Nationales Register für Seltene Erkrankungen
NARSE

Datenschutzkonzept mit Datenschutz-Folgenabschätzung[1]

Projekt NARSE (Nationales Register für Seltene Erkrankungen)

Autor/innen Dr. Jessica Vasseur, Jens Göbel
Institut für Medizininformatik
Johann Wolfgang Goethe-Universität Frankfurt am Main

Dr. Franziska Krause
Eva Luise und Horst Köhler Stiftung für Menschen mit Seltenen Erkrankungen und
BIH at Charité | Charité – Universitätsmedizin Berlin

Dr. Josef Schepers
Core Facility Digitale Medizin und Interoperabilität
BIH at Charité | Charité – Universitätsmedizin Berlin
Mitglied der TMF AG Datenschutz

Betreiber[2] Berlin Institute of Health at Charité (BIH)
Charité – Universitätsmedizin Berlin
Anna-Louisa-Karsch-Str. 2,
10178 Berlin

[1] Dieses Konzept basiert auf einer Schablone für OSSE-Datenschutzkonzepte von M. Muscholl, M. Lablans, A. Borg, F. Ückert und TOF Wagner, überarbeitet von J. Vasseur, K. Schüler und J. Göbel (v2.0, Juni 2022).

Es sind in Kapitel 1 „Einleitung“ und in der Anlage in Kapitel 8 „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten“ ergänzende Elemente einer rudimentären Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 Abs. (7) eingefügt worden. Datenschutzkonzept (DSK) und Datenschutz-Folgenabschätzung (DSFA) sollen zukünftig in einem stetigen Datenschutz-Assessment-Prozess in einem Dokument entwickelt und gepflegt werden, um ein Nebeneinander von zwei Dokumenten, die versetzt aufeinander verweisen, zu vermeiden.

[2] Verantwortlicher im Sinne des Art. 4 DSGVO

Änderungshistorie

Versionen DSK/DSFA	Was	Wer	Wann
v0.1	Erster Entwurf	JV, JG, FK	01.08.2022
v0.2	Überarbeitung	JV	02.09.2022
v0.6	Überarbeitung für Einreichung bei DSB	JV	16.09.2022
v0.7	Überarbeitung nach Beratung in TMF AG Datenschutz 23.09.2022	JS, JV	07.10.2022
v0.8	Abstimmungsvariante mit Ergänzung um rudimentäre DSFA	JS	15.10.2022
v0.9/v0.9a	Abstimmungsvariante nach Hinweisen von Klaus Pommerening Ergänzung DSFA-Liste (DSFA im engeren Sinne)	JS	04.11.2022
v0.92/v0.92a	Weitere Abstimmungen	JS	14.11.2022
v0.94/v0.94a	Weitere Abstimmungen und Weiterentwicklung der DSFA	JS, JV, JG	20.11.2022
v0.95/v0.95a	Weitere Abstimmungen und Weiterentwicklung der DSFA	JS, JV, JG	15.01.2023
v0.96/v0.96a	Finalisierung	JS, JV, JG	21.03.2023
v0.99/v0.99a	Nachbesserungen	JS, JV, JG	06.06.2023
v1.0/v0.99a	Nachbesserungen (Hinweise bDSB Charité)	JS, JV, JG	30.06.2023
v1.1/ v0.99a	Redaktionelle Überarbeitungen im DSK, Einfügen von 2.1. Rollen und Berechtigungen, Löschen von vorübergehenden Anhängen	FK	17.10.2023
v1.2/v0.99a	Anpassungen an Nutzungsordnung und Aktualisierung Grafiken	JS, FK	15.01.2024

Inhalt

1. Einleitung

1.1 Zielsetzung des vorliegenden Dokumentes und des stetigen Datenschutz-Assessment-Prozesses

Das Nationale Register für Seltene Erkrankungen (NARSE) soll durch die Verarbeitung von personenbezogenen Daten von Betroffenen einen relevanten Beitrag zum medizinischen Fortschritt leisten. Dabei sind sowohl die Rechte und Freiheiten der betroffenen Personen als auch die Verarbeitung ihrer personenbezogenen Daten in besonderem Maße zu schützen, insbesondere da es sich um Daten einer besonderen Kategorie personenbezogener Daten im Sinne von Art. 9 Absatz (1) Datenschutzgrundverordnung (DSGVO) handelt, die besonders sensibel sind und der ärztlichen Schweigepflicht nach § 203 StGB unterliegen können.

Das vorliegende Dokument umfasst als Initialfassung eines kontinuierlich zu pflegenden „Lebenden Dokumentes" ein klassisches Datenschutzkonzept (DSK) und eine gemäß Art. 35 DSGVO notwendige Datenschutz-Folgenabschätzung[3] (DSFA; engl.: Data Protection Impact Assessment, DPIA) in tabellarischer Form. Die in Art. 35 Absatz (7) geforderten Komponenten einer DSFA sind vorhanden und werden im stetigen Datenschutz-Assessment-Prozess in nachfolgenden Fassungen angepasst:

a) *eine systematische **Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung**, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;*[4]
b) *eine **Bewertung** der Notwendigkeit und Verhältnismäßigkeit **der Verarbeitungsvorgänge** in Bezug auf den Zweck;*
c) *eine **Bewertung der Risiken** für die Rechte und Freiheiten der betroffenen Personen und*
d) *die zur Bewältigung der Risiken geplanten **Abhilfemaßnahmen**, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird."*

Das vorliegende Dokument folgt der Vorstellung im Kurzpapier Nr. 5 der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz), wonach die DSFA als *„ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten*" zu verstehen ist[5]. Ferner wird der Deklaration der Datenschutzkonferenz gefolgt, wonach eine DSFA kein einmaliger Vorgang ist: *„Sollten sich z.B. neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren ergeben, die in der DSFA bisher nicht berücksichtigt wurden, so ist die DSFA zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung empfohlen."*[6]

---

[3] EU Datenschutzgrundverordnung (DSGVO) Art. 35 Absatz (7)

[4] Die DSFA-Tabelle wird mit fortlaufendem Versions-Suffix (a, b, c; …) in der Anlage 8 gepflegt. Änderungen des DSK führen immer zu einer neuen Versionsnummer von DSK (1.0, 1.1, 2.0) und DSFA (1.0a, 1.1a, 2.0a). Änderungen der DSFA kommen ohne und mit Änderungen des DSK infrage (1.0a, 1.0b, 1.0c, 1.1d). Änderungen der DSFA in der Anlage berühren nicht die Gültigkeit des DSK.

[5] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf Das vorliegende Dokument und die vorgesehene stetige und schrittweise Weiterentwicklung des Datenschutzkonzeptes und der Datenschutz-Folgenabschätzung beachten sieben Gewährleistungsziele des Standarddatenschutzmodells der Datenschutzkonferenz des Bundes und Länder und die darin abgebildeten zentralen Datenschutzanforderungen der DSGVO. Die sieben angestrebten Gewährleistungsziele des SDM sind:

(1) Datenminimierung
(2) Verfügbarkeit
(3) Integrität
(4) Vertraulichkeit
(5) Nichtverkettung
(6) Transparenz
(7) Intervenierbarkeit

[6] Überprüfung und Wiederholung des DSFA bei Änderungen fordert Art. 35 Absatz (11): Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

In diesem Sinne befasst sich das vorliegende Datenschutzkonzept mit den Verarbeitungsstrukturen und -prozessen des NARSE. Als Grundlage der technischen Infrastruktur für das Register dient die OSSE-Software (Open Source Registersystem für Seltene Erkrankungen)[7], die auch für andere Register, insbesondere im Bereich der Seltenen Erkrankungen, eingesetzt wird. Die Anfangsphase ist durch zentrale Datenspeicherung in der OSSE-Datenbank des NARSE und die manuelle Datenerfassung über die web-basierte OSSE-Benutzerschnittstelle (OSSE EDC) bestimmt. In einer zweiten Phase kommen indirekte Dateneinspielungen aus NARSE-Satellitendokumentationen (z.B. aus sekundären EDC-Systemen[8] oder Betroffenendokumentationen) und in einem weiteren Schritt die Datenübermittlung aus unabhängigen Datenbeständen, zum Beispiel aus den Datenintegrationszentren der Universitätsklinika, hinzu. Der Datenschutz-Assessment-Prozess wird kontinuierlich fortgeführt und das Datenschutzkonzept (inklusive DSFA), falls notwendig, entsprechend an technische Änderungen und neue Rahmenbedingungen angepasst.

Das vorliegende Datenschutzkonzept für die NARSE-Anfangsphase beruht ab Kapitel 2 auf einer konsentierten Schablone für OSSE-Datenschutzkonzepte und stellt eine zusammenfassende Dokumentation aller datenschutzrechtlichen Aspekte und Maßnahmen zur Einhaltung und Sicherung des Datenschutzes im initialen NARSE dar.

1.2 Zielsetzung & Zweck der Datenverarbeitung im NARSE

Mit Registern werden patientenbezogene Daten systematisch zum Zwecke der wissenschaftlichen Beschreibung und Analyse von Krankheiten, von Erkrankungsgeschehen und/ oder Behandlungsfolgen erfasst. Gerade bei Seltenen Erkrankungen, bei denen die Fallzahlen gering und die Erkenntnisse der Behandelnden durch eigene Beobachtungen limitiert sind, sind Register wichtige Instrumente der Epidemiologie und der Versorgungsforschung. Die wenigen in Deutschland bestehenden Register unterscheiden sich erheblich in ihrer Qualität, Trägerschaft und dem Umfang der erhobenen Datenelemente.

Das Nationale Register für Seltene Erkrankungen (NARSE) hat die Aufgabe, die epidemiologische Transparenz im Bereich der Seltenen Erkrankungen zu erhöhen und Vernetzung, Austausch, Erkenntnisgewinne sowie Zugang zur Versorgung, einschließlich neuer kausaler Therapien, zu verbessern. Besondere Beachtung wird den Patientinnen und Patienten mit ultraseltenen Erkrankungen (Prävalenz <1:50.000) gewidmet. Das NARSE soll unter anderem das Auffinden (Findability) und den Zugang (Accessibility) zu Betroffenendaten, die mit informierter Einwilligung für diesen Zweck bereitgestellt worden sind, organisieren, um so den Betroffenen mit bestimmten Seltenen Erkrankungen den Weg zur Therapie oder zur Teilnahme an klinischen Studien zu bahnen. Mit dem NARSE wird zudem eine wichtige Datengrundlage für wissenschaftliche Auswertungen und die Entwicklung neuer Behandlungsmethoden geschaffen.

Das NARSE wird in mehreren Stufen aufgebaut, die durch eine Evaluation im Rahmen des Innovationsfondsvorhaben FAIR4Rare mit einer Stärken- und Schwächenanalyse (SWOT[9]) begleitet und möglicherweise gestaltet wird. In der ersten Stufe erfolgt die Datenerfassung in die zentrale NARSE-Datenbank im Rahmen der etablierten OSSE-Architektur (siehe unten) über die nicht datenspeichernde, web-basierte OSSE-Benutzerschnittstelle (OSSE EDC). Ab der zweiten Stufe (angestrebt zu Beginn des Jahres 2024) sollen einwilligungsbasiert Daten aus dezentralen, NARSE-konform konfigurierten, datenspeichernden Satelliten in die zentrale Datenbank des NARSE übernommen werden. Dies können lokale Forschungsdatenbanken oder auch Betroffenen-geführte Dokumentationen sein. In der dritten Stufe (angestrebt zum Ende des Jahres 2024) sollen Daten aus Secondary-Use-Repositorien[10] unter Berücksichtigung der dort geltenden Datenschutz-Regelungen in die zentrale Datenbank des NARSE übermittelt werden, insbesondere aus den Datenintegrationszentren der Universitätsklinika. Bei jeder

[7] https://www.osse-register.de/

[8] Systeme des Electronic Data Capture, beispielsweise auf der Basis von REDCap-Tools (www.project-redcap.org)

[9] SWOT-Analyse: dt. Abk. für Analysis of strengths, weaknesses, opportunities and threats; die Stärken-Schwächen-Chancen-Risiken-**Analyse** stellt eine Positionierungsanalyse der eigenen Aktivitäten gegenüber dem Wettbewerb [JS hier: gegenüber alternativen Lösungen] dar. Aus: https://wirtschaftslexikon.gabler.de › definition › swot-analyse-52664. Zuletzt aufgerufen am 31. Oktober 2022

[10] In den Datenintegrationszentren der Universitätsklinika werden patientenbezogene Gesundheits-, Krankheits- und genetische Daten überwiegend aus dem Versorgungskontext und partiell aus dem Forschungskontext des jeweiligen Hauses standardisiert so aufbereitet, dass sie einrichtungsübergreifend gemeinsam genutzt werden können.

inneren und äußeren Änderung des NARSE, also auch bei der Erweiterung der Datenerhebungsvarianten wie der Übernahme von Daten aus anderen Systemen, wird geprüft, ob Anpassungen an DSK und/oder DSFA notwendig sind – zum Beispiel durch genaue Beschreibung der ergänzenden Verarbeitungstätigkeiten, der damit verbundenen Risiken und der als notwendig erachteten Schutzmaßnahmen.

1.3 Rechtsgrundlage

Die informierte Einwilligung der zu erfassenden Person (siehe Abschnitt 6.1 „Aufklärung und Einwilligung“) bildet die Rechtsgrundlage der Datenverarbeitung gemäß Art. 6 Absatz 1 lit. a i.V.m. Art. 9 Absatz 2 lit. a DSGVO. Sie nennt explizit die Institutionen und Personengruppen, die festgelegte Datenarten erheben, verarbeiten und nutzen dürfen. Auch die Weitergabe von anonymisierten oder pseudonymisierten Daten zu Forschungszwecken wird in der Einwilligung berücksichtigt, da speziell im Bereich der Seltenen Erkrankungen nicht ausgeschlossen werden kann, dass durch die Krankheitsdaten Rückschlüsse auf die Identität des/der Betroffenen gezogen werden können.

