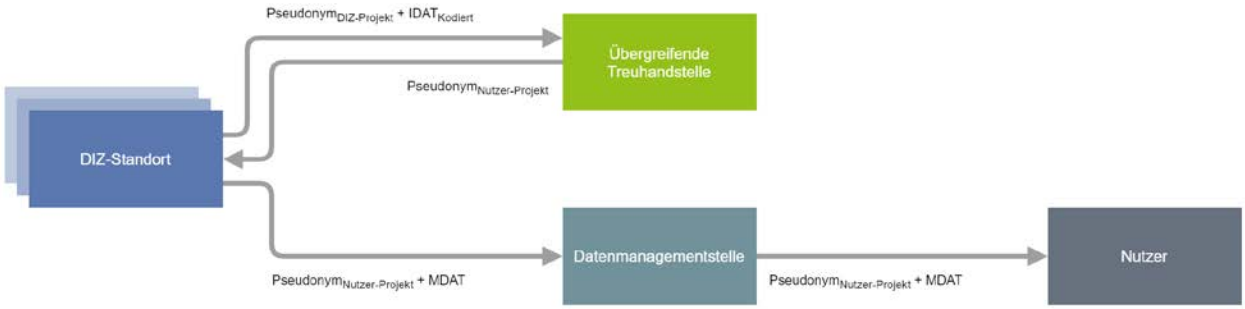

Abb. 8 Einbindung einer übergreifenden Treuhandstelle beim Record Linkage mit bidirektionaler Anbindung der Treuhandstelle an die DIZ-Standorte

6.2.6.3 Beschränkung der Verarbeitung auf notwendige Daten

Jeder Nutzungsantrag muss genaue Angaben dazu enthalten, welche Daten (Fälle und Variablen) für die Beantwortung der zugrundeliegenden wissenschaftlichen Fragestellung benötigt werden. Diese Datenauswahl muss insbesondere von den UACs der DIZ-Standorte kritisch geprüft und letztlich bestätigt werden, wenn es zu einer Daten-Nutzung kommen soll (vergl. Kap. 6.2.2.3). Die genaue Festlegung der ausgewählten Daten ist gleichermaßen für verteilte Analysen und Daten-Herausgaben relevant. In beiden Fällen wird die tatsächliche Verarbeitung personenbezogener Daten auf die im Nutzungsantrag angegebene Datenauswahl beschränkt. Das heißt, dass auch im Falle verteilter Analysen vor der Durchführung der verteilten Analyse bei jedem Geber zunächst eine Selektion der relevanten Daten erfolgt, die dann kopiert und isoliert für die Anwendung der verteilten Analyse zur Verfügung gestellt werden. Die Auswertungsskripte der Nutzer „sehen“ somit auch nur den Teil der Daten, der für die Beantwortung der wissenschaftlichen Fragestellung wirklich notwendig ist.

Bei Notwendigkeit aufgrund der wissenschaftlichen Fragestellung können in Einzelfällen aus den IDAT auch Angaben zum Geburtsdatum, die genauer sind als die Angabe von Geburtsjahr und Quartal, sowie Angaben zur Postleitzahl oder Gemeindekennziffer der Patientenadresse für die Bereitstellung zusammen mit den MDAT beantragt werden (vergl. Kap. 5.1.2). Diese Angaben unterliegen vor einer Freigabe für die

Daten-Nutzung einer besonderen Prüfung durch die zuständigen UACs. Eine Nutzung dieser Daten ist ausführlich von den Antragstellern zu begründen. Die Begründung muss sich auch auf den für die Auswertung notwendigen Detailgrad der Angaben beziehen. Alters- und Adressangaben sind immer soweit wie möglich zu vergröbern, ohne dass dadurch die beabsichtigte Auswertung gefährdet wird.

Bei Daten-Herausgaben an die Nutzer wird durch die Verwendung projektspezifischer Pseudonyme ($Pseudonym_{Nutzer\text{-}Projekt}$) zudem sichergestellt, dass Datensätze aus verschiedenen Projekten und von demselben Patienten bei ein und demselben Nutzer nicht anhand des mitübermittelten Pseudonyms zusammengeführt werden können. Insofern wird auch in diesen Fällen eine Beschränkung auf die notwendigen Daten je Projekt durch die gewählten Verfahrensweisen effektiv unterstützt.

6.2.7 Technische Grundsätze der Verarbeitungen

Die folgenden Grundsätze der Verarbeitung betreffen alle Verarbeitungen von Patientendaten im Rahmen der in Kap. 2 beschriebenen Anwendungsszenarien. Spezifische Regelungen und Vorgaben für die DIZ finden sich in Kap. 6.2.8 und für die übergreifende Treuhandstelle bzw. Datenmanagementstelle in Kap. 6.2.9.

6.2.7.1 Authentifizierung von Benutzern

Bis auf an anderen Stellen dieses Konzepts formulierten Vorgaben obliegt es den einzelnen Stellen, die Authentifizierung von Benutzern umzusetzen und im jeweiligen Datenschutzkonzept der Stelle darzulegen. DIZ-Standorten wird empfohlen, die Prüfung von Identität und Berechtigung von Benutzern durch das lokale Use & Access Komitee im Rahmen der Freischaltung einer Benutzerkennung vorzunehmen. Zudem wird den beteiligten Stellen der Einsatz von etablierten Authentifizierungsverfahren wie etwa OpenID Connect mit OAuth2 oder SAML 2.0 empfohlen.

6.2.7.2 Authentifizierung von Komponenten

Zugriffe von lokalen DIZ-Komponenten auf Komponenten einer übergreifenden Treuhandstelle oder einer Datenmanagementstelle erfolgen ausschließlich nach erfolgreicher Authentifizierung und Autorisierung der zugreifenden Komponenten. Dabei kommen etablierte Verfahren bzw. vom BSI empfohlene Verfahren zum Einsatz. Gleiches gilt für Zugriffe zwischen Komponenten einer übergreifenden Treuhandstelle und einer Datenmanagementstelle.

6.2.7.3 Datenübermittlungen

Die verschiedenen an einer Daten-Nutzung beteiligten Stellen kommunizieren über das öffentliche Internet. Die Sicherheit dieser Kommunikationsverbindungen wird mittels folgender Maßnahmen gewährleistet:

- Die Kommunikation zwischen den einzelnen Standorten erfolgt grundsätzlich über verschlüsselte Verbindungen (HTTPS). Die zum Einsatz kommenden Schlüssel und Zertifikate werden so erstellt, dass sie den aktuell anerkannten Anforderungen entsprechen (z. B. Schlüssellänge, Algorithmus, siehe BSI TR-02102[18]).
- Die Erstellung der nötigen Schlüssel und Zertifikate erfolgt in sicheren Umgebungen und ebenfalls entsprechend den Vorgaben des BSI.

[18] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

- Durch Firewalls wird sichergestellt, dass die Server, auf denen in die standortübergreifende Kommunikation eingebundene Softwarekomponenten betrieben werden, nur über die Protokolle und Ports erreichbar sind, die für die Kommunikation mit Benutzern oder mit Softwarekomponenten anderer Stellen unbedingt erforderlich sind (in der Regel HTTPS-Verbindungen).
- Zusätzlich zur Firewall sollen Reverse-Proxys sicherstellen, dass die in standortübergreifende Kommunikation eingebundenen Komponenten nicht direkt über eine öffentliche Internetadresse erreichbar sind. Die Komponenten sollen hinter den jeweiligen Reverse-Proxys angesiedelt und durch diese verborgen werden.
- Soweit möglich, wird der Bereich der zugriffsberechtigten Stellen auf IP-Ebene eingeschränkt.
- Es findet keine Übermittlung elektronischer Daten auf Datenträgern statt.

Vor jeder Übermittlung personenbeziehbarer Patientendaten werden die Voraussetzungen hierfür von der sendenden Stelle überprüft. Die Überprüfung der Voraussetzungen wird von der sendenden Stelle dokumentiert.

6.2.7.4 Protokollierung von Datenübermittlungen

Jegliche Übermittlung von personenbezogenen Patientendaten bzw. Pseudonymen zwischen beteiligten Stellen innerhalb der MII wird sowohl von der sendenden als auch der empfangenden Stelle mit folgenden Angaben protokolliert:

- Sendende und empfangende Stelle
- Datum und Uhrzeit der Übermittlung
- Spezifikation und Umfang der Daten
- Kontext oder Anlass der Übermittlung

Die aufgezeichneten Daten werden von den beteiligten Stellen für folgende Zwecke verarbeitet und eingesehen:

- im Rahmen der technischen Administration (Systemoptimierung und Fehlersuche)
- im Rahmen regelmäßiger Revisionsprüfungen (Innenrevision)
- im Rahmen der Aufdeckung möglicher Missbrauchsfälle (durch Stichproben und Suchen nach auffälligen Mustern)
- zur Erstellung anonymisierter Nutzungsstatistiken
- zum Nachweis der Datennutzung innerhalb der MII
- zur Wahrung der Informationspflichten der datenverarbeitenden Stellen
- zur Gewährleistung der Auskunftsrechte gegenüber betroffenen Personen

6.2.7.5 Auftragsverarbeitung

Es wird gewährleistet, dass personenbezogene Patientendaten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Es findet in diesen Fällen eine regelmäßige Kontrolle eines Auftragnehmers durch den Auftraggeber statt. Die Mitarbeiter eines Auftragnehmers werden auf das Datengeheimnis verpflichtet. Soweit Patientendaten zur Kenntnis genommen werden könnten, müssen die Mitarbeiter eines Auftragnehmers auch als „Mitwirkende“ der Ärzte im Sinne von § 203 StGB verpflichtet werden.

6.2.7.6 Getrennte Umgebungen

Entwicklungs-, Test- und Produktiv-Umgebungen sind strikt voneinander getrennt.

6.2.7.7 Kontinuierlicher Verbesserungsprozess

Ziel ist es, den Datenschutz kontinuierlich zu überprüfen und ggf. zu verbessern. Die Wirksamkeit der getroffenen Maßnahmen wird regelmäßig überprüft und mit den gesetzlichen Anforderungen abgeglichen.

Erforderliche Korrekturen können sich z. B. ergeben aus:

- Datenschutzvorfällen
- Anfragen von Mitarbeitern
- Anfragen von Patienten
- externe Anfragen
- neue Technologien/Sicherheitslücken
- sich verändernden Prozessen

Die Verantwortlichen und die Anwender/Nutzer werden in den Datenschutzprozess einbezogen. Jeder kann Verbesserungsvorschläge einbringen. Die Datenschutzdokumente werden jährlich auf Aktualität geprüft und ggf. angepasst.

6.2.8 Sicherheit der Verarbeitungen in den Datenintegrationszentren

Wie bereits in Kap. 1.2 beschrieben, fokussiert das vorliegende Datenschutzkonzept nicht die Datenschutzmaßnahmen an den einzelnen DIZ-Standorten. Hierfür sind jeweils lokale Datenschutzkonzepte ausgearbeitet worden, die detailliert die Regelungen und Maßnahmen an den DIZ-Standorten beschreiben. Generell gilt, dass die DIZ-Standorte als universitätsklinische Standorte auch in die Behandlung von Patienten eingebunden sind und als Standorte der Maximalversorgung mit großen jährlichen Fallzahlen auch nach § 6 der BSI-Kritisverordnung zu den kritischen Infrastrukturen zählen. Insofern gelten für diese Standorte erhöhte Anforderungen in Bezug auf die IT-Sicherheit.[19] Damit kann für diese Standorte eine umfangreiche Erfahrung im Umgang mit sensiblen Patientendaten sowie mit Verfahren zum Schutz dieser Daten vorausgesetzt werden.

Die jeweiligen DIZ-Standorte sind für die Sicherheit der gespeicherten Daten verantwortlich und bilden dies in lokalen Datenschutzkonzepten ab. Hierunter fallen auch die Prozesse zum Aufbau und zur kontinuierlichen Befüllung der jeweiligen Datenbestände. Den lokalen Treuhandstellen obliegt die Gewährleistung der Datensicherheit der für den Zweck der Pseudonymisierung gespeicherten Daten. Dies wird ebenfalls in den lokalen Datenschutzkonzepten der DIZ-Standorte dargelegt.

Insoweit die Rolle der Datenmanagementstelle im Rahmen eines Nutzungsvertrags von einem DIZ-Standort übernommen wird, treffen die hier gemachten Feststellungen auch auf die Datenmanagementstelle zu. Ergänzende bzw. spezifische Anforderungen sind im nachfolgenden Kapitel aufgeführt.

[19] siehe https://www.bsi.bund.de/SharedDocs/Textbausteine/DE/KRITIS/B3S/Gesundheit/2021_August_Gesundheit.html

6.2.9 Sicherheit der Verarbeitungen in der übergreifenden Treuhandstelle und der Datenmanagementstelle

6.2.9.1 Zugriff durch Systemadministratoren

Die an der jeweiligen Stelle gespeicherten Daten können prinzipiell von Standortadministratoren der jeweiligen IT-Infrastruktur eingesehen werden. Zugriffe auf die Daten durch Administratoren dürfen nur erfolgen, wenn dies zur Erfüllung ihrer Aufgaben zwingend erforderlich ist. Alle Administratoren sind schriftlich zu diesem Grundsatz und zur Verschwiegenheit zu verpflichten. Eine solche schriftliche Verschwiegenheitserklärung ist durch die jeweilige Stelle zu regeln und kann ggf. durch die bereits bei der Einstellung von Mitarbeitern unterzeichneten Erklärungen abgedeckt sein.

6.2.9.2 Zugangskontrolle

Server sind in standardkonformen Serverräumen gemäß BSI IT-Grundschutz-Kompendium (oder vergleichbare Richtlinien) untergebracht. Nur berechtigte Personen erhalten entsprechend ihres Tätigkeitsbereichs Zutritt zu den Servern. Arbeitsplätze entsprechen den im BSI Grundschutz-Kompendium genannten Anforderungen. Dabei werden zumindest folgende technische Maßnahmen eingesetzt:

- Die Serverräume sind als geschlossene Sicherheitsbereiche konzipiert.
- Der Zutritt ist durch Zutrittskontrollmechanismen geschützt.
- Die Serverräume sind mit ausreichend sicheren Türen und (falls vorhanden) Fenstern ausgestattet.
- Büroräume sind verschließbar.

Zumindest folgende organisatorische Maßnahmen werden eingesetzt:

- Schlüssel werden nur auf schriftliche Anweisung von einer autorisierten Person ausgegeben.
- Die Zahl der zugangsberechtigten Personen zu Serverräumen ist auf das erforderliche Minimum begrenzt.
- Schlüssel zu Serverräumen werden zeitnah eingezogen oder gesperrt (elektronische Schließsysteme), wenn der Zugang zu diesen Räumen nicht mehr erforderlich ist.
- Der Diebstahl oder Verlust von Schlüsseln wird unverzüglich gemeldet. Maßnahmen zur Gewährleistung bzw. Wiederherstellung der Sicherheit sind vorgesehen und werden zeitnah umgesetzt.
- Erfolgt aus Sicherheitsgründen eine Verteilung der Zugriffsrechte zu verschiedenen Systemen auf unterschiedliche Personengruppen, so wird die Zugangsberechtigung zu den Systemen in entsprechender Weise verteilt.
- Dokumentation der zugangsberechtigen Personen.
- Besucher bzw. fremdes Personal haben nur in Begleitung von berechtigten Mitarbeitern Zugang zu Servern.

6.2.9.3 Datenträgerkontrolle

Endgeräte, auf denen personenbezogene Patientendaten gespeichert werden, müssen in einer sowohl netzwerktechnisch als auch physisch besonders gesicherten Umgebung betrieben werden. Eingesetzte technische Maßnahmen:

- Alle Systeme auf denen personenbezogene Patientendaten gespeichert werden, werden physisch besonders gesichert.

- Werden Server oder Endgeräte auf denen personenbezogene Patientendaten gespeichert werden, etwa zu Reparaturzwecken an Dritte weitergegeben, so werden die Festplatten vorab entfernt und einbehalten.
- Wird die Zweckbestimmung von Servern oder von Endgeräten, auf denen personenbezogene Patientendaten gespeichert wurden, geändert, sodass sie in Bereichen geringerer Sicherheit eingesetzt werden, so werden die Festplatten ersetzt oder entsprechend den Empfehlungen des BSI bereinigt.
- Werden die enthaltenen Daten nicht mehr benötigt, so werden Speichermedien auf denen personenbezogene Patientendaten gespeichert wurden, datenschutzgerecht entsorgt oder entsprechend den Empfehlungen des BSI bereinigt.
- Werden Standard-Endgeräte ausgesondert oder ihre Zweckbestimmung geändert, so werden Festplatten oder integrierte Datenspeicher entsprechend den Empfehlungen des BSI bereinigt.
- Die digitale Speicherung personenbezogener Daten außerhalb des gesicherten Bereichs (z. B. off-site Backups) erfolgt ausschließlich in verschlüsselter Form.

Eingesetzte organisatorische Maßnahmen:

- Datenträger (sowohl digital als auch in Papierform) mit personenbezogenen Patientendaten werden in Abwesenheit zugriffsberechtigter Personen in verschlossenen Räumen oder Behältern verwahrt. Außerhalb von solchen Räumen oder Behältnissen werden sie stets so aufbewahrt bzw. behandelt, dass Unbefugte keinen Zugang oder Einblick haben.
- Alle Speichermedien, die personenbezogene Patientendaten enthalten könnten, werden nach Ende der Lebensdauer datenschutzgerecht entsorgt.

6.2.9.4 Speicherkontrolle

Eingesetzte technische Maßnahmen:

- Benutzerkontrolle (siehe Kap. 6.2.9.6), Zugangskontrolle (siehe Kap. 6.2.9.2) und Zugriffskontrolle (siehe Kap. 6.2.9.5).
- Personenbezogene Daten werden gelöscht sobald diese nicht mehr benötigt werden.

Eingesetzte organisatorische Maßnahmen:

- Der Kreis der nutzungsberechtigten Personen und der Umfang der erteilten Berechtigungen sind auf das Mindestmaß beschränkt.

6.2.9.5 Zugriffskontrolle

Alle Teilsysteme sind durch Zugriffsberechtigungen gesichert, die entsprechend der jeweiligen Aufgaben vergeben werden. Die Berechtigungen sind dabei auf ein Mindestmaß beschränkt. Es sind damit nur speziell autorisierte und zur strikten Vertraulichkeit verpflichtete Benutzer in der Lage, die zur Erfüllung ihrer Aufgabe notwendigen Maßnahmen im jeweiligen IT-System durchzuführen.

Eingesetzte technische Maßnahmen:

- Einsatz eines Zugriffsberechtigungssystems mit differenzierten Berechtigungen, z. B. für Lesen, Löschen und Bearbeiten. Berechtigungen können bei Bedarf entzogen werden.
- Differenzierte Berechtigungen für Anwendung, Datenbankserver und Betriebssystem.

Eingesetzte organisatorische Maßnahmen:

- Berechtigungen werden nur auf schriftliche Anweisung von einer autorisierten Person mit zugehöriger Protokollierung vergeben.
- Berechtigungen werden auf „need-to-know“ Basis vergeben und protokolliert.
- Es ist gewährleistet, dass nicht mehr benötigte Berechtigungen zeitnah entzogen werden.
- Alle zugriffsberechtigten Personen sind schriftlich darauf verpflichtet, den Zugriff auf personenbezogene Daten auf das zur Erfüllung der Tätigkeit erforderliche Maß zu beschränken.
- Alle zugriffsberechtigten Personen wurden schriftlich zur Verschwiegenheit zu verpflichtet sofern dies nicht schon im Rahmen der Einstellung erfolgt und damit abgedeckt ist.

6.2.9.6 Benutzerkontrolle

Eingesetzte technische Maßnahmen:

- Benutzer müssen sich authentifizieren, um Zugang zu den verwendeten Systemen zu erlangen (zumindest mit Benutzername/Passwort).
- Bei ausschließlicher Verwendung von Passwörtern werden die Komplexität von Passwörtern, die Häufigkeit von Passwortwechseln sowie die Begrenzung der Anzahl oder Häufigkeit fehlgeschlagener Login-Versuche technisch entsprechend den Empfehlungen des BSI zum Passwortgebrauch durchgesetzt.[20]
- Alle Systeme, auf denen personenbezogene Daten gespeichert werden, sind durch dedizierte Firewalls gegen das Internet abgeschirmt.
- Der netzwerkbasierte Zugriff auf die Server ist auf die erforderlichen Netzwerkprotokolle beschränkt (z. B. Portfreigaben).

Eingesetzte organisatorische Maßnahmen:

- Benutzerkonten werden nur auf schriftliche Anweisung von einer autorisierten Person erstellt.
- Benutzerkonten ausscheidender Mitarbeiter werden zeitnah gesperrt.
- Soweit Regeln zum Passwortgebrauch nicht technisch durchgesetzt werden können (z. B. Verbot der Weitergabe von Kennwörtern, Vorgehensweise bei Kenntnisnahme von Kennwörtern durch Dritte), sind alle Benutzer schriftlich auf ihre Einhaltung verpflichtet.

6.2.9.7 Eingabekontrolle

Eingesetzte technische Maßnahmen:

- Die Dateneingabe erfolgt ausschließlich durch authentisierte Personen (siehe Kap. 6.2.9.6).
- Protokollierung von Eingaben/Änderungen/Löschungen mit Dokumentation der zugreifenden Person, des Zeitpunkts des Zugriffes sowie des Kontexts des Zugriffes (z. B. Informationen zu Aufrufen und Abfrageergebnissen).
- Bei automatischer Datenübernahme Protokollierung der Datenherkunft bzw. Datenabstammung (Data Provenance).

[20] aktuell siehe ORP.4.A8 in https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2021.pdf

Eingesetzte organisatorische Maßnahmen:

- Die Benutzer sind über die Protokollierung (s. o.) im Rahmen der Autorisierung informiert (Nutzungsvereinbarung).

6.2.9.8 Wiederherstellbarkeit

Eingesetzte technische Maßnahmen:

- Regelmäßiges, automatisiertes und verschlüsseltes off-site Backup, das eine angemessene Zeit (min. 30 Tage) zur Verfügung steht.

Eingesetzte organisatorische Maßnahmen:

- Für alle verwendeten Systeme bestehen gültige Wartungsverträge. Alternativ können Ersatzgeräte vorgehalten werden.
- Ein Backupkonzept existiert und ist umgesetzt.
- Ein Wiederanlaufplan liegt vor.
- Notfallprozeduren und die Wiederherstellbarkeit der Backups werden regelmäßig getestet.

6.2.9.9 Zuverlässigkeit

Eingesetzte technische Maßnahmen:

- Die Server und Serverumgebungen werden überwacht. Auffälligkeiten werden automatisch gemeldet.
- Sicherheitsrelevante Updates werden auf allen Systemen (sowohl Server als auch Endgeräte) zeitnah eingespielt.
- Soweit für das jeweilige Betriebssystem verfügbar und vom BSI empfohlen wird Antiviren-Software eingesetzt und regelmäßig aktualisiert.
- Weitere Maßnahmen siehe Verfügbarkeitskontrolle (Kap. 6.2.9.10).
- An den Standorten wird Bedarf an und Verfügbarkeit von redundanten Serverkomponenten geprüft und entsprechend eingesetzt.