Die Datenübernahme aus anderen Repositorien wird in der Regel auf einer nachgeholten informierten Einwilligung zur Übermittlung in das und zur Nutzung im NARSE beruhen.

1.4 Überblick über die Datenverarbeitung

Im NARSE werden Daten von Betroffenen, die in den teilnehmenden Kliniken, Zentren, Praxen oder Patientenorganisationen (auch als „Standorte“ bezeichnet) behandelt werden, erhoben, verarbeitet und genutzt. Darunter fallen auch minderjährige Personen oder Personen miteingeschränkter Willensbildung; dies wird in Bezug auf die informierte Einwilligung berücksichtigt (siehe Abschnitt 6.1 „Aufklärung und Einwilligung“).

Die Daten werden auf folgende Weise im Register erfasst:

- ☐ zunächst nur manuell über die web-basierte OSSE-Benutzerschnittstelle (OSSE EDC)

Folgende Arten von Daten werden unter Beachtung des Grundsatzes der Datensparsamkeit und Datenminimierung gemäß Art. 5 der DSGVO erhoben:

- ☐ Identifizierende Daten (IDAT): Sie enthalten Daten (z.B. Name, Geburtsdatum und -ort, Kontaktdaten), die eine eindeutige Identifikation einer Person erlauben. Sie werden nicht im Register, sondern separat in einem Pseudonymisierungs- und Identitätsmanagement, einer Instanz der Mainzelliste[11], gespeichert und verwaltet, zu dessen nicht-weisungsgebundener Umsetzung vor dem Einschluss des ersten Patienten die Unabhängige Treuhandstelle der TU Dresden beauftragt worden ist.
- ☐ Medizinische Daten (MDAT): Dazu gehören routinemäßig erhobene Daten (genetische und Gesundheitsdaten), die über die Erkrankung und deren Verlauf im Register erfasst werden. Hierbei handelt es sich um besonders schützenswerte Daten. Es werden keine weiteren Datenarten (z.B. bildgebende Daten, biometrische Daten) erfasst und gespeichert.

Genauere Informationen zum Umfang der Daten finden sich im Anhang unter 8.2 „Datensätze“.

Alle Datenfelder, die im Register erfasst werden, sind in einem für alle OSSE-Register zentral betriebenen Metadaten-Repository (MDR) registriert und definiert. Die Registerstruktur (Formulare zur Erfassung von Basis- und Verlaufsdaten) wird mithilfe eines Formulareditors dynamisch festgelegt und zentral gespeichert (siehe Anhang 8.2 „Datensätze“).

Daten im NARSE werden zu Auswertungszwecken je nach Erforderlichkeit mit nicht-rückführbaren Exportpseudonymen oder mit den im Register verwendeten Pseudonymen exportiert (siehe Abschnitt 4.6 „Datenexport“).

Eine detaillierte Beschreibung der Komponenten und Prozesse wird in den Abschnitten 3. und 4. gegeben.

[11] https://www.unimedizin-mainz.de/imbei/informatik/ag-verbundforschung/mainzelliste.html

1.5 Bewertung der Zweckmäßigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

Hier wird die in Art. 35 Absatz (7) Buchstabe b) geforderte *„Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck“* vorgenommen:

Es existieren nur Schätzungen, wie viele Menschen mit Seltenen Erkrankungen in Deutschland leben. Es wird von einer Zahl in der Größenordnung von 4 Millionen Personen ausgegangen. Es wird ein Spektrum von 6.000 bis 10.000 verschiedenen Krankheiten angenommen, bei denen das Spektrum der Zahl der Betroffenen von mehreren zehntausend bis hinunter zu wenigen Einzelpersonen reicht. Es gibt im deutschen Gesundheitssystems mit vielen Tausenden Leistungserbringern und vielen Dutzend Leistungsfinanzieren, die jeweils getrennte Datensilos führen, keine epidemiologische Übersicht.

Für den Zweck der epidemiologischen Übersicht über die Inzidenz und Prävalenz Seltener Erkrankungen ist es notwendig und verhältnismäßig, ein nationales Register aufzubauen, das, unter anderem, von allen Zentren für Seltene Erkrankungen unterstützt wird.

Oft vergehen Jahre, bis Menschen mit Seltenen Erkrankungen eine Diagnose und eine Therapie erhalten. Letzteres gilt auch, wenn eine Diagnose bestimmt werden konnte, aber Informationen über veränderte Behandlungsoptionen, beispielsweise über neue kausale Therapien oder neue Enzymersatztherapien, die Betroffenen nicht erreichen. Beim Versuch der Rekrutierung von Patientinnen und Patienten für klinische Studien für Diagnostik und Therapien wird regelmäßig die für eine statistisch gesicherte Aussagekraft (Power, Evidenz) notwendige Probandenzahl nicht erreicht.

Für den Zweck der Kommunikation von Diagnostik- und Therapieoptionen (einschließlich der Einladung zu klinischen Studien), ist es notwendig und verhältnismäßig, Betroffenen, potentiell Betroffenen, ihren Eltern und/ oder Betreuern die Möglichkeit anzubieten, sich in ein nationales Register einzutragen oder eintragen zu lassen, das als Grundlage dafür dient, die Behandelnden, die Behandelbaren und deren Eltern oder Betreuer spezifisch über konkrete Entwicklungen von Diagnostik- und Therapieoptionen zu informieren.

1.6 Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen

Hier wird die in Art. 35 Absatz (7) Buchstabe c) geforderte *„Bewertung der Risiken für die Rechte und Freiheiten der betroffenen* Personen“ vorgenommen, deren Daten gemäß Art. 35 Absatz (1) der DSGVO in einer Weise verarbeitet werden, in der ohne Schutzmaßnahmen voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen entsteht:

Im NARSE werden personenbezogen sensible Gesundheits-, Erkrankungs- und genetische Daten im Sinne des Art. 9 der DSGVO gespeichert und verarbeitet. Bei nicht-erlaubtem individuellem Bekanntwerden einzelner Angaben können den Personen soziale und wirtschaftliche Schäden entstehen. Das Recht auf informationelle Selbstbestimmung würde verletzt. Freiheitsgrade des persönlichen Handelns wären bedroht.

Gemäß Art. 6 der DSGVO ist die Verarbeitung dieser Daten untersagt, wenn das Verbot nicht durch eine gehaltvolle Erlaubnis aufgehoben wird. Beim NARSE erfolgt durch die dokumentierte, informierte Einwilligung die Erlaubnis der Verarbeitung durch einen definierten Personenkreis und für definierte Zwecke.

Technische und organisatorische Schutzmaßnahmen (auch Abhilfemaßnahmen genannt), die in den Kapiteln 2 bis 6 des vorliegenden Datenschutzkonzepts näher beschrieben sind, stellen sicher,

- dass die Verarbeitung nur durch den berechtigten Personenkreis erfolgt,
- dass die Verarbeitung nur zu den erlaubten Zwecken erfolgt,
- dass die sensiblen Angaben keinen unberechtigten Personen bekannt werden.

Unter Einhaltung dieser Bedingungen dürfen die Risiken für die Rechte und Freiheiten der betroffenen Personen beim angestrebten Betrieb des NARSE als im geforderten und notwendigen Maß reduziert gelten. Diese Einschätzung wird mit den zuständigen Behördlichen Beauftragten für Datenschutz und Informationsfreiheit per Antrag auf Stellungnahme abgestimmt. Monita werden in einem kontinuierlichen Datenschutz-Assessment-Prozess aufgearbeitet.

2. Organisatorische Rahmenbedingungen laut Nutzungsordnung

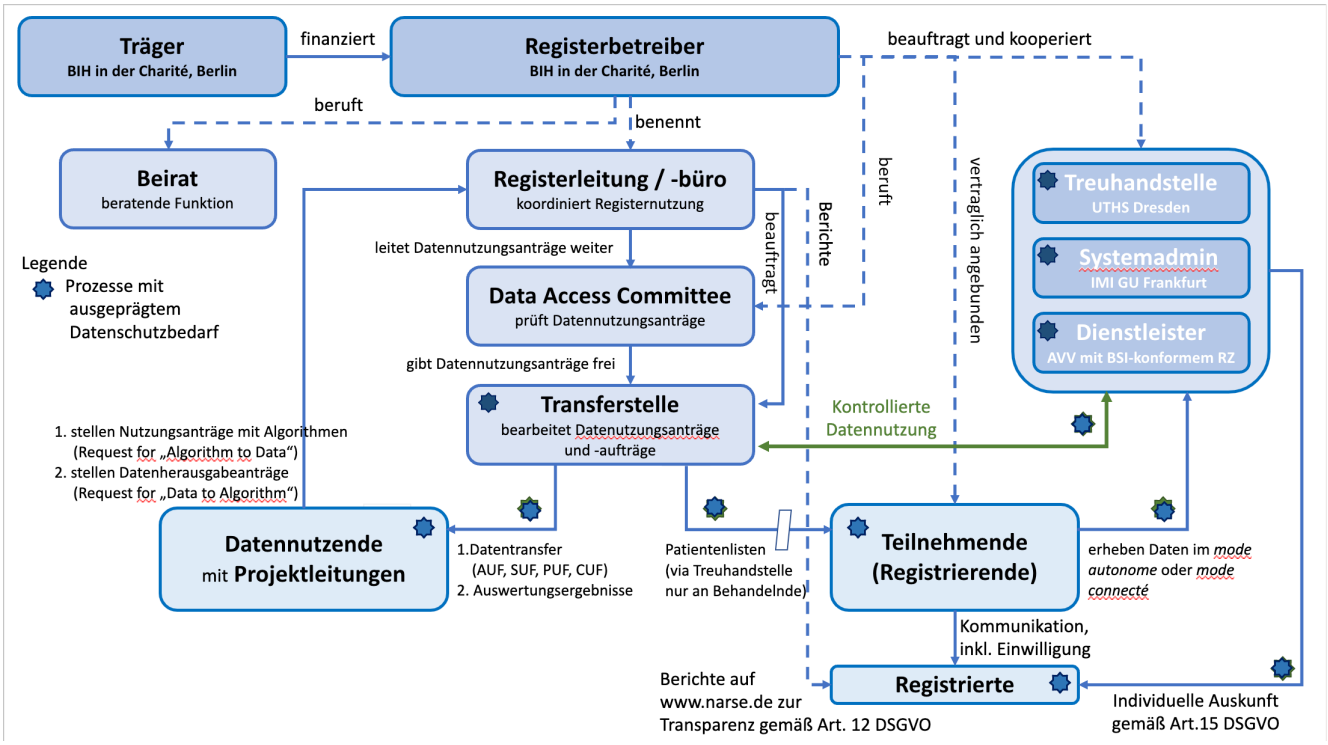


Abb.1 Organisationsstruktur des NARSE

2.1 Träger und Registerbetreiber, verantwortlich im Sinne des Art. 4 DSGVO

Aktueller Träger des Vorhabens und Registerbetreiber, und damit Verantwortlicher im Sinne des Art. 4 DSGVO, ist das Berlin Institute of Health (BIH) der Charité – Universitätsmedizin Berlin als Körperschaft des öffentlichen Rechts.

Berlin Institute of Health at Charité (BIH)
Charité – Universitätsmedizin Berlin
Anna-Louisa-Karsch-Str. 2
10178 Berlin

Registrierte und Teilnehmende werden über einen möglichen Wechsel der Trägerschaft rechtzeitig informiert und können in diesem Fall ihre Einwilligung in die Verarbeitung ihrer Daten im NARSE widerrufen (siehe 7.4 „Widerruf, Löschung, De-Identifizierung“).[12]

Vor dem Ende der zugesagten Finanzierung bis 2025 wird der Betreiber (BIH/Charité) sich rechtzeitig um Findung von Möglichkeiten zur Weiterführung und einer Verstetigung des NARSE bemühen.

[12] Der Träger BIH hat für den Zeitraum bis zum Ende des Jahres 2025 einen Haushaltsplan für den Betrieb des NARSE erstellt. Dieser wird jeweils zwei Jahre vor Ablauf um ein Jahr verlängert. Wenn eine Verlängerung nicht finanziert werden kann, wenn die Notwendigkeit zur Beendigung des Registerbetriebes festgestellt wird oder wenn vom Vorstand des BIH ein qualifizierter Wechsel der Trägerschaft eingeleitet wird, werden alle Betroffenen rechtzeitig informiert.

Die Betroffenen können wählen, ob in diesem Fall ihre (Identitäts)-Daten im Register gelöscht werden oder an den neuen qualifizierten Träger übergeben werden. Daten von Personen, die die Wahlmöglichkeit nicht wahrnehmen, werden entsprechend der erteilten Einwilligung behandelt. Das Recht auf Datenauskunft und der Bereitstellung einer Kopie der vorhandenen Daten bleiben davon unberührt.

2.2 Beirat

Die Weiterentwicklung des NARSE in den skizzierten Entwicklungsstufen erfolgt durch einen wissenschaftlichen Beirat, der sich aus Vertreter/innen des Registerbetreibers, Vertreter/innen des Think Tanks der Eva Luise und Horst Köhler Stiftung für Menschen mit Seltenen Erkrankungen sowie Projektpartnern aus dem begleitenden Evaluationsprojekt FAIR4Rare zusammensetzt. Die Mitglieder des Beirats werden vom Registerbetreiber berufen.

2.3 Registerleitung und Registerbüro

Die Registerleitung wird vom Registerbetreiber berufen. Zusammen mit dem Registerbüro wird der Registerbetrieb organisiert, einschließlich der Kommunikation mit dem Data Access Committee, der Transferstelle und der Benutzerverwaltung.
Als Registerleitung wurde am 17.11.2023 berufen:

Josef Schepers, Dr. med. Dipl.-Vw.
BIH at Charité | Charité – Universitätsmedizin Berlin
Stv. Leiter BIH Core Facility Digitale Medizin & Interoperabilität (CEI)
Anna-Louisa-Karsch-Str. 2
10178 Berlin

2.4 Registrierte

Registrierte sind Betroffene von einer Seltenen Erkrankungen, deren Daten einwilligungsbasiert durch Registrierende im NARSE erfasst werden.