Eingesetzte organisatorische Maßnahmen:

- Meldewege im Falle auftretender Störungen oder betriebs- oder sicherheitsrelevanter Ereignisse sind etabliert und getestet.
- Standardisierte Vorgehensweisen zur Änderungsverfolgung und zur Systemvalidierung sind etabliert.
- Alle Benutzer sind im sicheren Umgang mit den verwendeten Systemen unterwiesen und wurden zur Einhaltung der entsprechenden Richtlinien verpflichtet.

6.2.9.10 Verfügbarkeitskontrolle

Eingesetzte technische Maßnahmen:

- Auswahl der Serverräume entsprechend den Empfehlungen des BSI (Minimierung der Gefährdung durch Umwelteinflüsse, Verwendung von Klimaanlagen, unterbrechungsfreien Stromversorgung etc.).
- Ausstattung der Serverräume entsprechend den Empfehlungen des BSI (insb. ausreichend dimensionierte Kühlung und unterbrechungsfreie Stromversorgung).
- Beim Betrieb der Serverfestplatten werden Mechanismen der fehlertoleranten Speicherung (z. B. RAID) verwendet.

- Regelmäßiges off-site Backup der Nutzdaten sowie der zur Gewährleistung des sicheren und datenschutzkonformen Betriebs erforderlichen Daten (Protokolldaten etc.).
- Redundante Auslegung von Servern und Infrastruktur.

Eingesetzte organisatorische Maßnahmen:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.
- Es existiert ein Backup-Konzept.
- Die Wiederherstellbarkeit der Backups wird regelmäßig getestet.

6.2.9.11Sensibilisierung/ Schulungskonzept

Es ist wichtig, dass die Einhaltung des Datenschutzes der Betroffenen von allen Anwendern unterstützt wird. Die Maßnahmen dafür müssen den Anwendern bei der täglichen Arbeit bewusst sein. Die Anwender werden bei der Schulung explizit auch im Datenschutz geschult. Die Schulungen finden bei Projektbeginn statt. Regelmäßige Auffrischungsschulungen stellen die Aufrechterhaltung bzw. Steigerung des Datenschutzniveaus sicher.

6.3 Prozesse und Risiken

6.3.1 Einteilung und Bewertung der Risiken

Der Einteilung und Bewertung von Risiken werden zwei Bewertungskriterien mit folgender Skalierung zu Grunde gelegt:

1. Auswirkung (Schadenshöhe)
- Auswirkung ist für die Betroffenen unwesentlich (Score 1)
- Auswirkung ist für die Betroffenen geringfügig (Score 2)
- Auswirkung ist für die Betroffenen kritisch (Score 3)
- Auswirkung ist für die Betroffenen katastrophal (Score 4)

2. Wahrscheinlichkeit
- Eintritt des Risikos ist unvorstellbar (Score 1)
- Eintritt des Risikos ist unwahrscheinlich (Score 2)
- Eintritt des Risikos ist entfernt vorstellbar (Score 3)
- Eintritt des Risikos ist gelegentlich (Score 4)
- Eintritt des Risikos ist häufig (Score 5)

Abhängig vom jeweils hergestellten Produkt, dem eingesetzten und diskutierten technischen System und dem damit verbundenen Prozess sind die oben genannten und allgemein gefassten Kriterien zu konkretisieren.

Mehrere Ursachen, die zum selben Fehler und zur selben Fehlerfolge führen, haben demnach alle die gleiche Bedeutung, aber unterschiedliche Auftretenswahrscheinlichkeiten und damit am Ende unterschiedliche Risikobewertungen. Aus der Beziehung zwischen Auswirkung und der Wahrscheinlichkeit des Eintretens wird die Risikoklasse ermittelt. Bei der Bewertung bedeutet die Klasse 1 ein akzeptables Risiko, Klasse 2 bedeutet, dass das Risiko so niedrig, wie vernünftigerweise praktikabel ist (ALARP, as low as reasonably practicable). Die Klasse 3 bedeutet ein inakzeptables Risiko. Eine Übersicht über die Einteilung in Risikoklassen je nach Wahrscheinlichkeit und Schadenshöhe gibt Abb. 9.

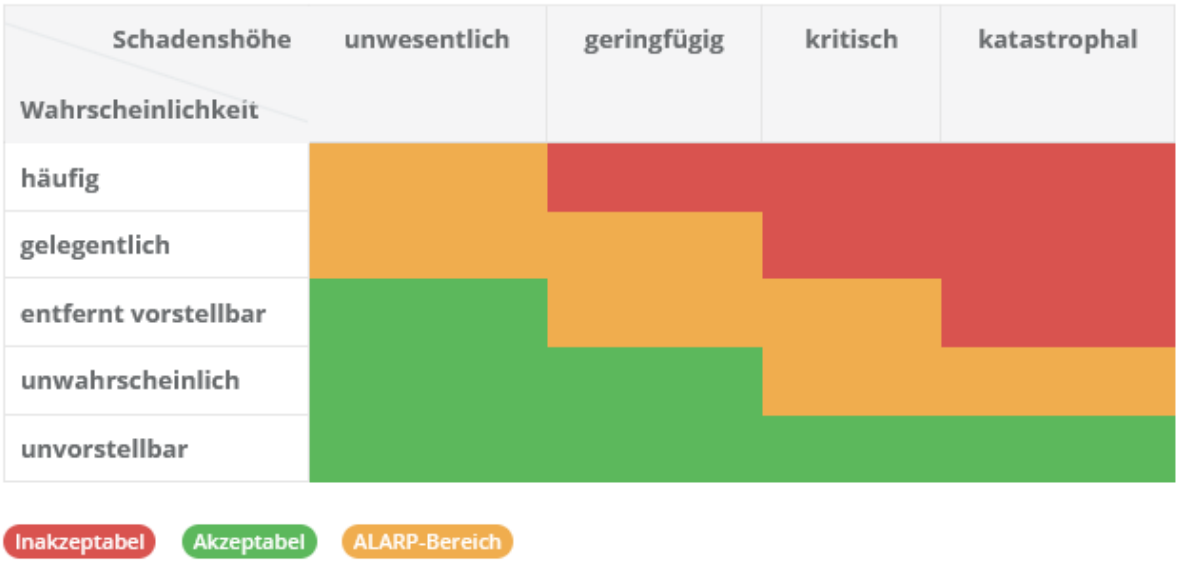

Abbildung 9: Verfahren der Risikobewertung

Die Bewertung aller Risiken erfolgt jeweils unter Berücksichtigung aller technischen und organisatorischen Schutzmaßnahmen.

6.3.2 Machbarkeitsanfragen

6.3.2.1 Prozessbeschreibung

Die Fallzahlanfrage dient der Vorabauskunft für Forschende, ob für ihre wissenschaftliche Fragestellung ausreichend Daten vorhanden sind. Die Ergebnisse sind nicht für eine Publikation geeignet und dürfen dafür nicht verwendet werden. Forschende müssen sich beim Forschungsdatenportal für Gesundheit registrieren, um die Funktionen der Machbarkeitsanfrage nutzen zu können.

Forschende können aus den zur Verfügung stehenden Datenelementen eine Anfrage zusammenstellen. Dies geschieht im Idealfall mithilfe einer Weboberfläche, die eine Zusammenstellung ermöglicht. Für Anfragen, die sich damit nicht abbilden lassen, ist es möglich, die Anfrage in Form einer Abfragesprache zusammenzustellen (z. B. FHIR-Search). In beiden Fällen haben die Forschenden dabei keinen Zugriff auf die zugrundeliegenden Daten. Sollen nur Patienten gezählt werden, für die eine Einwilligung vorliegt, kann dies als Filteroption gesetzt werden.

Die Anfragen werden als FHIR-Search-Query durch das Forschungsdatenportal an alle Standorte verteilt. Die Anfrage selbst hat keinen Personenbezug. Außerdem werden keine personenbeziehbaren Daten der Forschenden versendet. Die DIZ-Standorte führen die Anfrage in ihren FHIR-Servern auf den Patientendaten aus und generieren eine Summe in Form einer Patienten- oder Fallzahl unter Berücksichtigung der ausgewählten Kriterien und Datenelemente (zum Beispiel Blutdruck). Zur Absicherung der Anonymität der zurückgemeldeten Fallzahlen wird auf die Ausführungen in Kap. 6.2.6.1 verwiesen.

Den Forschenden werden als Ergebnis die rückgemeldeten Summen angezeigt, jedoch ohne Hinweis, von welchem Standort die Zahlen stammen. Das Forschungsdatenportal fasst bei Bedarf einzelne Ergebnisse zusammen, um sicherzustellen, dass der liefernde Standort nicht aus den Ergebnissen ableitbar ist.

6.3.2.2 Schutzbedarf

Tab. 2 Schutzbedarf bei Machbarkeitsanfragen

Gewährleistungsziel	Schutzbedarfsklasse	Begründung
Vertraulichkeit	Normal	Ausschließlich kumulierte Daten, kein Personenbezug
Integrität	Normal	Es wird ein absichtlich verfälschtes Ergebnis übermittelt
Verfügbarkeit	Normal	Ggf. keine sofortige Übermittlung des Ergebnisses möglich, es sind keine kritischen Prozesse mit der sofortigen Beantwortung der Anfragen verbunden

6.3.2.3 Risiken für die Rechte und Freiheiten der Betroffenen

Tab. 3 Unrechtmäßiger Zugriff auf Daten

Frage	Einschätzung
Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Einzelne Gesundheitsdaten einer bestimmten Person können offengelegt werden.
Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Gezielte Anfragen zur Offenlegung einer bestimmten Person.
Was sind die Risikoquellen?	Risikoquelle können mehrere gezielte Anfragen sein, die über Tracker oder Homogenitätsangriffe eine einzelne Person identifizieren können.
Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Alle Rückmeldungen werden verrauscht, eine genaue Darstellung der Maßnahmen zur Sicherstellung der Anonymisierung findet sich in Kap. 6.2.6.1
Wie ist die Einschätzung des Risikoschweregrades, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☐unwesentlich ☒geringfügig ☐kritisch ☐katastrophal
Wie ist die Einschätzung der Eintrittswahrscheinlichkeit des Risikos, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐unvorstellbar ☐unwahrscheinlich ☒entfernt vorstellbar ☐gelegentlich ☐häufig

Analyse der Ursachen und Folgen von unrechtmäßigen Zugriffen auf Daten und Einschätzung von deren Schweregrad und Eintrittswahrscheinlichkeit

Tab. 4 Unerwünschte Veränderung von Daten

Frage	Einschätzung
Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Bei der Veränderung von Daten treten keine direkten Auswirkungen für die betroffenen Personen ein.
Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Die Abfrageskripte können falsche Ergebnisse liefern.
Was sind die Risikoquellen?	Risikoquellen können schlecht programmierte Abfrageskripte sein.
Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Abfrageskripte werden vor Ausführung durch 4-Augenprinzip überprüft. Zudem werden Plausibilisierungen von Ergebnissen im Forschungsdatenportal durchgeführt. Weitere Hinweise in Kap. 6.2.7.6
Wie ist die Einschätzung des Risikoschweregrades, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒unwesentlich ☐geringfügig ☐kritisch ☐katastrophal
Wie ist die Einschätzung der Eintrittswahrscheinlichkeit des Risikos, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐unvorstellbar ☐unwahrscheinlich ☒entfernt vorstellbar ☐gelegentlich ☐häufig

Analyse der Ursachen und Folgen einer unerwünschten Veränderung der Daten und Einschätzung von deren Schweregrad und Eintrittswahrscheinlichkeit

Tab. 5 Datenverlust

Frage	Einschätzung
Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Bei dem Verlust von Daten treten keine direkten Auswirkungen für die betroffenen Personen ein.
Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Fehler bei der Speicherung und der Übermittlung der Ergebnisse.
Was sind die Risikoquellen?	Fehlendes Backup, ungesicherte Übertragungswege.
Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Backupkonzept, gesicherte Übertragungswege, siehe Beschreibungen in Kap. 6.2.8, 6.2.9.8, 6.2.9.9
Wie ist die Einschätzung des Risikoschweregrades, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒unwesentlich ☐geringfügig ☐kritisch ☐katastrophal
Wie ist die Einschätzung der Eintrittswahrscheinlichkeit des Risikos, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐unvorstellbar ☒unwahrscheinlich ☐entfernt vorstellbar ☐gelegentlich ☐häufig

Analyse der Ursachen und Folgen von Datenverlust und Einschätzung von deren Schweregrad und Eintrittswahrscheinlichkeit

6.3.2.4 Bewertung der Risiken

Tab. 6 Bewertung der Risiken bei Machbarkeitsanfragen

Ergebnis der Risikobewertung	☒ Akzeptabel ☐ ALARP (‚so niedrig, wie vernünftigerweise praktikabel‘) ☐ Inakzeptabel

Für eine ausführlichere Bewertung und Prüfung ist ein Formular im Anhang (Abschnitt 9.3) enthalten.