2.5 Teilnehmende (Registrierende)

Eine aktuelle Liste der am NARSE beteiligten Kliniken, Zentren und Patientenorganisationen ist (Registerstandorte) unter www.narse.de zu finden. Generell können alle Mitglieder der Registerstandorte als Registrierende das NARSE nutzen, wobei jeder Standort selbst entscheidet, welche seiner Mitglieder eine Zugangsberechtigung erhalten sollen.

2.6 Datennutzende mit Projektleitungen

Datennutzende sind natürliche oder juristische Personen, die an einem Nutzungsprojekt beteiligt sind und durch den rechtswirksamen Abschluss eines Nutzungsvertrags Vertragspartei zum NARSE werden (z.B. eine Universitätskörperschaft als rechtsfähiger Träger eines rechtlich unselbständigen Instituts oder einer anderen unselbständigen wissenschaftlichen Einrichtung). Datennutzende stellen an den Registerbetreiber entweder einen Antrag im Sinne von „Data to Algorithm“ (Herausgabe von Daten mit verschiedenen „Five-Safe“-Sicherheitsstufen) oder einen Antrag im Sinne von „Algorithm to Data“ (Kontrollierte Datenfernverarbeitung und Gastwissenschaftlerarbeitsplätze“). Im Rahmen der Datenbereitstellung über die Transferstelle werden die Registerdaten auf der Basis von Nutzungsverträgen für die Forschenden / Datennutzenden aus den verschiedenen Quellen zusammengestellt, deren Qualität überprüft und aufbereitet (z.B. pseudonymisiert, anonymisiert) und den Personen für Forschungszwecke zur Verfügung gestellt.

2.7 Treuhandstelle

Die unabhängige Treuhandstelle des NARSE übernimmt die Verwaltung der personenidentifizierenden Daten (IDAT) des NARSE, die Erzeugung und Verwaltung von Pseudonymen für verschiedene Zwecke sowie das zentrale digitale Einwilligungsmanagement. Die Treuhandstelle ist organisatorisch unabhängig vom Registerbetreiber und hat keinen Zugriff auf die im NARSE erfassten medizinischen Daten (MDAT).

Unabhängige Treuhandstelle Dresden
Bereich Medizin der

Technischen Universität Dresden
Fetscherstraße 74
01307 Dresden

2.8 Systemadministration

Die Systemadministration des NARSE ist für die die Bereitstellung und Wartung der verwendeten Registersoftware sowie die technische Speicherung und Verarbeitung der medizinischen im NARSE zuständig. Sie verwaltet außerdem die Metadaten aller Datenelemente oder Variablen des NARSE in Form eines Data Dictionaries, unterstützt die Transferstelle bei der Bereitstellung medizinischer Daten aus dem NARSE und den Registerbetreiber bei der Umsetzung der Betroffenenrechte (Löschung medizinsicher Daten im Rahmen eines Widerrufs, Auskunft über gespeicherte Daten).

Die im NARSE gespeicherten Daten können prinzipiell von den Administratoren/Administratorinnen der verwendeten IT-Infrastruktur eingesehen werden. Zugriffe auf die Daten durch Administratoren/Administratorinnen dürfen nur erfolgen, wenn dies zur Erfüllung ihrer Aufgaben zwingend erforderlich ist. Dies kann bei den folgenden Tätigkeiten der Fall sein:

- Systemkonfiguration und Systemwartung (z.B. Updates des Betriebssystems oder der Software)
- Manuelle Änderungen in der Datenbank (z.B. Standortzugehörigkeit einer im Register erfassten Person)
- Unterstützung beim Datenexport
- Unterstützende Dienstleistung zur Erfüllung der Betroffenenrechte im Auftrag des Verantwortlichen

Das Vorgehen beim Datenzugriff ist durch folgenden Prozess geregelt:

- Vor dem Zugriff wird geklärt, ob der Datenzugriff tatsächlich notwendig ist.
- Der Datenzugriff wird protokolliert. Das Protokoll umfasst dabei mindestens die folgenden Inhalte:
  - den Zeitpunkt des Datenzugriffs,
  - die beteiligten Administratoren/Administratorinnen,
  - den Grund des Datenzugriffs,
  - die involvierten Nutzdaten (nach Möglichkeiten anonymisiert oder pseudonymisiert).

Alle Administratoren/Administratorinnen sind entsprechend zu instruieren und zur Verschwiegenheit zu verpflichten[13].

Institut für Medizininformatik (IMI)
Goethe-Universität Frankfurt
Universitätsklinikum Frankfurt
Theodor-Stern-Kai 7
60590 Frankfurt am Main

2.9 Data Access Committee

Der Registerbetreiber benennt in Absprache mit dem Beirat ein Data Access Committee (DAC). Zu den Mitgliedern des Data Access Committee zählen medizinische Expert/innen, z.B. Vertreter/innen aus wissenschaftlichem und klinischem Fachpersonal der Teilnehmer des NARSE, Vertreter/innen von Patientenorganisationen oder der ACHSE, aber auch Vertreter/innen anderer Fachbereiche, insbesondere Datenschutz, Epidemiologie oder Medizinethik.

Dieses Data Access Committe (DAC) ist für die Prüfung und Bewilligung von Datennutzungsanträgen auf Export medizinischer Daten für interne und externe Forschungsprojekte verantwortlich.

Innerhalb des ersten halben Jahres wird vom NARSE-Betreiber eine Satzung und eine Nutzungsordnung verfasst und mit den Gremien des NARSE abgestimmt. Diese werden unter anderem regeln:

- Wer nutzungsberechtigt sein wird.
- Wie das Antrags- und Genehmigungsverfahren aussehen wird.

[13] Dies sollte in der Regel im Rahmen des Arbeitsverhältnisses an der zuständigen Institution ohnehin geschehen sein.

- Welche Kriterien ein Datennutzungsantrag erfüllen muss.
- In welcher Weise Behandelnde die Registerdaten für eigene Forschungszwecke nutzen können.
- Ob Informationen aus dem Register zur direkten Beeinflussung von Behandlung genutzt werden dürfen (z. B. durch die Suche nach ähnlichen Fällen).
- Wie der Verweis auf Bilddaten und Proben gehandhabt wird (kurz- und langfristig).
- Wie die Daten zu verschiedenen Erkrankungen voneinander abgegrenzt werden sollen.
- Wie die Kooperation mit vorhandenen Registern zu einzelnen seltenen Erkrankungen organisiert wird.

2.10 Transferstelle

Die Transferstelle übernimmt und koordiniert den gesamten Prozess der Bereitstellung von Daten aus dem NARSE für wissenschaftliche Auswertungen. Ferner gehört zu ihren Aufgaben die Überwachung von Fristen für Sachstands- und Abschlussberichte, für die Löschung übergebener Daten und für das An Bordholen und die Speicherung der Publikationen mit Beteilung des NARSE.

2.11 IT-Dienstleister (BSI-konformes Rechenzentrum)

Ein technischer Dienstleister ist ein externes, den Anforderungen des Bundesamts für die Sicherheit in der Informationstechnik (BSI) entsprechendes Rechenzentrum für das Hosting der Registersoftware und Registerdatenbank. Die datenschutzkonforme Datenverarbeitung wird durch Abschluss eines Auftragsverarbeitungs-Vertrags gewährleistet.

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Deutschland

3. Datenverarbeitende Komponenten

3.1 OSSE-Registersystem

Komponenten und Funktionen

Die OSSE-Software (Abbildung 2) dient der Erfassung und Speicherung medizinischer Basis- und Verlaufsdaten von betroffenen Personen. Datenfelder und Formulare sind zentral in einem Metadaten-Repository (MDR) bzw. Formulareditor registriert und beschrieben und können auch nach Start des laufenden Vorhabens modifiziert und ergänzt werden.

Die Eingabe der Daten erfolgt an den Standorten über die webbasierte Benutzerschnittstelle des OSSE EDC; zusätzlich können Daten aus externen Quellen über Schnittstellen für den Datenimport erfasst werden. Alle medizinischen Daten werden versioniert in der Datenbank des OSSE EDC gespeichert; über die Benutzeroberfläche geänderte und gelöschte Werte bleiben in der Datenbank erhalten und können bei Bedarf abgerufen werden.

Personenbezogene IDAT werden nicht im OSSE EDC, sondern direkt im für das Pseudonymisierungs- und Identitätsmanagement verantwortlichen Treuhandmodul „Mainzelliste“ der Unabhängigen Treuhandstelle der TU Dresden (UTHS Dresden) erfasst. Die Kommunikation zwischen dem Treuhandmodul in der UTHS und dem OSSE-Register findet auf eine Weise statt, die keine IDAT an das Register überträgt. Für den/die Benutzer/in erscheint die Eingabemaske der „Mainzelliste“ integriert in die webbasierte Benutzeroberfläche des OSSE EDC. Das zurückgelieferte Pseudonym, „PSN_{OSSE}“ (siehe Abschnitt 3.2 „Pseudonymisierungs- und Identitätsmanagement“), wird mit den MDAT gespeichert, aber nicht angezeigt, sodass auch manuell keine Zuordnung der IDAT mit dem PSN_{OSSE} außerhalb des Pseudonymisierungs- und Identitätsmanagements möglich ist. Da MDAT behandlungsnah lokal erfasst werden, können IDAT und MDAT aber im Browser zusammen angezeigt werden. Dies geschieht mithilfe temporärer Identifikatoren, über die der Browser z.B. Name und Vorname der erfassten Person abruft

und die sicherstellen, dass die Zuordnung zwischen dem PSN_{OSSE} und den IDAT der betroffenen Person außerhalb des Pseudonymisierungs- und Identitätsmanagements nicht bekannt wird.

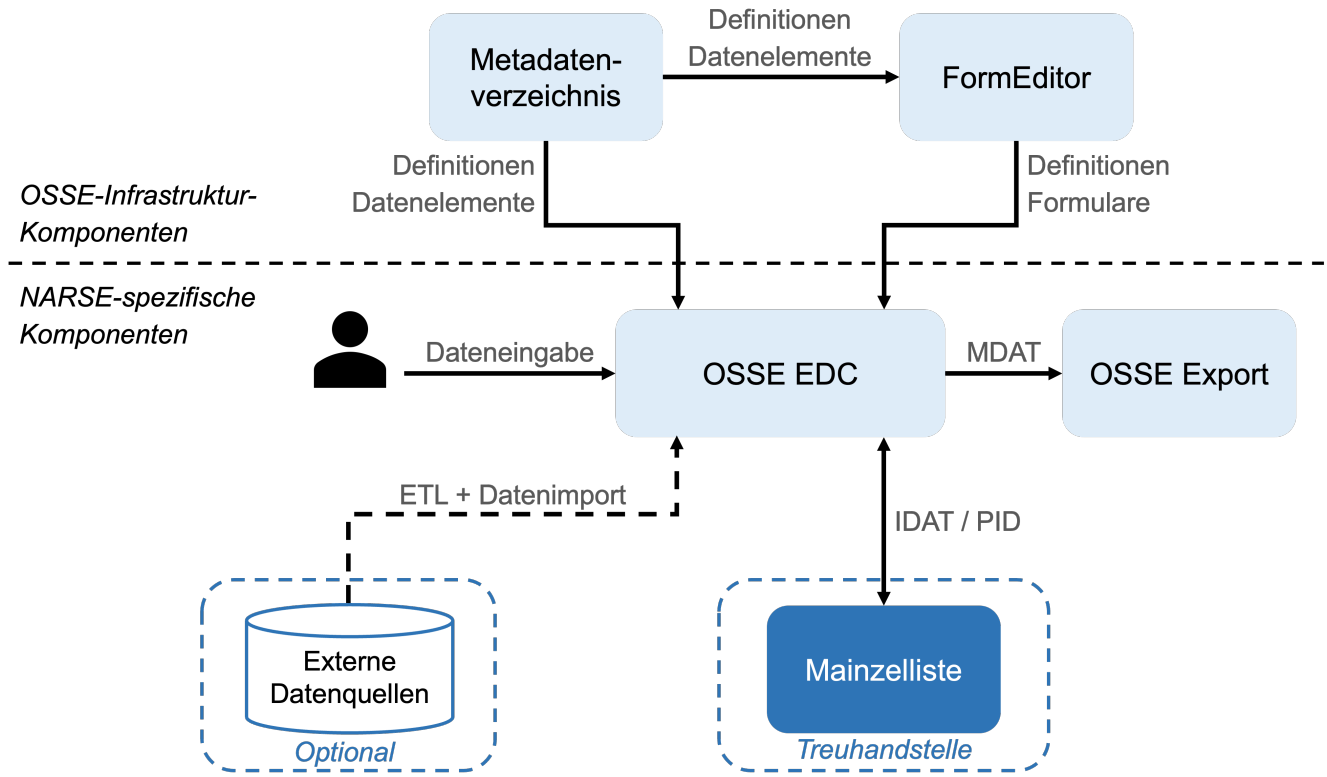


Abbildung 2: Aufbau des OSSE-Systems

 # „Trusted Third Party" = Unabhängige Treuhandstelle der TU Dresden"

Betrieb der Komponenten

Der Betrieb des OSSE-Registers erfolgt initial in der Verantwortung des Berlin Institute of Health (BIH) der Charité – Universitätsmedizin Berlin.

Die OSSE-Komponente wird auf einem angemieteten Server eines Anbieters für BSI-zertifizierte Rechenzentrumsleistungen realisiert. Mit dem Anbieter wird vom Betreiber des NARSE ein Vertrag zur Auftragsverarbeitung abgeschlossen. Der Vertragspartner des Betreibers für Rechenzentrumsleistungen wird auf der Website www.narse.de bekannt gegeben.

Für die Systemadministration der IT-Infrastruktur der OSSE-Komponenten und den technische Support wird mit einer anderen Einrichtung ein Vertrag zur Auftragsverarbeitung geschlossen. Initialer Vertragspartner ist das Institut für Medizininformatik (IMI) der Goethe-Universität Frankfurt. Der Vertragspartner des Betreibers für Systemadministration der IT-Infrastruktur der OSSE-Komponente und den technische Support wird auf der Website www.narse.de bekannt gegeben.

Der Betrieb des Pseudonymisierungsdienstes Mainzelliste (https://www.toolpool-gesundheitsforschung.de/produkte/mainzelliste) sowie des Identitäts- und Einwilligungsmanagements wird an die Unabhängige Treuhandstelle der TU Dresden überantwortet.

Workflow

MDAT werden in Formularen (Basis- und Verlaufsdatenformulare) erfasst, die im Bearbeitungsablauf folgende Statuswerte annehmen können:

- Unused: Das Formular wurde noch nicht von einem/r Benutzer/in geöffnet oder bearbeitet.
- Open: MDAT wurden in das Formular eingegeben und gespeichert.

- Reported: Die Dateneingabe ist vorerst beendet und die im Formular erfassten MDAT sind zur Sichtung und Kontrolle freigegeben (über die notwendige OSSE-Berechtigung „DataReport"). Änderungen sind temporär in diesem Status nicht möglich; über die OSSE-Berechtigung „DataValidation" kann der Status in „Open" oder „Validated" geändert werden.
- Validated: Die im Formular erfassten MDAT wurden validiert (über die notwendige OSSE-Berechtigung „DataValidation"). Eine nachträgliche Änderung ist nur mit erweiterten Zugriffsrechten möglich (OSSE-Berechtigung „RemoveValidation").

Zugänge, Rollen und Rechte

Zugriffsberechtigungen werden rollenbasiert durch einen Administrator / eine Administratorin des OSSE-Registers vergeben, damit jede Person nur die ihr zugeordneten und für sie relevanten Daten einsehen kann (siehe auch Abschnitt 6.2 „Autorisierung und Authentifizierung"). Jede/r Nutzer/in besitzt entsprechend ihrer/seiner Funktion eine oder mehrere Rollen, mit denen die Anmeldung erfolgt. Für die Definition der Zugriffsrechte werden Daten insbesondere nach ihrer Zuordnung zum datenerhebenden Standort und nach den beteiligten Berufsgruppen bzw. Funktionen klassifiziert. Eine detaillierte Liste der Rollen im NARSE und ihrer Beschreibung sowie der zugeordneten Berechtigungen findet sich im Anhang 8.3 „Rollen und Berechtigungen".

3.2 Pseudonymisierungs- und Identitätsmanagement

Pseudonymisierung ist ein zur Aufrechterhaltung eines hohen Datenschutzniveaus notwendiger Schritt, um eine im Register erfasste Person vor Rückidentifizierung zu schützen. Anstelle ihrer IDAT treten Pseudonyme. Bei der Anforderung eines Pseudonyms wird der Datensatz auf Übereinstimmung mit schon vorhandenen Datensätzen überprüft (Record Linkage). Je nach Grad der Übereinstimmung der IDAT und nach den eingestellten Schwellwerten, wird ein neuer Datensatz erzeugt oder ein vorhandener zurückgeliefert.

Pseudonyme

Für die Pseudonymisierung (siehe Abschnitt 3.2 „Pseudonymisierungs- und Identitätsmanagement") im NARSE wird eine Instanz der „Mainzelliste" genutzt, die von der beauftragten Unabhängigen Treuhandstelle der TU Dresden betrieben wird. Sie erzeugt für jede Person im Register einen eindeutigen Identifikator (PID) und ein Pseudonym zweiter Stufe (PSN_{OSSE}). Die Mainzelliste kann außerdem nicht-rückführbare Exportpseudonyme für den Export von Registerdaten zu Forschungszwecken erzeugen.

Manuelles Linken

Eine Schnittstelle der Mainzelliste erlaubt einem Administrator / einer Administratorin der Treuhandstelle, Ergebnisse des automatischen Matching manuell zu überprüfen und ggf. zu korrigieren, d.h. Duplikate zusammenzuführen oder fälschlicherweise zusammengeführte Datensätze zu trennen. Hierfür werden die Matchgewichte (Vergleichswerte zwischen den einzelnen Attributen von zu prüfenden Personen) angezeigt. Zur Entscheidungsfindung bei unklaren Fällen können in einem protokollierten Prozess auch MDAT hinzugezogen werden. Der/die Administrator/in der Mainzelliste teilt einem/r Verantwortlichen des Registerbetreibers die betroffenen Pseudonyme mit; seitens des Registerbetreibers werden die zugehörigen MDAT auf Übereinstimmung geprüft und der Treuhandstelle mitgeteilt, ob es sich mit hoher Wahrscheinlichkeit um dieselbe Person handelt oder nicht.

3.3 Metadaten-Repository

Das Metadaten-Repository (MDR) speichert die Bedeutung (Semantik) sämtlicher im NARSE verwendeten Datenelemente. Es bietet ein kontrolliertes Vokabular (Syntax) und kann maschinenlesbare, strukturierte Aussagen über Datenelemente treffen, beispielsweise konzeptuelle Domänen oder Wertebereiche. Hier sind auch die Felder der in diesem Konzept genannten Registerformulare (siehe Anhang 8.2 „Datensätze") definiert. Da das MDR keine personenbezogenen Daten verarbeitet, wird innerhalb dieses Datenschutzkonzepts nicht weiter darauf eingegangen.

3.4 Registerverzeichnis (Registry of Registries)

In einem Registerverzeichnis kann der Registerbetreiber das NARSE mit einer Kurzbeschreibung des Registers, den Ansprechpartnern und ggf. zusätzlich Metadaten und aggregierten Kerndaten registrieren. Die Daten werden von den Verantwortlichen aktiv hochgeladen. Es werden keine Patientendaten übertragen.

4. Datenverarbeitende Prozesse

4.1 Manuelle Dateneingabe

Anlegen einer Person im Register

Eine berechtigte dateneingebende Person legt eine zu erfassende Person im Register an, indem sie die IDAT der Person in die in die Benutzeroberfläche des OSSE EDC integrierte Maske der Mainzelliste eingibt.

Das OSSE EDC erhält ein Pseudonym (siehe Abschnitt 3.2 „Pseudonymisierungs- und Identitätsmanagement“), das mit dem Datensatz gespeichert wird. Dabei erhält die dateneingebende Person keine Rückmeldung, ob die zu erfassende Person in der Mainzelliste bereits vorhanden war oder neu angelegt wurde.

Auswahl einer Person im Register, Dateneingabe

Die dateneingebende Person erhält eine Liste der im Register erfassten Personen entsprechend der eigenen Berechtigungen (Sichtbarkeit von IDAT, Sichtbarkeit von erfassten Personen anderer Standorte). Nach Auswahl einer erfassten Person können deren Formulare bearbeitet werden; bei Vorliegen der entsprechenden Berechtigung werden im Browser die zugehörigen IDAT angezeigt.

Patient-reported Outcomes (PROs)

Einzelne Formulare können als PRO gekennzeichnet und durch die erfasste Person über einen durch den behandelnden Arzt / die behandelnde Ärztin oder eine andere berechtigte Person erstellten Zugang selbständig ausgefüllt werden.

4.2 Datenimport

Daten aus vorhandenen Datenverarbeitungssystemen oder Datensammlungen, z.B. aus Datenintegrationszentren (DIZ) oder anderen EDC-Systemen, können in das NARSE übernommen werden. Die Datenübernahme durchläuft folgende Schritte eines sogenannten ETL-Prozesses[14], wobei sich die Daten bis zum Import in das OSSE-Register immer auf den lokalen Systemen am jeweiligen Standort befinden:

1) IDAT und MDAT werden aus den Quellsystemen extrahiert.
2) IDAT werden im Rahmen der Transformation an das durch die Unabhängige Treuhandstelle der TU Dresden betriebene Pseudonymisierungs- und Identitätsmanagement übergeben und durch ein Pseudonym ersetzt.
3) Der ETL-Prozess lädt die pseudonymisierten MDAT über eine Webschnittstelle in das OSSE-Register.

4.3 Pseudonymisierung

Pseudonymisierung findet bei jeder Art von Datenerfassung in das OSSE-Register statt, sowohl bei der manuellen Dateneingabe als auch dem Datenimport.

[14] ETL steht für „Extract-Transform-Load“ und meint den technischen und inhaltlichen Transfer von Daten aus einem Quell-System in ein Ziel-System, wobei spezifische Anpassungen an den Daten (Zuweisung zu Datenfeldern, Formatänderungen, Übersetzung von Werten etc.) vorgenommen werden können.

Manuelle Patientenregistrierung

Gleichermaßen für die Registrierung eines neuen Patientendatensatzes wie auch für das Wiederfinden eines vorhandenen Datensatzes geben Nutzer/innen die IDAT in eine Eingabemaske der Mainzelliste ein, die im Browserfenster der OSSE-Benutzeroberfläche angezeigt wird. Die IDAT müssen vollständig eingegeben werden, da hier nicht, wie beispielsweise in einem klinischen Arbeitsplatzsystem, Auswahllisten nach Eingabe von Namensteilen angezeigt werden können. Ein Record-Linkage-Algorithmus prüft, ob die Person bereits in der Mainzelliste registriert ist. Falls nicht, so wird ein neuer Datensatz angelegt, indem die IDAT gespeichert und ein nicht-sprechender PID sowie das PSN_{OSSE} als Pseudonym zweiter Stufe erzeugt werden. Der/die Benutzer/in wird automatisch zur Patientenliste des OSSE-Registers zurückgeleitet, in das die MDAT zur neu angelegten oder ausgewählten Person eingegeben werden können. Browser und OSSE-Register kommunizieren dabei mittels temporärer Identifikatoren. Das PSN_{OSSE} wird für den Benutzer nicht sichtbar, d.h. es erscheint auch nicht im HTML-Code der angezeigten Formulare oder in HTTP-Anfragen des Webbrowsers. Mit diesem Verfahren ist sichergestellt, dass PSN_{OSSE} und IDAT zu keinem Zeitpunkt außerhalb der Mainzelliste einander zugeordnet werden können.

Während der Eingabe der MDAT im OSSE-Register, die lokal und behandlungsnah erfolgt, werden die IDAT der erfassten Person im Browser angezeigt, vorausgesetzt der/die Nutzer/in hat die entsprechende Berechtigung, IDAT zu sehen. Diese werden allerdings erst im Browser mit den MDAT zusammengeführt, sodass das OSSE-Register zu keinem Zeitpunkt Zugriff auf IDAT bekommt. Dazu ruft die Registersoftware für jedes PSN_{OSSE} bei der Mainzelliste eine sessionbasierte temporäre ID (Token) ab, mit der der Browser die zugehörigen IDAT von der Mainzelliste erhält (Abbildung 3).

Die im OSSE-Register gespeicherten Pseudonyme werden zu keiner Zeit angezeigt oder ausgegeben, sodass sie weder bei der Dateneingabe im Behandlungsumfeld noch durch Zusammenführen exportierter Daten einer erfassten Person zugeordnet werden können. Eine Re-Identifizierung (De-Pseudonymisierung) kann nur kontrolliert mithilfe der Mainzelliste durchgeführt werden.

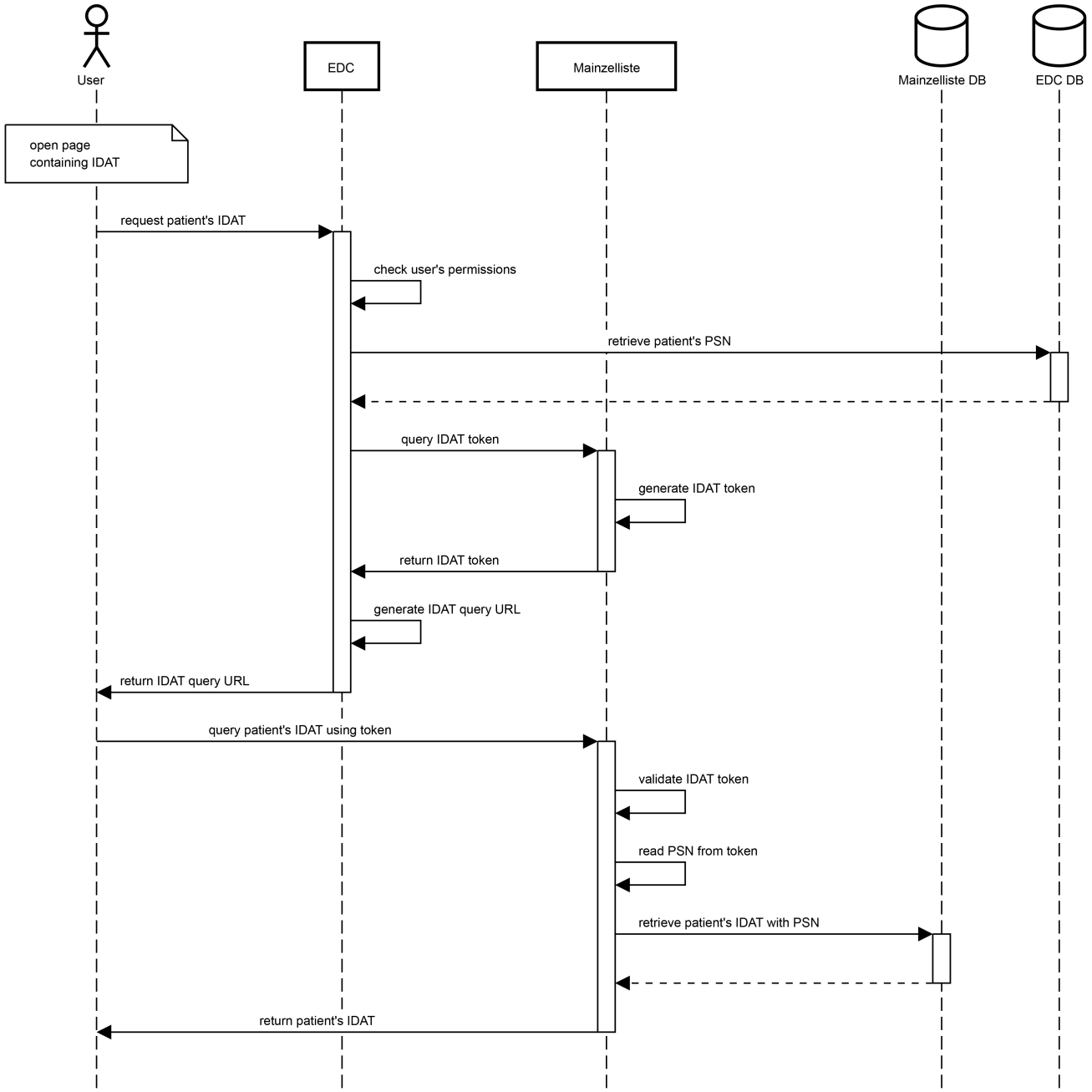


Abbildung 3: Abruf von IDAT

Pseudonymisierung beim Datenimport

Beim Datenimport werden die IDAT vor dem Laden der Datensätze (siehe Abschnitt 4.2 „Datenimport“) durch Pseudonyme ersetzt. Datenextraktion und -transformation werden durch eine Datenintegrationssoftware unterstützt. Dabei ist die Pseudonymisierung Teil der Datentransformation und wird mit einer eigens dafür entwickelten Komponente durchgeführt. Folgende Schritte werden durchlaufen:

1) Für jeden Datensatz ruft die Datenintegrationssoftware die Mainzelliste auf und übergibt die IDAT.
2) Die Mainzelliste ermittelt oder erzeugt das PSN_{OSSE} (analog zur manuellen Dateneingabe) und verschlüsselt es mit einem öffentlichen Schlüssel des OSSE-Registers, damit das OSSE-Pseudonym nicht außerhalb der Mainzelliste mit den IDAT zusammengeführt werden kann.
3) Die Mainzelliste liefert das verschlüsselte Pseudonym, $(PSN_{OSSE})tr$, an die Transformationskomponente, wo die IDAT durch das $(PSN_{OSSE})tr$ ersetzt werden.
4) Die Importschnittstelle entschlüsselt das $(PSN_{OSSE})tr$ und speichert die Daten mit dem PSN_{OSSE}

Durch dieses Verfahren ist sichergestellt, dass auch beim Datenimport keine Pseudonyme zugeordnet werden können, da die datenliefernde Seite, die den Personenbezug herstellen kann, nur das verschlüsselte $(PSN_{OSSE})_{tr}$ sieht.

Schlüsselerzeugung und Schlüsselverwaltung

Das Schlüsselpaar für die asymmetrisch verschlüsselte Übertragung der OSSE-Pseudonyme wird im OSSE-Register bei Systemstart erzeugt und nur zur Laufzeit im Speicher gehalten. Bei Neustart oder durch eine Funktion des Registers kann ein neues Schlüsselpaar erzeugt werden. Der aktuelle öffentliche Schlüssel kann durch eine dazu berechtigte Komponente (z.B. das Pseudonymisierungs- und Identitätsmanagement) jederzeit über eine Webschnittstelle beim OSSE-Register abgerufen werden.

4.4 Einwilligungsmanagement

Rechtsgrundlage der Nutzung der Daten im NARSE sind die informierten Einwilligungen der Registrierten durch die Patienten oder Probanden selbst oder durch deren gesetzliche Vertretenden.

In den Einwilligungen sind Differenzierungen möglich, die

- die Datennutzung in der gesamten Europäischen Union,
- die Erfassung genetischer Informationen,
- die Erneute Kontaktaufnahme und
- die Fallbesprechung durch SE-Boards

jeweils einschließen oder ausschließen.

Initial beginnt die Erhebung der Einwilligungen bei den datenerhebenden Ärztinnen und Ärzten papierbasiert mit Verwahrung des Originals bei den Erhebenden und der vertraulichen Zusendung einer Kopie des Einwilligungsdokumentes an die Unabhängige Treuhandstelle der TU Dresden (UTHS Dresden).

Das NARSE und die UTHS Dresden entwickeln zeitnah auf der Basis der in der UTHS Dresden genutzten Treuhandstellen-Tools aus der UTHS Greifswald oder gleichwertigen Werkzeugen ein digitales Einwilligungsmanagement, das an die Pseudonymisierungs- und Identifizierungsprozesse angeschlossen und in der Dresdner UTHS betrieben und gesteuert wird.

4.5 Kontrollierte Datenfernverarbeitung und Gastwissenschaftlerarbeitsplätze

Von der Transferstelle werden im Falle einer Kontrollierten Datenfernverarbeitung die Algorithmen geprüft und gegebenenfalls ausgeführt oder es wird ein Gastwissenschaftlerarbeitsplatz eingerichtet oder der benötigte Datensatz wird zusammengestellt. Prinzipiell sind verschiedene Formen der Datennutzung vorgesehen: On-Site-Nutzung (kontrollierte Datenfernverarbeitung, Gastwissenschaftlerarbeitsplätze) oder Off-Site-Nutzung (Agreed Use Files, Scientific Use Files, Public Use Files, Campus Use Files).

4.6 Datenexport

Medizinische Daten können zu Auswertungszwecken exportiert werden. Folgende Schritte werden beim Export durchlaufen:

1) OSSE schickt das interne Pseudonyme $PSN_{OSSE(\#)}$ zusammen mit einer Projektkennung an das Pseudonym- und Identitätsmanagement, das in der Unabhängigen Treuhandstelle betrieben wird.
2) Das Pseudonymisierungs- und Identitätsmanagement liefert ein einheitliches projektspezifisches Exportpseudonym ($PSN_{Projekt}$) zurück.
3) Der Datensatz wird entweder mit dem $PSN_{Projekt}$ ausgegeben.

Der Export aus dem geschützten Raum des NARSE und die Herausgabe der exportierten Daten für externe Datennutzung setzt einen Datennutzungsnutzungsantrag an das Data Access Committee (DAC), eine Zustimmung des DAC und einen Datennutzungsvertrag gemäß Datennutzungsordnung voraus. Das DAC prüft die Zielkonformität, die Rechtmäßigkeit und die Qualität des Datennutzungsantrags. In der Regel erfolgt die Herausgabe von Datensätzen mit $PSN_{Projekt}$.

Besonders bei Erkrankungen mit geringen Fallzahlen lassen sich MDAT bei Kenntnis des Krankheitsverlaufs oder zusätzlicher Daten auch ohne Kenntnis der IDAT konkreten betroffenen Personen zuordnen. Auch bei der Verwendung nicht-rückführbarer Exportpseudonyme kann nicht immer sicher von absoluter oder faktischer Anonymität ausgegangen werden. Mitunter besteht nur formale Anonymität. Deshalb wird auch der Export pseudonymisierter Daten und der Zweck ihrer Nutzung in der informierten Einwilligung berücksichtigt und an eine verpflichtende Nutzungsvereinbarung gekoppelt.

5. Organisatorische Rahmenbedingungen

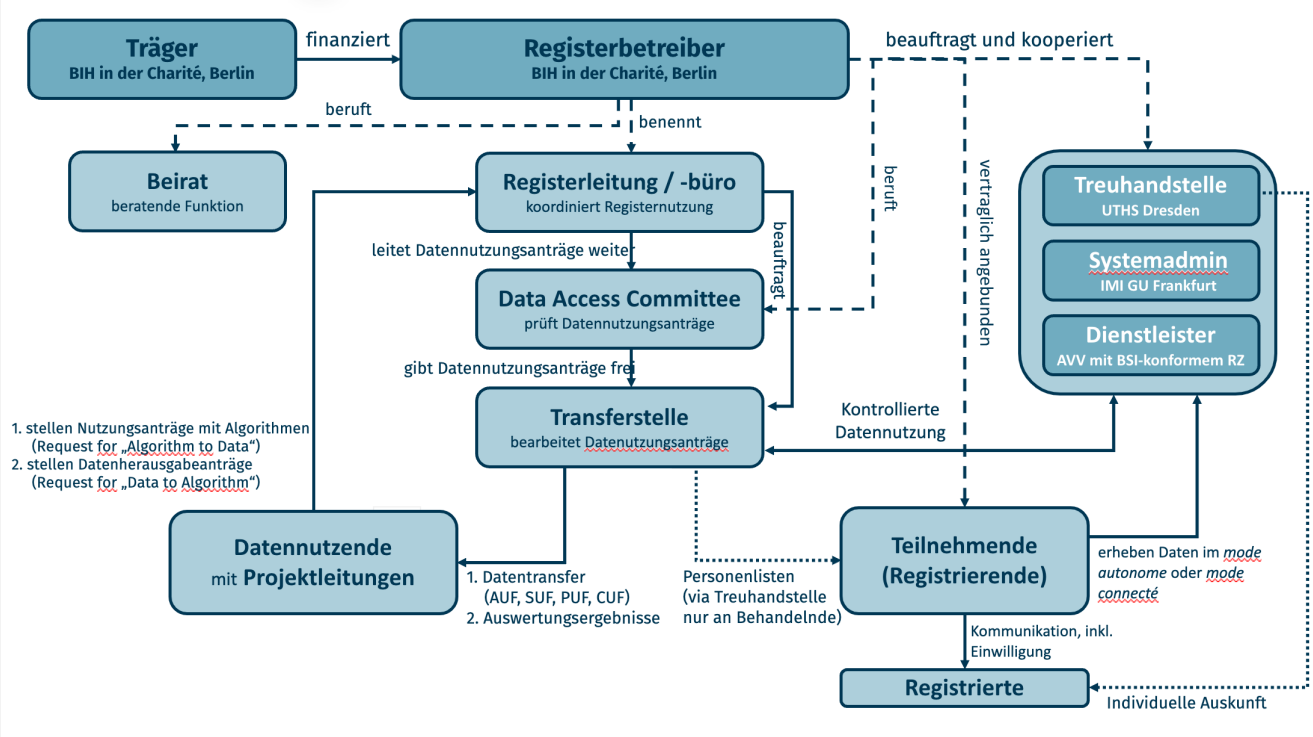


Abbildung 4: Organisationsstruktur des NARSE

5.1 Betrieb der Komponenten

Der Betrieb des OSSE-Registers erfolgt initial in der Verantwortung des Berlin Institute of Health (BIH) der Charité – Universitätsmedizin Berlin. Der Registerbetreiber übernimmt auch die Rolle der Studienleitung. Alle aktuellen Vertragspartner werden auch auf der Website www.narse.de bekannt gegeben.

Die OSSE-Komponente wird auf einem angemieteten Server eines Anbieters für BSI-zertifizierte Rechenzentrumsleistungen realisiert. Mit dem Anbieter wird vom Betreiber des NARSE ein Vertrag zur Auftragsverarbeitung abgeschlossen.

Für die Systemadministration der IT-Infrastruktur der OSSE-Komponenten und den technischen Support wird initial mit dem Institut für Medizininformatik (IMI) der Goethe-Universität Frankfurt ein Vertrag zur Auftragsverarbeitung geschlossen.

Der Betrieb des Pseudonymisierungs- und Identitätsmanagementstools Mainzelliste (https://www.toolpool-gesundheitsforschung.de/produkte/mainzelliste) sowie des zentralen Einwilligungsmanagements wird an die Unabhängige Treuhandstelle der TU Dresden (UTHS Dresden) im Rahmen eines Joint Controller Vertrages überantwortet.

5.2 Teilnehmende

Eine aktuelle Liste der am NARSE beteiligten Kliniken, Zentren und Patientenorganisationen ist unter www.narse.de zu finden. Generell können alle Mitglieder der Registerstandorte als Teilnehmende das NARSE nutzen, wobei jeder Standort selbst entscheidet, welche seiner Mitglieder eine Zugangsberechtigung erhalten sollen (siehe Abschnitt 6.2 „Autorisierung und Authentifizierung“).

5.3 Beirat

Die Weiterentwicklung des NARSE in den skizzierten Entwicklungsstufen erfolgt durch einen wissenschaftlichen Beirat, der sich aus Vertreter/innen des Registerbetreibers, Vertreter/innen des Think Tanks der Eva Luise und Horst Köhler Stiftung für Menschen mit Seltenen Erkrankungen sowie Projektpartnern aus dem begleitenden Evaluationsprojekt FAIR4Rare zusammensetzt.

5.4 Data Access Committee

Der Registerbetreiber benennt in Absprache mit dem Beirat ein Data Access Committee (DAC). Zu den Mitgliedern des Data Access Committee zählen medizinische Experten, z.B. Vertreter/innen aus wissenschaftlichem und klinischem Fachpersonal der Teilnehmer des NARSE, Vertreter/innen von Patientenorganisationen oder der ACHSE, aber auch Vertreter/innen anderer Fachbereiche, insbesondere Datenschutz, Epidemiologie oder Medizinethik.

Dieses Data Access Committe (DAC) ist für die Prüfung und Bewilligung von Datennutzungsanträgen auf Export medizinischer Daten für alle Forschungsprojekte verantwortlich.