6.3.3 Verteilte Analysen

6.3.3.1 Prozessbeschreibung

Verteilte Analysen sind ein für die Analyse von Daten relevanter und zur Überlassung von Daten komplementärer Ansatz. Hierbei wird eine Analyse der für ein Auswertungsprojekt bewilligten Daten des Gebers am jeweiligen DIZ-Standort selbst vorgenommen und die erzielten Zwischenergebnisse können an

weitere Standorte weitergegeben, bzw. zentral zusammengeführt werden. Die Zwischenergebnisse sind dabei nicht mehr auf einzelne Individuen zurückführbar (anonym).

Daten für verteilte Analysen werden ebenso beantragt wie Daten, die für eine Analyse aus den DIZ-Standorten ausgeleitet werden sollen. Dazu reichen die Antragsteller einen Projektantrag beim Deutschen Forschungsdatenportal für Gesundheit ein. An jedem DIZ-Standort prüft das jeweilige UAC, ob Daten im benötigten Umfang zum beantragten Projekt beigetragen werden können, ob der DIZ-Standort sich am Projekt beteiligen möchte und ob es eine Rechtsgrundlage für die Analyse der benötigten Daten gibt. Wird der Antrag abgelehnt, endet der Prozess an dieser Stelle für den jeweiligen DIZ-Standort.

Nach Abschluss eines Nutzungsvertrags stellt der Nutzer die für die Durchführung der Analysen notwendigen Analysemethoden und -Routinen zur Verfügung. Diese können in Form eines Software-Containers (z. B. Docker-Container), in Form eines Scripts (z. B. R oder Python) oder auch in Form von Auswertungsvorgaben für eine bestimmte Plattform für verteilte Auswertungen (z. B. DataSHIELD) ausgestaltet sein. Zusätzlich zu diesen Analysemethoden und -Routinen reicht der Nutzer eine Erklärung der Unbedenklichkeit in Bezug auf Schadsoftware ein. Die Einreichung dieser Methoden samt der Bescheinigung erfolgt je nach Festlegung im Nutzungsvertrag bei der dort ebenfalls festgelegten Datenmanagementstelle oder dem Forschungsdatenportal. In jedem Fall wird eine weitere, zentrale Prüfung der Analysemethoden und -Routinen durch Experten der MII organisiert. Dadurch soll möglichst vermieden werden, dass über die Analysemethoden und -Routinen Schadsoftware in die Standorte eingetragen wird. Zudem soll durch die Analysemethoden und -Routinen schon sichergestellt werden, dass die Analyseergebnisse frei von Personenbezug sind.

Die Geber erhalten die Analysemethoden und -Routinen dann je nach Festlegung im Nutzungsvertrag von der Datenmanagementstelle oder dem Forschungsdatenportal als koordinierender Stelle. Beim Transfer an die Geber wird auf Protokollebene oder mit Hilfe ergänzender Prüfsummen o. ä. sichergestellt, dass keine unbemerkte Veränderung der Analysemethoden und -Routinen im Rahmen des Transfers geschieht. Wird eine Plattform wie etwa DataSHIELD für die Verteilung der Analysemethoden und -Routinen an die Geber genutzt, wird diese Plattform vorher auf die fehlerfreie Übertragung von Analysemethoden und -Routinen geprüft.

Die Geber stellen sicher, dass in der jeweiligen lokalen Umgebung, auf die die Analysemethoden und -Routinen zugreifen können, nur die für die Auswertung benötigten und beantragten Daten (Fälle und Variablen) zugreifbar sind (vergl. Kap. 0). Zudem wird sichergestellt, dass die Analysemethoden und Routinen in einer geschützten Umgebung ausgeführt werden, von der aus weder ein Zugriff auf das interne Netz der DIZ-Standorte noch auf das Internet möglich ist (Sandboxing). Wenn eine umfassend geprüfte Plattform für verteilte Analysen verwendet wird, kann die Kommunikation über einen kontrollierten Kanal zu einer festgelegten zentralen Stelle über das Internet erlaubt bleiben.

In dem Fall, dass für die Auswertung die Kennzeichnung von Datensätzen ein und desselben Patienten an verschiedenen Standorten mit demselben Pseudonym erforderlich ist, kann eine übergreifende Treuhandstelle für die Erstellung und Zuordnung solch standortübergreifend eindeutiger Pseudonyme eingebunden werden (vergl. Kap. 6.2.6.2). Nach dem Start und der Durchführung der Analyse an den Standorten prüft ein Mitarbeiter die Ergebnisse auf Vollständigkeit und Anonymität, bevor diese zurück an die zentrale Stelle (Datenmanagementstelle oder Forschungsdatenportal) geschickt werden. Auch die Rückübermittlung von Ergebnissen wird auf Protokollebene oder mit Hilfe von ergänzenden Prüfsummen o. ä. gegen unbemerkte Veränderungen abgesichert. Im Falle der Nutzung einer übergreifenden Plattform

wie etwa DataSHIELD, wird diese zuvor auf die korrekte Ermittlung sicherer anonymer Ergebnisse und deren korrekte Übertragung hin überprüft.

Wenn vorgesehen ist, dass eine weitere Aggregation der Ergebnisse vor der Übermittlung an den Nutzer stattfinden muss, wird diese je nach Festlegung im Nutzungsvertrag durch die Datenmanagementstelle oder das Forschungsdatenportal vorgenommen. Der Nutzer erhält dann die von allen Gebern zusammengetragenen Ergebnisse je nach Festlegung im Nutzungsvertrag von der Datenmanagementstelle oder dem Forschungsdatenportal. Auch diese Ergebnisübermittlung wird entweder auf Protokollebene oder durch ergänzende Prüfsummen o. ä. gegen unbemerkte Veränderungen abgesichert.

6.3.3.2 Schutzbedarf

Tab. 7 Schutzbedarf bei verteilten Analysen

Gewährleistungsziel	Schutzbedarfsklasse	Begründung
Vertraulichkeit	Normal	Ausschließlich kumulierte Daten, kein Personenbezug
Integrität	Hoch	Die Ergebnisse sollten exakt sein.
Verfügbarkeit	Normal	Keine sofortige Übermittlung des Ergebnisses erforderlich, es sind keine Zeit-kritischen Prozesse mit der sofortigen Beantwortung der Anfragen verbunden. Dennoch sollen als verfügbar erklärte Daten am Ende auch tatsächlich verfügbar sein.

6.3.3.3 Risiken für Rechte und Freiheiten der Betroffenen

Tab. 8 Unrechtmäßiger Zugriff auf Daten

Frage	Einschätzung
Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Patientendaten können offengelegt werden.
Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Unerlaubte Zugriffe auf weitere Daten im internen Netz der DIZ-Standorte und unerlaubte Ausleitungen von Daten über das Internet
Was sind die Risikoquellen?	Fehler oder Schadcode in den Analysemethoden und -Routinen oder deren fehlerhafte Übertragung bzw. Manipulation bei der Übertragung.
Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Qualitätssicherungsmaßnahmen wie in der Prozessbeschreibung beschrieben. Es werden nur entsprechend geprüfte Analysemethoden und -Routinen ausgeführt. Entweder findet eine Kontrolle der Ergebnisdaten lokal statt oder es wird eine vorher umfangreich geprüfte Plattform eingesetzt. Durch Ausführung der Analysemethoden und -Routinen in einer geschützten Umgebung (Sandboxing) werden Zugriffe auf das interne Netz und das Internet verhindert (s. Prozessbeschreibung). Zur Pseudonymisierung der Daten siehe Kap. 6.2.6.2, zur Beschränkung der zugreifbaren Daten siehe Kap. 0.
Wie ist die Einschätzung des Risikoschweregrades, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☐unwesentlich ☒geringfügig ☐kritisch ☐katastrophal
Wie ist die Einschätzung der Eintrittswahrscheinlichkeit des Risikos, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐unvorstellbar ☐unwahrscheinlich ☒entfernt vorstellbar ☐gelegentlich ☐häufig

Analyse der Ursachen und Folgen von unrechtmäßigen Zugriffen auf Daten und Einschätzung von deren Schweregrad und Eintrittswahrscheinlichkeit

Tab. 9 Unerwünschte Veränderung von Daten

Frage	Einschätzung
Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Bei der Veränderung von Daten treten keine direkten Auswirkungen für die betroffenen Personen ein.
Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Die Analysemethoden und -Routinen können falsche Ergebnisse liefern oder Ausgangsdaten ändern.
Was sind die Risikoquellen?	Risikoquellen können schlecht programmierte Analysemethoden und -Routinen sein.
Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Analysemethoden werden vor Ausführung umfangreich geprüft (siehe Prozessbeschreibung). Die Auswertung selbst findet nur auf Kopien der Daten statt (siehe Kap. 0)
Wie ist die Einschätzung des Risikoschweregrades, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒unwesentlich ☐geringfügig ☐kritisch ☐katastrophal
Wie ist die Einschätzung der Eintrittswahrscheinlichkeit des Risikos, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐unvorstellbar ☐unwahrscheinlich ☒entfernt vorstellbar ☐gelegentlich ☐häufig

Analyse der Ursachen und Folgen einer unerwünschten Veränderung der Daten und Einschätzung von deren Schweregrad und Eintrittswahrscheinlichkeit

Tab. 10 Datenverlust

Frage	Einschätzung
Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Bei dem Verlust von Daten treten keine direkten Auswirkungen für die betroffenen Personen ein.
Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Fehler bei der Speicherung und der Übermittlung der Ergebnisse bzw. Fehler bei der Ausführung von Analysemethoden und -Routinen.
Was sind die Risikoquellen?	Fehlendes Backup, ungesicherte Übertragungswege. Löschung von Daten durch Analysemethoden und -Routinen.
Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Zur Wiederherstellbarkeit und Verfügbarkeit von Daten siehe Kap. 6.2.9.8und 6.2.9.10, zur Absicherung der Ergebnisübermittlungen siehe die Prozessbeschreibung und Kap. 6.2.7.3. Analysemethoden werden vor Ausführung umfangreich geprüft (siehe Prozessbeschreibung). Die Auswertung selbst findet nur auf Kopien der Daten statt (siehe Kap. 0)
Wie ist die Einschätzung des Risikoschweregrades, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒unwesentlich ☐geringfügig ☐kritisch ☐katastrophal
Wie ist die Einschätzung der Eintrittswahrscheinlichkeit des Risikos, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐unvorstellbar ☒unwahrscheinlich ☐entfernt vorstellbar ☐gelegentlich ☐häufig

Analyse der Ursachen und Folgen von Datenverlusten und Einschätzung von deren Schweregrad und Eintrittswahrscheinlichkeit

6.3.3.4 Bewertung der Risiken

Tab. 11 Bewertung der Risiken bei verteilten Analysen	
Ergebnis der Risikobewertung	☒ Akzeptabel ☐ ALARP (‚so niedrig, wie vernünftigerweise praktikabel‘) ☐ Inakzeptabel

Für eine ausführlichere Bewertung und Prüfung ist ein Formular im Anhang (Abschnitt 9.3) enthalten.