Innerhalb des ersten halben Jahres wird vom NARSE-Betreiber eine Satzung und eine Nutzungsordnung verfasst und mit den Gremien des NARSE abgestimmt. Diese werden unter anderem regeln:

- Wer nutzungsberechtigt sein wird.
- Wie das Antrags- und Genehmigungsverfahren aussehen wird.
- Welche Kriterien ein Datennutzungsantrag erfüllen muss.
- In welcher Weise Behandelnde die Registerdaten für eigene Forschungszwecke nutzen können.
- Ob Informationen aus dem Register zur direkten Beeinflussung von Behandlung genutzt werden dürfen (z. B. durch die Suche nach ähnlichen Fällen).
- Wie der Verweis auf Bilddaten und Proben gehandhabt wird (kurz- und langfristig).
- Wie die Daten zu verschiedenen Erkrankungen voneinander abgegrenzt werden sollen.
- Wie die Kooperation mit vorhandenen Registern zu einzelnen seltenen Erkrankungen organisiert wird.

5.5 Registerleitung

Die Studienleitung ist zuständig für:

- Datenmanagement
- Plausibilitätskontrollen
- Datenexporte
- Erstellen von Berichten

5.6 Systemadministration

Die im NARSE gespeicherten Daten können prinzipiell von den Systemadministratoren/Systemadministratorinnen der verwendeten Server eingesehen werden. Zugriffe auf die Daten durch Administratoren/Administratorinnen dürfen nur erfolgen, wenn dies zur Erfüllung ihrer Aufgaben zwingend erforderlich ist. Dies kann bei den folgenden Tätigkeiten der Fall sein:

- Systemkonfiguration und Systemwartung (z.B. Updates des Betriebssystems oder der Software)
- Manuelle Änderungen in der Datenbank (z.B. Standortzugehörigkeit einer im Register erfassten Person)
- Unterstützung beim Datenexport
- Unterstützende Dienstleistung zur Erfüllung der Betroffenenrechte im Auftrag des Verantwortlichen

Das Vorgehen beim Datenzugriff ist durch folgenden Prozess geregelt:

- Vor dem Zugriff wird geklärt, ob der Datenzugriff tatsächlich notwendig ist.
- Der Datenzugriff wird protokolliert. Das Protokoll umfasst dabei mindestens die folgenden Inhalte:
  - den Zeitpunkt des Datenzugriffs,
  - die beteiligten Administratoren/Administratorinnen,
  - den Grund des Datenzugriffs,
  - die involvierten Nutzdaten (nach Möglichkeiten anonymisiert oder pseudonymisiert).

Alle Administratoren/Administratorinnen sind entsprechend zu instruieren und zur Verschwiegenheit zu verpflichten[15].

6. Weitere Maßnahmen zum Datenschutz

Um den Datenschutz[16] bei der Verarbeitung von personenbezogenen Daten zu gewährleisten, werden weitere Maßnahmen getroffen. Über die in diesem Abschnitt genannten Maßnahmen finden sich die relevanten gültigen technischen und organisatorischen Maßnahmen (TOMs), um die Sicherheit der erhobenen und verarbeiteten personenbezogenen Daten zu gewährleisten, siehe Abschnitt 8.4 „Technische und organisatorische Maßnahmen“.

6.1 Informationelle Gewaltenteilung

Der Pseudonymisierungsdienst „Mainzelliste“ sowie das Identitäts- und Einwilligungsmanagement werden logisch und physikalisch getrennt von allen Komponenten betrieben, die MDAT speichern. Für den Betrieb des Pseudonymisierungsdienstes sowie des Identitäts- und Einwilligungsmanagement wird die Verantwortung an die Unabhängige Treuhandstelle der TU Dresden übergeben. Diese Institution steht unter eigener rechtlicher Verantwortung und ist dem Registerbetreiber gegenüber bei Weisungen, die die Datenschutzziele wie Vertraulichkeit, Verfügbarkeit und Integrität gefährden, nicht weisungsgebunden.

So ist sichergestellt, dass Personen, die im NARSE außerhalb des Behandlungszusammenhangs Zugriff auf medizinische Daten haben, keine Zuordnung zu realen Personen treffen können.

6.2 Autorisierung und Authentifizierung

Autorisierung von Benutzern/Benutzerinnen

Die Autorisierung von Benutzern/Benutzerinnen (Zuweisung zu definierten Rollen) des NARSE erfolgt durch Administratoren/Administratorinnen der jeweiligen Standorte oder Administratoren/Administratorinnen des Registerbetreibers entsprechend den lokalen Strukturen und Erfordernissen.

Autorisierung von Komponenten

Der Zugriff von IT-Komponenten untereinander wird in der jeweiligen Konfiguration festgelegt. Dazu werden ab Beginn der Inbetriebnahme des NARSE die IP-Adresse des zugreifenden Systems und ein Passwort erfasst.

Authentifizierung von Benutzern/Benutzerinnen

Die Authentifizierung von Benutzern/Benutzerinnen gegenüber dem NARSE erfolgt über Benutzername und Passwort mit der Möglichkeit, durch eine Zwei-Faktor-Authentifizierung ein erhöhtes Maß an Sicherheit zu erreichen. Der zweite Faktor besteht aus einem zeitlich begrenzt gültigen Einmal-Passwort, das nach dem TOTP-Verfahren auf einem Endgerät des Nutzers/der Nutzerin erzeugt wird. Nutzer/Nutzerinnen müssen die Verwendung des zweiten Faktors selbständig aktivieren und erhalten bei der Aktivierung drei unbegrenzt gültige Einmal-Passwörter für den Fall, dass das Endgerät zur Erzeugung der Passwörter unbrauchbar wird.

[15] Dies sollte in der Regel im Rahmen des Arbeitsverhältnisses an der zuständigen Institution ohnehin geschehen sein.

[16] Datenschutzgrundverordnung (DSGVO)

Authentifizierung von Komponenten

Zugriffe zwischen verschiedenen IT-Komponenten über das Internet finden nur nach erfolgreicher Authentifizierung statt. Die Authentifizierung des OSSE EDCs gegenüber dem MDR und Formulareditor erfolgt über Login und Passwort, die bei der Initialisierung bzw. der Installation des Registers festgelegt werden. Die Authentifizierung des OSSE EDCs gegenüber dem Pseudonymisierungsdienst Mainzelliste, der von der UTHS Dresden betrieben wird, erfolgt über einen bei der Installation festgelegten API-Key.

6.3 Maßnahmen in der IT-Infrastruktur

Sicherheit der gespeicherten Daten

Alle in den zentralen Komponenten des NARSE erhobenen Daten werden lokal in Datenbanken auf virtuellen Servern gespeichert. Nur Administratoren/Administratorinnen des jeweiligen Servers haben Zugriff auf die Daten. Alle Server befinden sich in Rechenzentren mit Standort in Deutschland, die über eine Zugangskontrolle per Chipkarte oder ähnlich sichere Token für jeweils berechtigte Personen verfügen.

Darüber hinaus sind die medizinischen Daten auf dem Server in einem nach dem Stand der Technik verschlüsselten Container gespeichert. Das Kennwort zur Entschlüsselung ist ausschließlich den Systemadministratoren/Systemadministratorinnen bekannt.

Sicherheit der Kommunikation

Die Vertraulichkeit der Kommunikation zwischen den Komponenten wird durch folgende Maßnahmen sichergestellt:

- Die Kommunikation zwischen den Komponenten, ebenso wie die Kommunikation zwischen dem Browser eines/einer Nutzers/Nutzerin und dem OSSE EDC oder dem Pseudonymisierungsdienst Mainzelliste in der UTHS Dresden, erfolgt grundsätzlich über verschlüsselte Verbindungen (HTTPS). Die dafür eingesetzten Schlüssel und Zertifikate sind so zu erstellen, dass sie den aktuell anerkannten Anforderungen entsprechen (z.B. X.509 Zertifikate mit einem 2048 Bit RSA Schlüssel). Aktuelle Anforderungen können den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik entnommen werden[17].
- Durch Firewalls ist sichergestellt, dass die Server, auf denen die zentralen Komponenten laufen, nur über diejenigen Protokolle und Ports erreichbar sind, die für die Kommunikation mit Benutzern oder anderen Komponenten erforderlich sind (in der Regel HTTPS-Verbindungen). Der administrative Zugang ist auf das Intranet des Betreibers beschränkt.

Protokollierung

Es erfolgt eine Protokollierung der Zugriffe von Nutzer/innen auf die Komponenten sowie Zugriffe zwischen den Komponenten. Das Protokoll enthält mindestens:

- Die Identität der zugreifenden Person oder Komponente.
- Datum und Uhrzeit des Zugriffs.
- Den Inhalt des Zugriffs (die übermittelten Daten, ggf. aggregiert) oder Informationen, aus denen dieser rekonstruiert werden kann (z.B. Verweis auf einen Datenbankeintrag o.ä.).

Das Protokoll wird zusammen mit den Nutzdaten des entsprechenden Servers gespeichert und zwischen einem und sechs Monaten aufbewahrt. Die aufgezeichneten Daten dürfen nur im Rahmen der technischen Administration (insbesondere zur Fehlersuche) und bei der Verfolgung von Missbrauch eingesehen werden.

[17] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

6.4 Five Safes und gestufte Datenzugangsformen

Organisatorisch-Technische(r) Datennutzungszugang oder Datennutzungsform

… Form des Zugangs zur Datennutzung mit folgenden Unterscheidungen:

- ☐ On-site-Nutzung
  - Kontrollierte Datenfernverarbeitung
  - Gastwissenschaftlerarbeitsplatz
- ☐ Off-Site-Nutzung
  - Agreed Use Files
  - Scientific Use Files
  - Public Use Files
  - Campus Use Files
- ☐ Personenlisten zu Händen Behandelnder Ärztinnen und Ärzte oder Einrichtungen

Five Safes

… ist ein fünfdimensionales Konzept zur sicheren Nutzung von Daten, wobei mehr Strenge in einer Dimension zu mehr Freiheitsgraden in einer anderen führen kann: Sichere Projekte, Sichere Menschen, Sichere Umgebungen, Sichere Daten und Sichere Ergebnisse. Die Kombination der Kontrollen führt zu einer 'sicheren Nutzung'. Diese werden meist als Fragen formuliert, zum Beispiel

Safe projects	Is this use of the data appropriate?
Safe people	Can the users be trusted to use it in an appropriate manner?
Safe settings	Does the access facility limit unauthorised use?
Safe data	Is there a disclosure risk in the data itself?
Safe outputs	Are the statistical results non-disclosive?

Diese Dimensionen sind Skalen, keine Grenzen. Das heißt, Lösungen können eine Mischung aus mehr oder weniger Kontrollen in jeder Dimension haben, aber das Gesamtziel der "sicheren Nutzung" ist unabhängig von der jeweiligen Mischung. Bei einer öffentlich zugänglichen Datei (Public Use File), die frei heruntergeladen werden kann, kann beispielsweise nicht kontrolliert werden, wer sie wo oder zu welchem Zweck verwendet. Im Gegensatz dazu kann eine Datei, auf die nur über eine sichere Umgebung (Safe Setting) mit zertifizierten Benutzern (Safe People) zugegriffen wird, sehr sensible Informationen enthalten.

Kontrollierte Datenfernverarbeitung in der Transferstelle

… Datennutzungsform, bei der ein extern erstelltes Skript eines Nutzenden durch die Transferstelle des NARSE im Auftrag kontrolliert ausgeführt wird. Die Ergebnisse werden den Nutzenden gemäß Nutzungsvertrag überprüft zur Verfügung gestellt.

Gastwissenschaftlerarbeitsplatz (GWAP) bei der Transferstelle

… technisch und organisatorisch gegen unerlaubte und unlautere Datennutzung eingerichteter Arbeitsplatz im lokalen Safe Setting, an denen die Daten des Registers gegebenenfalls mit Ergänzungen durch Gast-Wissenschaftlerinnen und Wissenschaftler analysiert werden können.

Agreed Use File (AUF)

… individuell von Antragstellenden erbetene („solicited“) und mit diesen vereinbarte, formal anonymisierte Datensätze, die von der Transferstelle mit individuellem Nutzungsvertrag im Einklang mit den Einwilligungen doppelt pseudonymisiert zur Nutzung in externen sicheren Umgebungen (Safe Setting) mit zertifizierten Benutzern (Safe People) übergeben werden.

Scientific Use File (SUF)

… standardisierte, „faktisch anonymisierte“ 18Datensätze, die von der Transferstelle des NARSE für gängige Statistiken erstellt werden. SUF bieten im Vergleich zur „On-Site-Nutzung“ und zu „Agreed Use Files“ ein geringeres Analysepotenzial, sind jedoch so strukturiert, dass sie sich für einen großen Teil der wissenschaftlichen Forschungsvorhaben eignen. Die Herausgabe erfolgt nur an Safe Settings und Safe People auf der Basis von genehmigten Nutzungsanträgen oder Nutzungsanzeigen.

Public Use File (PUF)

… „absolut anonymisierte19“, nicht mehr personenbeziehbare Datensätze (Mikrodaten). Aufgrund der starken Anonymisierung sind in PUF nur ausgewählte Merkmale enthalten. Fachlich tief gegliederte Merkmale werden in der Regel aggregiert. Tiefere räumliche Abgrenzungen können auf der Basis von PUF meist nicht vorgenommen werden. Sie können nach erfolgreicher Registrierung kostenlos heruntergeladen werden. PUF werden für das Analyseprogramm R angeboten oder mit entsprechenden Einleseroutinen bereitgestellt. Ihre Nutzung ist nicht ortsgebunden.

Campus Use File (CUF)

… absolut anonymisierte, auch „verwischte“ oder „verfälschte“ Datensätze, mit denen das NARSE den Umgang mit Mikrodaten in der wissenschaftlichen Lehre fördert. Anhand von CUF haben Studierende die Möglichkeit, sich Methodenkenntnisse anzueignen sowie erste Erfahrungen mit der Auswertung von Mikrodaten zu sammeln.

Nutzungsantrag

… das Dokument, mit dem die Nutzung von Mikrodaten des NARSE in Form eines Nutzungsprojektes beantragt wird. Es enthält u. a. die wissenschaftliche oder klinische Begründung für die Nutzung der Daten sowie die Beschreibung der Kriterien und Konfigurationen, nach denen die Nutzung durchgeführt werden soll. Ein Nutzungsantrag kann bis auf Weiteres nur schriftlich (papierformularbasiert) gestellt werden und wird nach Genehmigung Bestandteil des Nutzungsvertrags.

Nutzungsanzeige

… das alternative Dokument, mit dem die Nutzung von Mikrodaten durch einen internen Nutzer durch den Betreiber des NARSE in Form eines Nutzungsprojektes bekanntgegeben und dokumentiert wird. Es enthält u.a. die Qualitätssicherungs- oder wissenschaftliche oder klinische Begründung für die Nutzung der Daten und sowie die Beschreibung der Kriterien und Konfigurationen, nach denen die Nutzung durchgeführt werden soll. Eine Nutzungsanzeige muss schriftlich dokumentiert werden; nach deren Freigabe kann die Nutzung ohne Nutzungsvertrag erfolgen.

Nutzungsvertrag

… das Dokument, in dem alle wesentlichen Punkte der Datennutzung nach Nutzungsantraggeregelt sind. Der Abschluss eines Nutzungsvertrags ist die Voraussetzung für den Start eines Nutzungsprojekts über die lokalen Daten hinaus.

7. Wahrung von Betroffenenrechten

7.1 Aufklärung und Einwilligung

Die informierte Einwilligung (siehe Anhang 8.1 „Patienteneinwilligung NARSE“) ist Rechtsgrundlage der Datenverarbeitung. Mit der Einwilligung erklärt sich die betroffene Person insbesondere dazu bereit, dass

[18] §§ 5, 16 BundesstatistikG

[19] Siehe zuvor

- ihre IDAT an das Pseudonymisierungs- und Identitätsmanagement übermittelt und dort gespeichert werden,
- ihre MDAT gemäß Registerdefinition im NARSE erfasst werden,
- diese MDAT von Forscher/innen des NARSE, die benannt und an die Nutzungsbedingungen gebunden sind, lokal ausgewertet werden können und
- MDAT aus dem OSSE-Register anonymisiert oder mit einem nicht-rückführbaren Exportpseudonym exportiert und für Forschungszwecke, die in der Einwilligung näher definiert sind, an externe Forscher oder Institutionen, die benannt und an die Nutzungsbedingungen gebunden sind, übermittelt werden.
- In den Einwilligungen sind Differenzierungen möglich, die
  - die Datennutzung in der gesamten Europäischen Union,
  - die Erfassung genetischer Informationen,
  - die Erneute Kontaktaufnahme und
  - die Fallbesprechung durch SE-Boards

  jeweils einschließen oder ausschließen.

Mit Einholen der Einwilligung wird die betroffene Person über ihre Betroffenenrechte (Recht auf Auskunft, Widerruf, Berichtigung, Einschränkung der Verarbeitung und Beschwerde bei einer Aufsichtsbehörde) informiert.

7.2 Auskunft über gespeicherte Daten

Im NARSE erfasste Personen haben das Recht, Auskunft darüber zu erhalten, ob und welche Daten von ihnen im Register gespeichert werden, und diese Daten einzusehen. Der Antrag auf Auskunft ist schriftlich an den Registerbetreiber zu stellen. Daraufhin wird ein menschenlesbarer Ausdruck der Daten erzeugt und der erfassten Person ausgehändigt.

Betroffene Personen haben das Recht auf Auskunft folgender Daten und Informationen (Art. 15 Absatz 1 lit. e-h DSGVO):

- Verarbeitungszwecke
- Kategorien der personenbezogenen Daten, die verarbeitet werden
- Empfänger oder Kategorien von Empfängern, die die personenbezogenen Daten erhalten haben
- Geplante Dauer der Speicherung
- Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- Verfügbare Informationen über die Herkunft der Daten
- Im Register gespeicherte Daten

7.3 Datenübertragbarkeit

Im NARSE erfasste Personen haben das Recht, die Sie betreffenden personenbezogenen Daten, die sie selber einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sofern von einer betroffenen Person Daten in das NARSE eingetragen worden sind und die Person die Datenübertragung in einen anderen Datenbestand anfordert, wird der Betreiber des NARSE die Person nach Möglichkeit unterstützen.

7.4 Widerruf, Löschung, De-Identifizierung

Erfasste Personen haben das Recht, die Einwilligung in die Verarbeitung ihrer Daten im NARSE zu widerrufen. Der Widerruf ist als eindeutige Willensbezeugung direkt an die Unabhängige Treuhandstelle (UTHS) oder an den behandelnden Arzt / die behandelnde Ärztin zu richten, der/die diesen an die UTHS weiterleitet. Es ist möglich, den Widerruf in schriftlicher Form über die Homepage www.narse.de oder per E-Mail zu kommunizieren.

Im Falle eines Widerrufs entscheidet die widerrufende Person, wie mit ihren Daten verfahren werden soll. Die im Register erfassten MDAT können vollständig gelöscht oder durch Löschen der zugehörigen IDAT und des Pseudonyms, in welchem Fall sie weiterhin für Auswertungen zur Verfügung stehen, de-identifiziert werden. Wenn eine Löschung der Daten voraussichtlich die Verwirklichung eines bereits gestarteten oder die Nachvollziehbarkeit eines beendeten Forschungsprojekts unmöglich macht oder ernsthaft beeinträchtigt, werden die Daten im Rahmen gesetzlich bestehender Ausnahmeregelungen nicht gelöscht. In diesen Fällen werden die Daten so gesperrt, dass sie nur noch für die den gesetzlichen Ausnahmeregelungen zugrundeliegenden notwendigen Zwecken verarbeitet werden können.

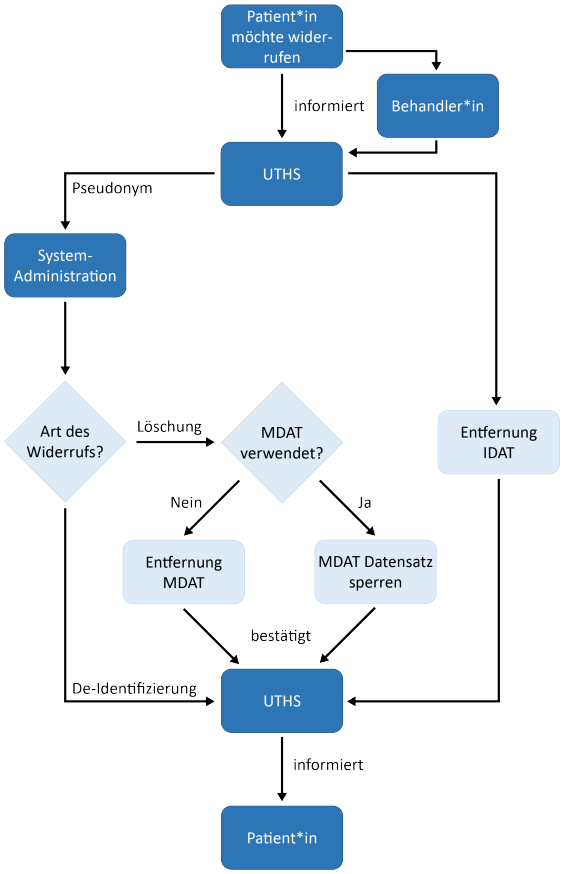


Abbildung 5: Ablauf des Widerrufs der Einwilligung

Im Fall einer De-Identifizierung werden die IDAT einer erfassten Person inklusive zugehöriger Pseudonyme vernichtet. Es verbleiben nur die MDAT, die in der Regel keinen Rückschluss auf eine Person zulassen[20].Speziell im Bereich der Ultraseltenen Erkrankungen kann aber nicht ausgeschlossen werden, dass durch MDAT-Rückschlüsse auf die Identität eines/einer Betroffenen gezogen werden können.

Zur De-Identifizierung werden die Datensätze im Pseudonymisierungs- und Identitätsmanagement (Mainzelliste) durch die UTHS gelöscht und das bisherige PSN_{OSSE} der widerrufenden Person durch ein zufälliges Pseudonym ersetzt. Für den Fall, dass Daten archiviert wurden, wird dieser Vorgang ebenso für die archivierten Datensätze durchgeführt. Durch den Algorithmus zur Erzeugung von Pseudonymen ist sichergestellt, dass die Pseudonyme einer de-identifizierten Person nicht mehr für neu erfasste Personen verwendet werden. Die UTHS informiert die Systemadministration des OSSE-Registers, um sicherzustellen, dass die im OSSE-Register verbleibenden MDAT entsprechend umpseudonymisiert werden.

Im Falle der vollständigen Löschung werden die IDAT analog zur De-Identifizierung durch die UTHS gelöscht. Zusätzlich informiert die UTHS die Systemadministration des OSSE-Registers anhand des verwendeten Pseudonyms der widerrufenden Person, um die Löschung der im OSSE-Register erfassten MDAT zu veranlassen; dies umfasst auch die Löschung der Daten im Audit Trail des OSSE-Registers. Die Systemadministration des OSSE-Registers führt die Löschung durch und bestätigt der zuständigen UTHS die erfolgte Löschung der MDAT.

Die vollständige Löschung oder De-Identifizierung ist von der zuständigen UTHS, mit Unterstützung der Systemadministration des OSSE-Registers, zeitnah, maximal innerhalb von einem Monat nach Bekanntwerden des Widerrufs, vorzunehmen[21]. Der Erhalt des Widerrufs wird der betroffenen Person schriftlich oder per E-Mail an die für den Widerruf verwendete Kontaktadresse bestätigt, unter Angabe eines Zeitpunkts, bis wann die Daten gelöscht werden (hier ist die 1-Monatsfrist ab Bekanntwerden des Widerrufs einzuhalten).

7.5 Dauer der Speicherung

Das NARSE soll langfristig betrieben werden ohne ein festgelegtes Enddatum. In einem internen Prozess wird regelmäßig überprüft, ob das NARSE weiterlaufen soll oder ob die Registeraktivitäten eingestellt werden sollen.

[20] Anonymisierte Daten fallen nicht unter den Anwendungsbereich der DSGVO.

[21] Die meist impraktikable Anonymisierung in Datensicherungen ist verzichtbar, sofern die Sicherungen nur durch zuständige Systemadministrator/innen eingesehen werden können und alte Sicherungen regelmäßig gelöscht werden.

Die erhobenen Daten bleiben bis auf weiteres im NARSE gespeichert, bis eine betroffene Person ihre Einwilligung widerruft (s. 7.4 „Widerruf, Löschung, De-Identifizierung“) oder bis zu 10 Jahren, nachdem sämtliche Registeraktivitäten eingestellt wurden.

Falls der Datenbestand nicht mehr in der vorgesehenen Form genutzt werden kann, prüft der Betreiber des Registers, ob eine Rechtsgrundlage für eine anderweitige Verwendung der Daten, gegebenenfalls in anonymisierter Form, besteht. Falls diese Prüfung negativ ausfällt, sind die Daten zu löschen.

8. Anhang I: Patienteninformation, Patienteneinwilligung und Technische Angaben

8.1 Patienteneinwilligung NARSE

Die aktuelle Version der Patienteninformation und-einwilligung, ebenso die für Sorgeberechtigte und Jugendliche, befindet sich auf www.narse.de zum Herunterladen.

Stand 13.01.2024:

- 2023-10-17_NARSE_Info_Jugendliche_Einwilligung_V1.2
- 2024-01-13_NARSE_Patienteninfo_Einwilligung_V1.3
- 2024-01-13_NARSE_Elterninfo_Einwilligung_V1.3

8.2 Datensätze

2024-01-05_NARSE_Datenelemente_DE.pdf

NARSE Datensatz

Stand 12.01.2024

Medizinische Daten

	Datenelement	Format	Pflicht	Kommentar
Einwilligung	Einwilligungsdatum	Datum (YYYY-MM-DD)	X	
	Einwilligung Datennutzung	Ja / Nein	X	
	Einwilligung Datennutzung international (EU)	Ja / Nein		Wenn Einwilligung Datennutzung = Ja
	Einwilligung Rekontaktierung für Forschungszwecke oder Vernetzung	Ja / Nein		Wenn Einwilligung Datennutzung = Ja
	Einwilligung Erfassung genetischer Informationen	Ja / Nein		Wenn Einwilligung Datennutzung = Ja
	Einwilligung Fallbesprechung	Ja / Nein		Wenn Einwilligung Datennutzung = Ja
	Einschlussdatum	Datum (YYYY-MM-DD)	X	
Formale Kriterien	Gesicherte Diagnose(n): ORPHAcode	ORPHAcode		Mehrfacheingabe
	Gesicherte Diagnose(n): ICD Code	ICD Code (ICD-10-GM-2020 hinterlegt)		Mehrfacheingabe
	Gesicherte Diagnose(n): ICD Version	Freitext		Mehrfacheingabe
	Verdachtsdiagnose(n): ORPHAcode	ORPHAcode		Mehrfacheingabe
	Verdachtsdiagnose(n): ICD Code	ICD Code (ICD-10-GM-2020 hinterlegt)		Mehrfacheingabe
	Verdachtsdiagnose(n): ICD Version	Freitext		Mehrfacheingabe
Persönlicher und Familiärer Hintergrund	Alterskategorie	Unbekannt / Säugling (<1 Jahr) / Kleinkind (>1 bis <6 Jahre) / Schulkind (>6 bis <12 Jahre) / Jugendliche*r (>12 bis <18 Jahre) / Erwachsene*r (≥18 bis <50 Jahre) / Erwachsene*r (≥50 Jahre) / Ungeboren / Verstorben	X	
	Geschlecht	Weiblich / Männlich / Unbestimmt / Divers / Unbekannt	X	
	Aktueller Status: Datum	Datum (YYYY-MM-DD)		Mehrfacheingabe
	Aktueller Status: Status	Lebend / Tot / Nicht weiterverfolgt		Mehrfacheingabe
	Sterbealter	Zahl (0<=x<=100) in Jahren		Wenn Status = Tot
	An SE verstorben	Ja / Nein / Unbekannt		Wenn Status = Tot
	Andere Todesursache	Freitext		Wenn An SE verstorben = Nein
	Mutter von dieser SE betroffen	Ja / Nein / Unbekannt	X	
	Mutter verstorben	Ja / Nein / Unbekannt		
	Sterbealter der Mutter	Zahl (0<=x<=100) in Jahren		
	Vater von dieser SE betroffen	Ja / Nein / Unbekannt	X	
	Vater verstorben	Ja / Nein / Unbekannt		
	Sterbealter des Vaters	Zahl (0<=x<=100) in Jahren		
	Geschwister von dieser SE betroffen	Ja / Nein / Unbekannt	X	
	Betroffene Geschwister: Alter	Zahl (0<=x<=100) in Jahren		