6.3.4 Daten-Herausgaben

6.3.4.1 Prozessbeschreibung

Für wissenschaftliche Projekte bzw. Fragestellungen, die auf der Basis verteilter Analysen nicht durchgeführt werden können, werden pseudonymisierte Individualdaten den Nutzern zu Auswertungszwecken übermittelt.
Antragsteller reichen hierzu einen Projektantrag beim Deutschen Forschungsdatenportal für Gesundheit ein. Der Projektantrag muss eine Beschreibung der angefragten Daten sowie die Ein- und Ausschlusskriterien für die Patientenauswahl enthalten. Jeder DIZ-Standort prüft, ob er Daten im benötigten Umfang zum beantragten Projekt beitragen kann, ob er sich am Projekt beteiligen möchte und ob es eine Rechtsgrundlage für die Ausleitung und Analyse der benötigten Daten gibt. Wird der Antrag abgelehnt, endet der Prozess an dieser Stelle für den DIZ-Standort.

Nach Abschluss eines Nutzungsvertrags startet die Daten-Nutzung. Sobald alle organisatorischen Grundlagen gelegt sind und das Projekt in die aktive Phase kommt, werden die Geber aufgefordert, die beantragten Daten bereitzustellen. Dazu extrahieren sie die angefragten Daten aus ihren Systemen. Je nach Komplexität des Projekts und lokalen Bedingungen können dafür mehrere Umsetzungsschritte erforderlich werden. Bei der Extraktion muss berücksichtigt werden, dass nur die Daten von Patienten verwendet werden, für deren Verarbeitung eine entsprechende Rechtsgrundlage vorliegt, was im Regelfall eine informierte Einwilligung auf Basis der Einwilligungsdokumente der MII sein sollte (vergl. Kap. 3.2.3.1).

Die Geber stellen sicher, dass die Daten im erforderlichen Format, in der notwendigen Qualität und ausschließlich gemäß bewilligtem Projektantrag bereitgestellt werden. Dafür prüfen sie die Datensätze nach Erzeugung dahingehend, ob die erwarteten Patientenzahlen mit den beantragten Datenelementen enthalten sind.

Lokale Patientenpseudonyme ($Pseudonym_{DIZ}$) werden vor der Ausleitung durch projektspezifische Pseudonyme ($Pseudonym_{DIZ\text{-}Projekt}$) ersetzt. Standortübergreifend eindeutige Pseudonyme ($Pseudonym_{Nutzer\text{-}Projekt}$) werden dann entweder von der Datenmanagementstelle oder einer übergreifenden Treuhandstelle erstellt. In den Fällen, in denen für die Auswertung der Daten die Datensätze ein und desselben Patienten von mehreren Standorten als zueinander gehörig gekennzeichnet werden müssen und dies im Antrag bereits so dargestellt wurde, wird immer eine übergreifende Treuhandstelle eingebunden, die dann die Erstellung der standortübergreifend eindeutigen Pseudonyme

nach einem vorher durchgeführten Record Linkage übernimmt. Eine ausführliche Darstellung dieses Prozesses mit seinen verschiedenen Varianten findet sich in Kap. 6.2.6.2.

Die Übermittlung der Daten erfolgt dann je nach durchgeführtem Record Linkage und Zuständigkeit für die Erstellung standortübergreifend eindeutiger Pseudonyme entweder direkt an die Datenmanagementstelle oder über die übergreifende Treuhandstelle an die Datenmanagementstelle.

Die Datenmanagementstelle nimmt die Daten aller Geber entgegen und führt eine grobe Plausibilisierung der Daten nach der Anzahl und Art der übermittelten Variablen durch. Sie führt die vorliegenden Daten in einem großen Datensatz zusammen und tauscht (wenn dies nicht schon durch eine übergreifende Treuhandstelle übernommen wurde) die projektspezifischen Pseudonyme der Geber ($Pseudonym_{DIZ\text{-}Projekt}$) gegen neue standortübergreifend eindeutige Pseudonyme ($Pseudonym_{Nutzer\text{-}Projekt}$) aus. Anschließend werden die einzelnen Datensätze nach Zufallsprinzip durchmischt, um die Zuordenbarkeit zu den Gebern zu minimieren.

Die Datenmanagementstelle archiviert sowohl die gelieferten Rohdaten als auch die an den Nutzer ausgeleiteten Daten und alle für die Aufbereitung verwendeten Algorithmen sowie ggf. auch die Zuordnung der DIZ-spezifischen mit den übergreifend gültigen Pseudonymen ($Pseudonym_{DIZ\text{-}Projekt}$ und $Pseudonym_{Nutzer\text{-}Projekt}$) für die Dauer des Nutzer-Projekts und nach guter wissenschaftlicher Praxis und den Vorgaben des Nutzungsvertrags noch 10 Jahre darüber hinaus. In den Fällen, in denen eine übergreifende Treuhandstelle eingebunden wird, ist diese für die Speicherung und Archivierung der Zuordnung der Pseudonyme ($Pseudonym_{DIZ\text{-}Projekt}$ und $Pseudonym_{Nutzer\text{-}Projekt}$) für die Dauer des Nutzer-Projekts und nach guter wissenschaftlicher Praxis und den Vorgaben des Nutzungsvertrags noch 10 Jahre darüber hinaus zuständig.

Nutzer können ihre Daten über eine https-verschlüsselte Webseite herunterladen. Sie müssen sich hierfür authentifizieren. Ihre Authentifizierung und Autorisierung wird durch das Forschungsdatenportal für Gesundheit vor dem Download gegengeprüft.

Erzeugen die Nutzer während ihrer Analysen weitere Daten, die individuell einzelnen Pseudonymen zugeordnet werden können, also abgeleitete Daten, so werden diese an die Geber zurückübermittelt. Hierzu läuft der Prozess der Datenausleitung „rückwärts“. Nutzer können die Daten zusammen mit den erhaltenen Pseudonymen ($Pseudnym_{Nutzer\text{-}Projekt}$) auf einer verschlüsselten Webseite der Datenmanagementstelle hochladen. Die Datenmanagementstelle nimmt sie entgegen und sortiert die einzelnen Datensätze mithilfe der eigenen archivierten Daten oder unter Einbindung der übergreifenden Treuhandstelle den jeweiligen Standorten und den von diesen ursprünglich übermittelten Pseudonymen ($Pseudonym_{DIZ\text{-}Projekt}$) zu. Im Anschluss erfolgt dann die Übermittlung der einzelnen Daten – ggf. auch unter Einbindung der übergreifenden Treuhandstelle – an die jeweiligen Geber.

6.3.4.2 Schutzbedarf

Tab. 12 Schutzbedarf bei Daten-Herausgaben

Gewährleistungsziel	Schutzbedarfsklasse	Begründung
Vertraulichkeit	Hoch	Daten der Schutzstufe D-E (vergl. Kap. 5.3)
Integrität	Hoch	Ggf. nicht korrekter Daten zur Auswertung übermittelt
Verfügbarkeit	Normal	Ggf. keine sofortige Übermittlung der Daten zur Auswertung möglich

6.3.4.3 Risiken für Rechte und Freiheiten der Betroffenen

Tab. 13 Unrechtmäßiger Zugriff auf Daten

Frage	Einschätzung
Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Einzelne Gesundheitsdaten einer bestimmten Person können offengelegt werden.
Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Offenlegung von personenbezogenen Gesundheitsdaten durch Datenherausgabe an oder Kenntnisnahme durch nicht berechtigte Personen
Was sind die Risikoquellen?	Fehler bei der Datenbereitstellung, eine nicht ausreichend abgesicherte Datenübermittlung oder unzulässige Methoden der Datennutzung
Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Beschränkung auf notwendige Verarbeitungen (Kap. 6.2.2) Beschränkung der Verarbeitung auf notwendige Daten (Kap. 0) Pseudonymisierung (Kap. 6.2.6.2) Sichere Datenübermittlungen (Kap. 6.2.7.2, 6.2.7.3 und 6.2.7.4) Sicherheitsmaßnahmen bei den beteiligten Stellen (Kap. 6.2.8 und 6.2.9) Vertragliche Verpflichtungen der Nutzer und weiterer beteiligter Stellen (Kap. 6.2.1)
Wie ist die Einschätzung des Risikoschweregrades, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☐unwesentlich ☒geringfügig ☐kritisch ☐katastrophal
Wie ist die Einschätzung der Eintrittswahrscheinlichkeit des Risikos, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐unvorstellbar ☐unwahrscheinlich ☒entfernt vorstellbar ☐gelegentlich ☐häufig

Analyse der Ursachen und Folgen von unrechtmäßigen Zugriffen auf Daten und Einschätzung von deren Schweregrad und Eintrittswahrscheinlichkeit

Tab. 14 Unerwünschte Veränderung von Daten

Frage	Einschätzung
Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Bei der Veränderung von Daten treten keine direkten Auswirkungen für die betroffenen Personen ein, da im DIZ und in den weiteren beteiligten Stellen immer nur mit Kopien von Behandlungsdaten gearbeitet wird. Indirekte Folgen sind hingegen möglich, z. B. bei der Rückmeldung fehlerhafter Ergebnisse aus der Forschung o. ä. (s. Kap. 7.2).
Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Fehler bei der Herausgabe/Zusammenstellung von Daten, bei der Übermittlung oder Nutzung der Daten beim Nutzer
Was sind die Risikoquellen?	Fehlerhafte Herausgaben oder Zusammenstellungen von Daten, fehlerhafte Übermittlungen oder fehlerhafte Auswertungen
Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Beschränkung auf notwendige Verarbeitungen (Kap. 6.2.2) Beschränkung der Verarbeitung auf notwendige Daten (Kap. 0) Sichere Pseudonymisierungsverfahren (Kap. 6.2.6.2) Sichere Datenübermittlungen (Kap. 6.2.7.2, 6.2.7.3 und 6.2.7.4) Sicherheitsmaßnahmen bei den beteiligten Stellen (Kap. 6.2.8 und 6.2.9) Prüfschritte im Prozessablauf (siehe Prozessbeschreibung) Vertragliche Verpflichtungen der Nutzer und weiterer beteiligter Stellen (Kap. 6.2.1)
Wie ist die Einschätzung des Risikoschweregrades, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒unwesentlich ☐geringfügig ☐kritisch ☐katastrophal
Wie ist die Einschätzung der Eintrittswahrscheinlichkeit des Risikos, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐unvorstellbar ☐unwahrscheinlich ☒entfernt vorstellbar ☐gelegentlich ☐häufig

Analyse der Ursachen und Folgen einer unerwünschten Veränderung der Daten und Einschätzung von deren Schweregrad und Eintrittswahrscheinlichkeit

Tab. 15 Datenverlust

Frage	Einschätzung
Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Bei dem Verlust von Daten treten keine direkten Auswirkungen für die betroffenen Personen ein, da dieser immer nur Kopien von Behandlungsdaten in den DIZ oder weiteren beteiligten Stellen betrifft. Indirekte Folgen sind hingegen möglich, wenn z. B. wichtige Ergebnisse aufgrund von Datenverlust nicht zurückgemeldet werden können (s. Kap. 7.2).
Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Fehler bei der Speicherung und der Übermittlung von Daten oder Ergebnissen.
Was sind die Risikoquellen?	Fehlerhafte Speicherung oder Übertragung von Daten bei einer der beteiligten Stellen
Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Sichere Datenübermittlungen (Kap. 6.2.7.2, 6.2.7.3 und 6.2.7.4) Maßnahmen zur Verfügbarkeit (Kap. 6.2.9.10) und Wiederherstellbarkeit (Kap. 6.2.9.8) Sicherheitsmaßnahmen an den DIZ-Standorten (Kap. 6.2.8) Zugangs- (Kap. 6.2.9.2), Zugriffs- (Kap. 6.2.9.5) und Speicherkontrolle (Kap. 6.2.9.4) Vertragliche Verpflichtungen der Nutzer und weiterer beteiligter Stellen (Kap. 6.2.1)
Wie ist die Einschätzung des Risikoschweregrades, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒unwesentlich ☐geringfügig ☐kritisch ☐katastrophal
Wie ist die Einschätzung der Eintrittswahrscheinlichkeit des Risikos, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐unvorstellbar ☒unwahrscheinlich ☐entfernt vorstellbar ☐gelegentlich ☐häufig

Analyse der Ursachen und Folgen von Datenverlust und Einschätzung von deren Schweregrad und Eintrittswahrscheinlichkeit

6.3.4.4 Bewertung der Risiken

Tab. 16 Bewertung der Risiken bei Daten-Herausgaben

Ergebnis der Risikobewertung	☒ Akzeptabel ☐ ALARP (‚so niedrig, wie vernünftigerweise praktikabel‘) ☐ Inakzeptabel

Für eine ausführlichere Bewertung und Prüfung ist ein Formular im Anhang (Abschnitt 9.3) enthalten.

6.4 Ergebnis der Datenschutzfolgenabschätzung

Aus Sicht der Taskforce Datenschutz der MII als Autor dieses Datenschutzkonzepts bestehen bei den hier beschriebenen Anwendungsszenarien für die von der Datenverarbeitung betroffenen Patienten keine hohen Risiken für deren Rechte und Freiheiten, die eine vorherige Konsultation nach Art. 36 DSGVO erfordern würden. Dieser Einschätzung liegt eine detaillierte Bewertung der in diesem Konzept beschriebenen, umfangreichen technischen und organisatorischen Maßnahmen zugrunde.

Das vorliegende Konzept fokussiert standortübergreifende Prozesse und Verarbeitungen in der MII, an denen jeweils mehrere unterschiedliche Stellen in der MII beteiligt sind. Insofern kann die Bewertung von Risiken und eindämmenden Maßnahmen im Rahmen einer Datenschutz-Folgenabschätzung nicht alle jeweils an den beteiligten Stellen lokal geregelten Prozesse vollständig berücksichtigen. Insbesondere konnte auch kein Abgleich mit lokalen Datenschutzkonzepten oder Geschäftsordnungen durchgeführt werden. Insofern muss an den beteiligten Stellen die Datenschutz-Folgenabschätzung unter Berücksichtigung lokaler Prozesse und den hierfür geltenden Regeln und Policies komplettiert werden. Hierfür wurden im Anhang in Abschnitt 9.3 ergänzende Formulare hinterlegt, mit deren Hilfe die Bewertungsprozesse der beteiligten Stellen dokumentiert werden können. Hierbei ist insbesondere zu prüfen, ob Grundannahmen dieses Konzepts möglicherweise durch Besonderheiten vor Ort unterlaufen oder in besonderer Weise abgeschwächt werden oder auf sonstige Weise besondere Risiken vor Ort im Rahmen der Beteiligung an einem der hier beschriebenen Anwendungsszenarios entstehen können, für die keine ausreichenden lokalen oder übergreifenden technischen oder organisatorischen Gegenmaßnahmen bestehen.

7. Umsetzung von Betroffenenrechten

7.1 Auskunft

7.1.1 Zweck

Patienten haben das Recht, nach Art. 15 DSGVO Auskunft über die Daten zu verlangen, die von ihnen im Rahmen eines der hier beschriebenen Anwendungsszenarios (vergl. Kap. 2) verarbeitet werden. Über dieses Recht sind sie von der verantwortlichen Stelle zu informieren. Welche Stellen diese Verantwortlichkeit trifft und wie ggf. die Zuständigkeiten im Rahmen von gemeinsamer Verantwortlichkeit geregelt sind, ist in Kap. 4 beschrieben. Zu den Informationspflichten gehört auch, die Stelle anzugeben, an die sich ein Patient mit seinem Auskunftsersuchen zu richten hat.

7.1.2 Prozess

Da die Identitätsdaten (IDAT) von Patienten nur in den für die Behandlung zuständigen DIZ-Standorten vorgehalten werden (vergl. Kap. 5.3), sind diese aktuell die einzigen Stellen, die Auskunftsersuchen entgegennehmen und bearbeiten können. Am DIZ-Standort kann ein Abgleich der Identitätsdaten mit den von der lokalen Treuhandstelle gespeicherten Identitätsdaten (je nach Art der Umsetzung in kodierter oder unkodierter Form) erfolgen. Nach einer Validierung des Auskunftsersuchens (die personenbezogenen Patientendaten dürfen nicht ohne entsprechende Kontrolle der Berechtigung herausgegeben werden) kann dann das lokale Pseudonym ($Pseudonym_{DIZ}$) mit Hilfe der lokalen Treuhandstelle ermittelt werden, so dass die mit diesem Pseudonym gekennzeichneten Datensätze identifiziert und für die Auskunftserteilung zusammengestellt werden können.

Im Rahmen von Daten-Nutzungen können bei den Nutzern auch individuell patientenbezogene Daten in Form abgeleiteter Daten nach Ziff. 1.11 NO neu entstehen, für die das Auskunftsrecht nach Art. 15 DSGVO ebenfalls gilt. Für diese Fälle muss am DIZ-Standort überprüft werden, ob Daten des auskunftsersuchenden Patienten in Nutzungsprojekte mit Daten-Herausgaben eingegangen sind. Ist das der Fall, muss das zugehörige projektspezifische Pseudonym ($Pseudonym_{DIZ\text{-}Projekt}$) – ggf. unter Einbindung einer Treuhandstelle, die dieses in ein standortübergreifendes, aber projektspezifisches Pseudonym ($Pseudonym_{Nutzer\text{-}Projekt}$) übersetzt – an die in diesem Nutzerprojekt benannte Datenmanagementstelle geschickt werden. Die Datenmanagementstelle ermittelt entweder das zugehörige, standortübergreifende und projektspezifische Pseudonym ($Pseudonym_{Nutzer\text{-}Projekt}$) selbst oder bekommt es von einer eingebundenen übergreifenden Treuhandstelle übermittelt und kann mit diesem – koordiniert durch das Forschungsdatenportal – die Kontaktierung des Nutzers veranlassen. Der Nutzer ist gemäß Nutzungsvertrag in solchen Fällen zur Mitwirkung verpflichtet und kann mit Hilfe des übermittelten Pseudonyms ($Pseudonym_{Nutzer\text{-}Projekt}$) die abgeleiteten Daten zurückübermitteln, die dann über die Datenmanagementstelle und ggf. eine eingebundene Treuhandstelle zurück an den DIZ-Standort übermittelt werden. Dieser kann somit auch abgeleitete Daten aus Nutzerprojekten in die für eine Auskunftserteilung erstellte Datensammlung mit aufnehmen.

7.1.3 Grenzen

Ein Ausschluss der Auskunftserteilung zum Wohl der betroffenen Person ist nach § 630g BGB möglich, wenn es um Daten geht, die aus der Patientenakte stammen. Diese Regelung setzt die Öffnungsklausel aus Art. 23 (1) i DSGVO im nationalen Recht um. Dem Ausschluss sind dabei hohe Hürden gesetzt [4, S. 221]. Weitere Beschränkungen sind in § 27 (2) BDSG formuliert und betreffen zum einen Situationen,

in denen die Wahrnehmung des Auskunftsrechts voraussichtlich die Verwirklichung der Forschungszwecke unmöglich macht oder ernsthaft beeinträchtigt und die Beschränkung des Auskunftsrechts für die Erfüllung der Forschungszwecke notwendig ist. Zum anderen sind Situationen genannt, in denen Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand bedeuten würde. Diese Regelungen berufen sich auf die Öffnungsklauseln für nationale Gesetze in Art. 89 (2) DSGVO, ohne diese aber weiter zu konkretisieren oder zu spezifizieren.

7.2 Re-Kontaktierung und Ergebnismitteilung

7.2.1 Zweck

Patienten können im Rahmen einer Einwilligungserklärung gemäß der Einwilligungsdokumente der MII in die folgenden Re-Kontaktierungsoptionen einwilligen:

- Um von ihnen zusätzliche, für wissenschaftliche Fragen relevante Informationen zu erfragen, sie über neue Forschungsvorhaben/Studien zu informieren und/oder ihre Einwilligung in die Verknüpfung ihrer Patientendaten mit medizinischen Informationen aus anderen Datenbanken einzuholen, und/oder
- um sie über medizinische Zusatzbefunde zu informieren.

Zusätzlich wird in den Einwilligungsdokumenten der MII darauf hingewiesen, dass unabhängig von der Einwilligung in eine der beiden genannten Optionen eine Kontaktaufnahme erfolgen kann, um den Patienten über ihren behandelnden Arzt oder ihren Hausarzt eine Rückmeldung über Analyseergebnisse zu geben, die für sie persönlich von erheblicher Bedeutung sein könnten. Diese Re-Kontaktierungsoption, die im Rahmen der Einwilligung auch nicht „deaktiviert“ bzw. abgelehnt werden kann, ist für Situationen gedacht, in denen aus der ärztlichen Ethik heraus oder gemäß ärztlichem Berufsrecht eine Rückmeldung sehr dringender, in jedem Fall handlungsrelevanter Ergebnisse zwingend erscheint. Da auf Basis der vorliegenden Versionen der Einwilligungsdokumente der MII nur aus der Behandlung stammende Daten in Forschungsprojekte eingebracht werden können und diese in aller Regel nur bereits befundete Daten enthalten, ist mit solchen Ausnahmesituationen tatsächlich wohl nur sehr selten, wenn überhaupt zu rechnen. Allerdings erlauben die Einwilligungsdokumente der MII die Speicherung der Daten über einen Zeitraum von 30 Jahren (vergl. Kap. 8), so dass für diesen langen Zeitraum nicht hinreichend sicher ausgeschlossen werden kann, dass Forschungsprojekte auch einmal zu Ergebnissen von solcher Handlungsrelevanz führen können.

Die Handreichung zu den Einwilligungsdokumenten der MII bindet jegliche Rückmeldung von Ergebnissen oder Zusatzbefunden an zwei wichtige Bedingungen:

- An den beteiligten DIZ-Standorten werden jeweils klar definierte, ethisch und klinisch angemessene Prozesse zum Umgang mit Zusatzbefunden etabliert.
- Zudem muss in den Projektanträgen auf den Umgang mit Zusatzbefunden eingegangen werden.

Eine Fußnote in der Handreichung zu den Einwilligungsdokumenten stellt zudem klar, dass der Begriff „Zusatzbefunde“ in diesem Kontext nicht so zu verstehen ist, dass damit Befunde im Sinne einer abgesicherten klinischen Diagnostik gemeint sind.

Auf Risiken einer Mitteilung von Zusatzbefunden, z. B. für den Abschluss privater Kranken- oder Lebensversicherungen oder auch mit Blick auf genetische Informationen, die auch etwas über enge Familienangehörige aussagen können, wird in der Patienteninformation der MII hingewiesen.

7.2.2 Prozess

Der Nutzer, dessen Forschungsprojekt zu einem Re-Kontaktierungsanlass führt, übermittelt diesen Umstand zusammen mit dem ihm übermittelten Pseudonym ($Pseudonym_{Nutzer\text{-}Projekt}$) an die Datenmanagementstelle, die wiederum entweder selbst oder mit Einbindung der für das Nutzungsprojekt benannten übergreifenden Treuhandstelle zum einen das zu dem Pseudonym passende DIZ ermittelt und zum anderen dieses Pseudonym in ein projektspezifisches Pseudonym des relevanten DIZ ($Pseudonym_{DIZ\text{-}Projekt}$) wandelt. Mit diesem DIZ-spezifischen Pseudonym können die Informationen dann an den in die Behandlung des Patienten eingebundenen DIZ-Standort übermittelt werden. Am DIZ-Standort kann dann ggf. mit Hilfe der lokalen Treuhandstelle aus dem projektspezifischen Pseudonym ($Pseudonym_{DIZ\text{-}Projekt}$) das im DIZ dauerhaft genutzte Pseudonym ($Pseudonym_{DIZ}$) und aus diesem mit Hilfe der lokalen Treuhandstelle auch die Identität des Patienten ermittelt werden.

An dem DIZ-Standort ist von den behandelnden Ärzten anhand der am Standort implementierten Richtlinien zu entscheiden, ob und in welcher Form die Ergebnisse oder die Re-Kontaktierungsanfrage an den Patienten herangetragen werden. Zudem muss zwingend geprüft werden, ggf. auch unter Einbindung der lokalen Treuhandstelle, ob die dokumentierte Einwilligungserklärung des Patienten eine solche Rückmeldung oder Re-Kontaktierung erlaubt. Sind diese Fragen alle positiv geklärt, kann eine Re-Kontaktierung des Patienten durch den DIZ-Standort als behandelnde Einrichtung erfolgen.

7.3 Widerruf

7.3.1 Zweck

Patienten haben nach Art. 7 (3) DSGVO jederzeit das Recht, ohne Angabe von Gründen ihre informierte Einwilligung zu widerrufen und nach Art. 17 (1) b DSGVO eine Löschung bzw. Anonymisierung ihrer auf Basis der Einwilligung verarbeiteten Patientendaten zu verlangen. Über dieses Recht werden sie in der zu der Einwilligungserklärung gehörenden Patienteninformation aufgeklärt. Dort wird auch eine Anlaufstelle für einen Widerruf benannt. Im Regelfall ist das eine Stelle oder Organisationseinheit innerhalb des DIZ-Standorts, der in die Behandlung eingebunden ist. Im Folgenden wird insofern generalisierend nur noch vom DIZ-Standort als zuständiger Stelle ausgegangen.

7.3.2 Prozess

Da die Identitätsdaten (IDAT) von Patienten nur in den für die Behandlung zuständigen DIZ-Standorten vorgehalten werden (vergl. Kap. 5.3), sind diese aktuell die einzigen Stellen, die Widerrufe entgegennehmen und bearbeiten können. Am DIZ-Standort kann ein Abgleich der Identitätsdaten mit den von der lokalen Treuhandstelle gespeicherten Identitätsdaten (je nach Art der Umsetzung in kodierter oder unkodierter Form) erfolgen. Nach einer Validierung des Widerrufs (die personenbezogenen Patientendaten dürfen nicht ohne entsprechende Kontrolle der Berechtigung gelöscht oder anonymisiert werden) kann dann das lokale Pseudonym ($Pseudonym_{DIZ}$) mit Hilfe der lokalen Treuhandstelle ermittelt werden, so dass die mit diesem Pseudonym gekennzeichneten Datensätze identifiziert und für die Löschung oder Anonymisierung markiert werden können.

Im Rahmen von Daten-Nutzungen können vom Widerruf betroffene Daten auch bei aktuellen Nutzern, einer Datenmanagementstelle und ggf. auch einer übergreifenden Treuhandstelle verarbeitet werden. Für diese Fälle muss am DIZ-Standort überprüft werden, ob Daten des widerrufenden Patienten in

Nutzungsprojekte mit Daten-Herausgaben eingegangen sind. Ist das der Fall, muss das zugehörige projektspezifische Pseudonym ($Pseudonym_{DIZ\text{-}Projekt}$) – ggf. unter Einbindung einer Treuhandstelle, die dieses in ein standortübergreifendes, aber projektspezifisches Pseudonym ($Pseudonym_{Nutzer\text{-}Projekt}$) übersetzt – an die in diesem Nutzerprojekt benannte Datenmanagementstelle geschickt werden. Die Datenmanagementstelle ermittelt entweder das zugehörige, standortübergreifende und projektspezifische Pseudonym ($Pseudonym_{Nutzer\text{-}Projekt}$) selbst oder bekommt es von einer eingebundenen übergreifenden Treuhandstelle übermittelt und kann mit diesem – koordiniert durch das Forschungsdatenportal – die Kontaktierung des Nutzers über das Forschungsdatenportal veranlassen. Der Nutzer ist gemäß Nutzungsvertrag in solchen Fällen zur Mitwirkung verpflichtet und kann mit Hilfe des übermittelten Pseudonyms ($Pseudonym_{Nutzer\text{-}Projekt}$) die vom Widerruf betroffenen Daten ermitteln.

Der Nutzer kann dann entweder die Daten löschen und dies gegenüber dem Forschungsdatenportal in Textform bestätigen. Das Forschungsportal leitet diese Information an alle beteiligten Stellen inklusive des betroffenen Gebers weiter, die dann ebenfalls die markierten Daten löschen oder anonymisieren. Anderenfalls kann der Nutzer einen begründeten Antrag auf Ausnahme von der vertraglichen Löschpflicht stellen und diesen Antrag an das Forschungsdatenportal leiten, welches diesen unter Einbindung einer übergreifenden Treuhandstelle oder der für das Projekt benannten Datenmanagementstelle an den betroffenen Geber weiterleitet. Das UAC des betroffenen Gebers muss dann über diesen Antrag entscheiden. Das Ergebnis dieser Prüfung wird über das Forschungsdatenportal dem Nutzer übermittelt, der dann entweder die Daten doch löschen und die oben beschriebene Bestätigungskaskade auslösen muss, oder im Falle einer positiven Bestätigung seines Antrags die betroffenen Patientendaten weiter verarbeiten darf. Das Forschungsdatenportal hat in jedem Fall solche Anträge und die Entscheidungen der UACs in anonymer Form auf einer Website öffentlich zugänglich zu dokumentieren.

Sind die Daten des widerrufenden Patienten in keine Daten-Nutzung eingegangen, werden alle für die Löschung oder Anonymisierung markierten Daten am DIZ-Standort gelöscht oder anonymisiert. Die lokale Treuhandstelle hat den Widerruf samt Umsetzung zu dokumentieren.

7.3.3 Grenzen

Nach Art. 17 (3) d DSGVO gilt das Recht auf Löschung der Betroffenen nicht, soweit dieses voraussichtlich die Verwirklichung wissenschaftlicher Forschungsziele unmöglich macht oder ernsthaft beeinträchtigt. Diese Ausnahme von der Löschpflicht ist somit auch die gesetzliche Grundlage für das oben beschriebene Antragsverfahren, welches Nutzern nach Ziff. 2.10 Abs. 3 und 4 NO eröffnet wird. Diese gesetzliche Grundlage kann in bestimmten Fällen allerdings auch für die Verarbeitung von Patientendaten am DIZ-Standort selbst gelten. Beispielhaft kann diese Regelung angewendet werden, wenn Patientendaten nach guter wissenschaftlicher Praxis zu Zwecken der Nachvollziehbarkeit von Forschungsprojekten archiviert werden und das Löschen eines der archivierten Datensätze die Nachvollziehbarkeit vollständig aufheben würde.[21]

[21] Dass Art. 17 (3) d DSGVO im Fall einer Archivierung nach guter wissenschaftlicher Praxis angewendet werden kann, wurde im Rahmen eines von der TMF vergebenen Gutachtens vom Gutachter Thilo Weichert bestätigt. Das Gutachten wird 2022 in der Schriftenreihe der TMF als Band 19 erscheinen.

7.4 Weitere Betroffenenrechte nach Art. 16, 18, 20 und 21 DSGVO

Die Umsetzung weiterer Betroffenenrechte erfolgt analog zu den bereits geschilderten Rechten. In den folgenden Abschnitten wird insoweit nur auf Besonderheiten der Umsetzung bzw. relevante Grenzen eingegangen.

7.4.1 Berichtigung nach Art. 16 DSGVO

Die Validierung eines Berichtigungsersuchens erfolgt analog zu Auskunftsersuchen oder Widerrufen. Die Identifikation von für die Berichtigung relevanten Datensätzen erfolgt analog zu Widerrufen. Sollte im Einzelfall die geforderte Berichtigung aus Sicht der beteiligten Stellen eher einer Verfälschung der Daten entsprechen, so ist dies im Zweifelsfall wie ein Widerruf zu werten.

7.4.2 Einschränkung nach Art. 18 DSGVO

Die Validierung eines Einschränkungsersuchens erfolgt analog zu Auskunftsersuchen oder Widerrufen. Die Identifikation von für die Einschränkung relevanten Datensätzen erfolgt analog zu Widerrufen. Es wird auf die Grenzen des Rechts auf Einschränkung verwiesen, die in Art. 16 (1) DSGVO benannt werden.

7.4.3 Datenübertragbarkeit nach Art. 20 DSGVO

Die Validierung einer Anforderung auf Datenübertragung nach Art. 20 DSGVO erfolgt analog zu Auskunftsersuchen oder Widerrufen. Die Identifikation der hierfür relevanten Datensätze am DIZ-Standort erfolgt analog zu Auskunftsersuchen oder Widerrufen. Da die Datenübertragbarkeit sich nur auf vom Patienten selbst bereitgestellte Daten bezieht, umfasst dieser Anspruch nicht die vollständigen Patientendaten. Ob ein Datum hiervon umfasst ist, ist im Einzelfall zu prüfen. In jedem Fall kann der Anspruch auf Datenübertragbarkeit vollständig von den jeweils betroffenen DIZ-Standorten als behandelnden Einrichtungen erfüllt werden. Eine Beteiligung weiterer Stellen ist hier nicht erforderlich, da Patienten diesen keine Daten „bereitstellen“.

7.4.4 Widerspruch nach Art. 21 DSGVO

Die Validierung eines Widerspruchs nach Art. 21 DSGVO erfolgt analog zu Widerrufen. Während Widerrufe sich auf eine Verarbeitung von Patientendaten beziehen, die auf eine informierte Einwilligung gestützt wird, geht es bei einem Widerspruch um eine Verarbeitung auf gesetzlicher Grundlage. Die Identifikation von Datensätzen, die von einem Widerspruch betroffen sind, erfolgt analog zu einem Widerruf. Die vom Widerruf betroffenen Daten sind nach Art. 21 (1) zu löschen oder zu anonymisieren, es sei denn, die verantwortliche Stelle kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder es geht nach Art. 21 (6) um eine Verarbeitung, die zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist.

8. Fristen (Dauer der Speicherung)

Gemäß den Einwilligungsdokumenten der MII können Patientendaten an den DIZ-Standorten im Falle einer vorliegenden Einwilligung für 30 Jahre ab dem Zeitpunkt der Einwilligung in pseudonymer Form für Forschungsprojekte vorgehalten werden. In besonderen Fällen können Patientendaten auch über diesen Zeitpunkt hinaus von erheblicher Bedeutung für die Wissenschaft sein. In diesen Fällen kann in Abstimmung mit den zuständigen Datenschutzaufsichtsbehörden und einer unabhängigen Ethikkommission geklärt werden, ob auch eine weitergehende Nutzung der betroffenen Patientendaten möglich ist.

Für nicht eingewilligte Daten können andere Fristen gelten, die sich aus dem jeweiligen Landeskrankenhausrecht ergeben können.

Im Rahmen von Daten-Nutzungen gelten die Fristen aus dem jeweiligen Nutzungsvertrag und den ergänzenden Allgemeinen Nutzungs- und Vertragsbedingungen. Dies schließt im Falle von Datenherausgaben auch eine Archivierungsfrist von 10 Jahren nach guter wissenschaftlicher Praxis für die im Projekt genutzten Patientendaten mit ein.

Nach Ablauf der Fristen werden die betroffenen Daten gelöscht oder wirksam anonymisiert. Die wirksame Anonymisierung kann somit eine Löschung ersetzen [6].

9. Anhang

9.1 Glossar

ABIDE	Aligning Biobanking and DIC Efficiently; ergänzendes Fördermodul der MII
AG	Arbeitsgruppe
ALARP	As Low As Reasonably Practicable; Begriff aus dem Risikomanagement
ANVB	Allgemeine Nutzungs- und Vertragsbedingungen für die Bereitstellung und Nutzung von Patientendaten, Biomaterialien und Analysemethoden und -routinen im Rahmen der MII; Anhang zum einheitlichen Nutzungsvertrag der MII
B3S	Branchenspezifische Sicherheitsstandards gemäß § 8a BSIG
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (www.bfdi.bund.de)
BGB	Bürgerliches Gesetzbuch
Bloom-Filter	von Burton H. Bloom veröffentlichte Datenstruktur überlagerter Hash-Werte eines Vokabulars zur einfachen und fehlertoleranten Überprüfung des Vorhandenseins einer möglichen Zeichenfolge in dem Vokabular (http://crystal.uta.edu/~mcguigan/cse6350/papers/Bloom.pdf)
BMBF	Bundesministerium für Bildung und Forschung (www.bmbf.de)
BSI	Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de)
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSI-Gesetz
CORD	Collaboration on Rare Diseases; Verbundantrag für einen konsortienübergreifenden Use Case im Rahmen der MII
DataSHIELD	Open-Source-Software zur sicheren, föderativen Auswertung biomedizinischer Daten auf der Basis von R (www.datashield.ac.uk)
DFG	Deutsche Forschungsgemeinschaft (www.dfg.de)
DIFUTURE	Data Integration for Future Medicine (https://difuture.de)
DIZ	Datenintegrationszentrum im Förderkonzept Medizininformatik des BMBF
DS	Datenschutz
DSGVO	Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung (Verordnung 2016/679)
DS-GVO	siehe DSGVO
DSK	Datenschutzkonferenz – Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (www.datenschutzkonferenz-online.de)
DuD	Zeitschrift „Datenschutz und Datensicherheit“ (www.dud.de)
EG	Europäische Gemeinschaft

FDPG	Deutsches Forschungsdatenportal Gesundheit; Zentrale Antrags- und Registerstelle in der MII
FHIR	Fast Healthcare Interoperability Resources; HL7-Standard (http://hl7.org/fhir)
GesR	GesundheitsRecht; Zeitschrift (www.gesr.de)
GKV	Gesetzliche Krankenversicherung
GVO	Grundverordnung
HiGHmed	Heidelberg – Göttingen – Hannover Medical Informatics (www.highmed.org)
HL7	Health Level Seven; Internationale SDO für den Bereich der Interoperabilität von IT-Systemen im Gesundheitswesen (www.hl7.org)
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure HTTP: Protokoll für verschlüsselte und signierte Verbindungen auf Basis von HTTP
ID	Identifikationsnummer
IDAT	Identifizierende Daten (eines Patienten)
IETF	Internet Engineering Task Force (www.ietf.org)
IP	Internet Protocol
ITSG	Gesetz zur Erhöhung informationstechnischer Systeme – IT-Sicherheitsgesetz
KRITIS	Kritische Infrastrukturen gemäß ITSG
LfD	Landesbeauftragte(r) für den Datenschutz
MBO	Musterberufsordnung für Ärzte
MDAT	Medizinische Daten
MFT	Medizinischer Fakultätentag (www.medizinische-fakultäten.de)
MI	Medizininformatik
MII	Medizininformatik-Initiative des BMBF (www.medizininformatik-initiative.de)
MIRACUM	Medizininformatik in Forschung und Versorgung in der Universitätsmedizin | Medical Informatics in Research and Care in University Medicine (www.miracum.org)
MWV	Medizinisch Wissenschaftliche Verlagsgesellschaft OHG, Berlin (www.mwv-berlin.de)
NJW	Neue Juristische Wochenschrift (www.njw.de)
NO	Nutzungsordnung der MII (www.medizininformatik-initiative.de/de/nutzungsordnung)
NRW	Nordrhein-Westfalen
NSG	Nationales Steuerungsgremium der MI-Initiative des BMBF
NV	Nutzungsvertrag der MII (www.medizininformatik-initiative.de/de/nutzungsvertrag)
OAuth2	Open Authorization, Version 2; offenes Autorisierungsprotokoll für verteilte Anwendungen der IETF
OHG	Offene Handelsgesellschaft
OpenID	Open Identification; Authentifizierungsstandard der OpenID-Foundation
ORP	Organisation und Personal; Klasse der BSI-Grundschutzbausteine
PDF	Portable Document Format von Adobe (www.adobe.com)
PLZ	Postleitzahl

POLAR	Polypharmacy – Drug Interactions – Risks; Verbundantrag für einen konsortienübergreifenden Use Case im Rahmen der MII
PPRL	Privacy Preserving Record Linkage
Projectathon	Veranstaltungsformat der MII, in dem die interkonsortiale Zusammenarbeit der Standorte sowie die Realisierung von Projektzielen auf technischer Ebene samt prozessualer und organisatorischer Voraussetzungen erprobt wird
RAID	Redundant Array of Inexpensive / Independent Disks: Einheit aus Controller und mehreren Festplatten für erhöhte Geschwindigkeit und/oder Sicherheit
SAML	Security Assertion Markup Language, XML-basierte Auszeichnungssprache zur Beschreibung von sicherheitsbezogenen Informationen
SDO	Standards Development Organization
SGB	Sozialgesetzbuch
SMITH	Smart Medical Information Technology for Healthcare (www.smith.care)
SMPC	Secure Multi-Party Computation: Auswertung verteilter Daten in einer Weise, dass keine Informationen über die verteilten Daten selbst die datenhaltenden Einrichtungen verlassen und das Ergebnis mit der Auswertung eines ganzheitlichen Datensatzes vergleichbar ist
StGB	Strafgesetzbuch
TF	Taskforce
TK	Telekommunikation
TMF	TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (www.tmf-ev.de)
TR	Technische Richtlinie
UAC	Use & Access Committee
VUD	Verband der Universitätsklinika Deutschlands (www.uniklinika.de)
XML	extensible Markup Language
ZARS	siehe FDPG

9.2 Literaturverzeichnis

1. Roßnagel, A., Kontinuität oder Innovation? Der deutsche Spielraum in der Anpassung des bereichsspezifischen Datenschutzrechts. DuD, 2018. **2018**(8): S. 477–481.
2. Haas, P., Schneider, U.K. *Rahmenbedingungen Cloud-basierter Krankenhausinformationssysteme*. 2021. Health Innovation Hub des Bundesministeriums für Gesundheit, Version 1.3, https://kh-digitalisierung.de/krankenhauszukunftsgesetz/cloud-gutachten/ (Abruf: 2021–02–02).
3. Schneider, U.K., *Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen*. 2015, Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin, https://www.mwv-open.de/site/books/10.32745/9783954663224/ (Abruf: 2020–07–10).
4. Dierks, C., Roßnagel, A., *Sekundärnutzung von Sozial- und Gesundheitsdaten – Rechtliche Rahmenbedingungen*. 2019, MWV, Berlin, https://mwv-open.de/site/books/10.32745/9783954665181/.
5. Cornelius, K., Spitz, M., Auskunfts- und Einsichtnahmerechte von Patienten im digitalisierten Gesundheitswesen. GesR, 2019. **18**(2): S. 69–76.
6. BfDI *Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche*. 2020. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 29.06.2020, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf (Abruf: 2021–06–30).
7. Schantz, P., Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. NJW, 2016. **2016**(26): S. 1841–1904.
8. DSK *Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO*. 2019. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Datenschutzkonferenz (DSK), November 2019, https://www.datenschutzkonferenz-online.de/media/dskb/20191213_erfahrungsbericht_zur_anwendung_der_ds-gvo.pdf (Abruf: 2020–02–27).
9. Ehmann, E., Selmayr, M., Hrsg. *DS-GVO. Datenschutzgrundverordnung. Kommentar*. 2. Aufl. 2018, C.H.Beck, München.
10. Kühling, J., Buchner, B., Hrsg. *Grundverordnung/BDSG. Kommentar*. 2. Aufl. 2018, C.H.Beck, München.
11. Sydow, G., Hrsg. *Europäische Datenschutzgrundverordnung. Handkommentar*. 2. Aufl. 2018, Nomos, Baden-Baden.
12. DSK Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO. 2019. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Datenschutzkonferenz (DSK), 3.4.2019, https://www.datenschutzkonferenz-

online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf (Abruf: 2019–05–21).

13. LfD-Niedersachsen *Schutzstufenkonzept der LfD Niedersachsen*. 2018. Die Landesbeauftragte für den Datenschutz Niedersachsen, Oktober 2018, https://www.lfd.niedersachsen.de/download/137188/Schutzstufenkonzept_LfD_Niedersachsen_.pdf (Abruf: 2019–04–15).
14. Bossert, S., Strech, D., An integrated conceptual framework for evaluating and improving 'understanding' in informed consent. Trials, 2017. **18**(1): S. 482.
15. Pommerening, K., Drepper, J., Helbing, K., Ganslandt, T., *Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF 2.0*. 2014, Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin, https://www.mwv-open.de/site/books/10.32745/9783954662951/ (Abruf: 2020–07–07).

9.3 Formulare zur Bewertung der Datenschutz-Folgenabschätzung

Auf den drei folgenden Seiten finden sich jeweils Formulare für die Bewertung der Datenschutz-Folgenabschätzung durch eine der verantwortlichen Stellen für die Anwendungsszenarien

- Machbarkeitsanfragen,
- verteilte Analysen und
- Daten-Herausgabe.

9.3.1 Bewertung der Datenschutz-Folgenabschätzung für Machbarkeitsanfragen

am Standort:

Tab. 17 Bewertung der Risiken bei Machbarkeitsanfragen

Prüfung durch den Datenschutzbeauftragten:	☐ Erfolgt ☐ nicht erfolgt
Ergebnis der Risikobewertung:	☐ Akzeptabel ☐ ALARP (‚so niedrig, wie vernünftigerweise praktikabel‘) ☐ Inakzeptabel
Wiedervorlage am:	
Sofern Handlungsbedarf besteht, Auflistung der offenen Maßnahmen:	

Ort, Datum: Klicken oder tippen Sie hier, um Text einzugeben.

_____

Unterschrift

Name: Klicken oder tippen Sie hier, um Text einzugeben.

Institution: Klicken oder tippen Sie hier, um Text einzugeben.

9.3.2 Bewertung der Datenschutz-Folgenabschätzung für verteilte Analysen

am Standort:

Tab. 18 Bewertung der Risiken bei verteilten Analysen

Prüfung durch den Datenschutzbeauftragten:	☐ Erfolgt ☐ nicht erfolgt
Ergebnis der Risikobewertung:	☐ Akzeptabel ☐ ALARP (‚so niedrig, wie vernünftigerweise praktikabel‘) ☐ Inakzeptabel
Wiedervorlage am:	
Sofern Handlungsbedarf besteht, Auflistung der offenen Maßnahmen:	

Ort, Datum: Klicken oder tippen Sie hier, um Text einzugeben.

_____

Unterschrift

Name: Klicken oder tippen Sie hier, um Text einzugeben.

Institution: Klicken oder tippen Sie hier, um Text einzugeben.

9.3.3 Bewertung der Datenschutz-Folgenabschätzung für Daten-Herausgaben

am Standort:

Tab. 19 Bewertung der Risiken bei Daten-Herausgaben

Prüfung durch den Datenschutzbeauftragten:	☐ Erfolgt ☐ nicht erfolgt
Ergebnis der Risikobewertung:	☐ Akzeptabel ☐ ALARP (‚so niedrig, wie vernünftigerweise praktikabel‘) ☐ Inakzeptabel
Wiedervorlage am:	
Sofern Handlungsbedarf besteht, Auflistung der offenen Maßnahmen:	

Ort, Datum: Klicken oder tippen Sie hier, um Text einzugeben.

_____

Unterschrift

Name: Klicken oder tippen Sie hier, um Text einzugeben.

Institution: Klicken oder tippen Sie hier, um Text einzugeben.