8.3 Rollen & Berechtigungen

Rolle	Wer	Aufgaben	Berechtigungen
Träger	Berlin Institute of Health at Charité (BIH)	• Bereitstellung finanzielle Mittel für die Entwicklung und den Betrieb des Registers	• keine Einsicht in IDAT und MDAT
Registerbetreiber	Berlin Institute of Health at Charité (BIH)	• technischer und administrativer Betrieb des Registers • Verantwortlicher im Sinne des Art. 4 DSGVO • Führung der Geschäfte des Registers • Entscheidungen rund um die Weiterentwicklung des Registers	• keine Einsicht in IDAT und MDAT
Studienleitung	Berlin Institute of Health at Charité (BIH)	• zentraler Standort (Koordinierungsstelle) • Ansprechpartner für andere Registerstandorte • Ansprechpartner für inhaltliche Fragen	• Einsicht in MDAT • Datenexport • zentrale Definition von Nutzerrollen

		• Zugriff auf alle medizinischen Daten aller teilnehmenden Einrichtungen • Erstellung von Datenexporten und Auswertungen • Ansprechpartner für Data Access Committee bei Fragen zu Datennutzungsanträgen oder Auswertungen • Prüfung der Zulassungsberechtigung von Nutzern • zentrale Definition von Nutzerrollen • zentrale Verwaltung der Registerstandorte (teilnehmende Einrichtungen) • zentrale Nutzerverwaltung (Anlegen von Nutzerkonten, Zuweisung von Rollen) • Beantwortung von Nutzerfragen bei technischen Problemen oder Unklarheiten	• zentrale Verwaltung der Standorte (teilnehmende Einrichtungen) • zentrale Nutzerverwaltung (Anlegen von Nutzerkonten, Zuweisung von Rollen)
Beirat	FAIR4Rare + Think Tank SE	• Diskussion strategischer Fragen in beratender Funktion (keine konkreten Befugnisse) • Bestätigung der Zusammensetzung des Data Access Committees	• Keine Einsicht in IDAT und MDAT
Teilnehmer	Datenerfassende Standorte des Registers, z.B. Kliniken, Zentren, Organisationen	• Location Admin, der für den Standort Nutzer anlegen und vordefinierte Rollen vergeben kann	• keine Einsicht in MDAT und IDAT
Data Access Committee	Betreiber, med. Experten (Vertreter der Teilnehmer), ACHSE, ELHKS, Datenschutz…	• Prüfung und Bewilligung von Datennutzungsanträge/Anfragen	• Einsicht in MDAT
Treuhandstelle	UTHS Dresden	• Betrieb des zentralen ID-Managements du Pseudonymisierungstools (Mainzelliste) • Betrieb des zentralen Einwilligungsmanagements (gICS) • Ansprechpartner für Widerruf der Einwilligung • Ansprechpartner für datenschutzrechtliche Angelegenheiten (Betroffenenrechte) • Bearbeitung von Anfragen zu Identifikation eines Patienten	• Einsicht in IDAT
Systemadministration	Institut für Medizininformatik, Goethe-Universität Frankfurt	• dokumentierte manuelle Anpassungen in der Datenbank	• Einsicht in MDAT, wenn erforderlich (dokumentierter Zugriff)
Technische Dienstleister	Dienstleister, tba	• Bereitstellung der technischen Infrastruktur (Hoster)	• keine Einsicht in IDAT und MDAT

Teilnehmende Forscher*innen	Angehörige der NARSE Teilnehmer	• Angehörige der teilnehmenden Einrichtungen • Erfassung von Daten im NARSE • Stellung von Datennutzungsanträgen	• Einsicht in IDAT und MDAT ihrer Patientinnen und Patienten
Externe Interessensgruppen		• Stellung von Datennutzungsanträge	• keine Einsicht in IDAT und MDAT • erhalten nur aggregierte Daten nach Antragstellung

OSSE-Berechtigungen

- ☐ CreatePatients Permission to add new patients to your own location
- ☐ DataEntry Permission to enter and edit medical data of your own location
- ☐ See my location's patients Permission to read data of your own location
- ☐ See other locations' patientsPermission to read data of any patient, i.e. also those of other locations
- ☐ See my IDAT Permission to see the IDAT of patients of your own location
- ☐ See all IDAT Permission to see the IDAT of any patient, i.e. also those of other locations
- ☐ DataExport Permission to export all medical data
- ☐ DataReport Permission to change the form status from open to reported
- ☐ DataValidation Permission to change the form status from reported to validated
- ☐ RemoveValidation Permission to change the form status from validated to open again
- ☐ PatientAccounts Permission to handle patient accounts

- ☐ Manage locations Permission to view, create and edit locations.
- ☐ Manage user roles Permission to view, create and edit user roles of all locations.
- ☐ Manage my location's user accountsPermission to view, create and edit user accounts of the own location, including allocation of roles and passwords.
- ☐ Manage all user accounts Permission to view, create and edit user accounts of all locations, including allocation of roles and passwords.

OSSE-Rollen: Zuordnung von Berechtigungen

Role	Global Admin	Location Admin	Dateneingabe	Datenansicht	Datenexport	IT Admin
Location	*zentral*	*pro Standort*	*pro Standort*	*pro Standort*	*zentral*	*zentral*
CreatePatients	-	-	X	-	-	-
DataEntry	-	-	X	-	-	-
See my location's patients	-	-	X	X	X	X
See other locations' patients	-	-	-	-	X	X
See my IDAT	-	-	X	-	-	-
See all IDAT	-	-	-	-	-	-
DataExport	-	-	-	-	X	-
DataReport	-	-	-	-	-	-

Role	Global Admin	Location Admin	Daten-eingabe	Daten-ansicht	Daten-export	IT Admin
Location	*zentral*	*pro Standort*	*pro Standort*	*pro Standort*	*zentral*	*zentral*
DataValidation	-	-	-	-	-	-
RemoveValidation	-	-	-	-	-	-
PatientAccounts	-	-	-	-	-	-
Manage locations	X	-	-	-		-
Manage user roles	X	-	-	-		-
Manage my location's user accounts	-	X	-	-		-
Manage all user accounts	X	-	-	-		-
Change software settings	X	-	-	-		-

8.4 Technische und organisatorische Maßnahmen (TOMs)

- ☐ Technische und organisatorische Maßnahmen (TOMs) OSSE: 2023-01-13_TOM_OSSE_v2.pdf
- ☐ Technische und organisatorische Maßnahmen des Dienstleisters: 2024-01-25_TOM_Hetzner.pdf

9. Tabellarische Datenschutz-Folgenabschätzung

DSFA: Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten

9.1 Gesetzliche Vorschrift betreffend DSFA und Definition für vorliegendes Dokument

Bei der Abfassung und Umsetzung eines Datenschutzkonzeptes (DSK) für das Nationale Register für Seltene Erkrankungen (NARSE) ist eine gesetzliche Vorschrift im Berliner Landesdatenschutzgesetz §26 Absatz (2) zu beachten, die eine entsprechende Dokumentation vor der Inbetriebnahme der „*automatisierten Verarbeitung personenbezogener Daten"* vorsieht. Für die Anforderungen der Bundesebene an Datenschutzkonzepte hat Thilo Weichert im Gutachten „Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung"[22] im Frühjahr 2022 dargestellt, dass in § 22 Abs. 2 Bundesdatenschutzgesetz (BDSG) die Inhalte eines Datenschutzkonzepts benannt werden.[23] Der Hauptteil des vorliegende Dokument (Kapitel 1 bis 7) erfüllt die Anforderungen der Bundesebene und der Berliner Landesebene an eine Datenschutzkonzept. .

Daneben ist zu beachten, dass auf der Europaebene mit der Datenschutzgrundverordnung (DSGVO), deren Regelungen bei umfangreichen Verarbeitungen von besonderen Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) ebenfalls einzuhalten sind, im Jahr 2018 der neue Begriff der „**Datenschutz-Folgenabschätzung"** (DSFA, Art. 35) eingeführt worden ist, ohne explizit einen Bezug zu Datenschutzkonzepten herzustellen. DSFA steht für die „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten". Eine verpflichtend geforderte DSFA muss [gemäß DSGVO Artikel 35 (7)] neben der Beschreibung von Verarbeitungsvorgängen und deren „Risiken für die Rechte und Freiheiten der betroffenen Personen" auch die Darstellung von „Abhilfemaßnahmen" zur Bewältigung der Risiken vorstellen. Der Begriff „Datenschutzkonzept" kommt in der DSGVO nicht vor. Gemäß Absatz (1)[24] von Artikel 35, muss die Abschätzung „**vorab"** durchgeführt und dokumentiert werden.

Aufgrund von Absprachen mit der Behördlichen Datenschutzbeauftragten der Charité und mit der AG Datenschutz des TMF e.V. erfolgt im vorliegenden **Datenschutzdokument für das NARSE** eine bedingte Zusammenführung

- des **Datenschutzkonzeptes (DSK)** gemäß Berliner (§ 26) und Bundes-Datenschutzgesetz (§ 22) und
- der **Datenschutz-Folgenabschätzung (DSFA)** gemäß DSGVO Artikel 35.

Im Sinne der Pflege in einem Dokument (=> Thilo Weichert) wird eine tabellarische DSFA als auswechselbare Anlage integriert [Kapitel 8 „Tabellarische Datenschutz-Folgenabschätzung" mit Abschnitt 8.2 „DSFA-Tabelle"]. Es wird verabredet, dass die Stellungnahme der TMF AG-Datenschutz zum Datenschutzkonzept sich primär auf den Hauptteil des vorliegenden Dokumentes [Kapitel 1 bis 7] bezieht, dass ein vollständiges klassisches DSK umfasst. Allfällige Änderungen des Kapitels 8 werden so abgefasst, dass die Gültigkeit des Hauptdokumentes und der Stellungnahme der TMF-AG-Datenschutz unberührt bleiben.

Die beiden folgenden Kästen dienen der Erläuterung des Vorgehens.

Exkurs 1

[22] Thilo Weichert 2022: Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung. S.200. Gutachten für den TMF e.V.

[23] *„Die Pflicht, ein Datenschutzkonzept für ein Forschungsvorhaben vorzulegen, besteht nicht generell, sondern nur gemäß einigen speziellen Gesetzen. Eine entsprechende Pflicht kann generell allenfalls aus den Dokumentationspflichten nach Art. 5 Abs. 2 DSGVO abgeleitet werden. Eine präzise Festlegung der notwendigen Inhalte ergibt sich aus den Gesetzen nicht. Als den Datenschutz umfassendes Dokument sollte es das Verarbeitungsverzeichnis, die Darstellung der technisch-organisatorischen Maßnahmen, die Datenschutz-Folgenabschätzung, die Einschränkung der Betroffenenrechte und die kompensierenden Garantien sowie, soweit es hierauf ankommt, die nötigen Interessenabwägungen enthalten.* Kap. 11.3, Kap. 11.4)"

[24] DSGVO Artikel 35 (1): *„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge,* ***so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.*** *Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden."*

Erläuterungen zur bedingten Zusammenführung von Datenschutzkonzept (DSK) und Datenschutz-Folgenabschätzung (DSFA) für das NARSE im vorliegenden Dokument

Bei der Abfassung und Umsetzung eines Datenschutzdokumentes für das in Berlin vom BIH betriebenen NARSE sind das Landesdatenschutzgesetz (insbesondere § 26), das Bundesdatenschutzgesetz (insbesondere § 22) und Europäische Datenschutzgrundverordnung (DSGVO; insbesondere Artikel 35) zu beachten.

Das Berliner Landesdatenschutzgesetz fordert in §26 Absatz (2) die Abfassung eines Datenschutzkonzeptes (DSK):

> *„[1]Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung einer automatisierten Verarbeitung personenbezogener Daten sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. [2]Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken ist die Ermittlung der Maßnahmen in angemessenen Abständen zu wiederholen.“*

Thilo Weichert verweist im Gutachten „Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung“[25] auf § 22 Abs. 2 Bundesdatenschutzgesetz (BDSG) [26] das Inhalte eines Datenschutzkonzepts erläutert, ohne abschließend den Anwendungsbereich festzulegen. *Die Pflicht, ein Datenschutzkonzept für ein Forschungsvorhaben vorzulegen, besteht nicht generell, sondern nur gemäß einigen speziellen Gesetzen. Eine entsprechende Pflicht kann generell allenfalls aus den Dokumentationspflichten nach Art. 5 Abs. 2 DSGVO abgeleitet werden. Eine präzise Festlegung der notwendigen Inhalte ergibt sich aus den Gesetzen nicht. Als den Datenschutz umfassendes Dokument sollte es das Verarbeitungsverzeichnis, die Darstellung der technisch-organisatorischen Maßnahmen, die Datenschutz-Folgenabschätzung, die Einschränkung der Betroffenenrechte und die kompensierenden Garantien sowie, soweit es hierauf ankommt, die nötigen Interessenabwägungen enthalten.* Kap. 11.3, Kap. 11.4). „Typischerweise enthalten solche Konzepte die Darstellung der Zwecke und Rechtsgrundlagen der Verarbeitung, die Regelung der Verantwortlichkeit, die Prozesse und Datenflüsse sowie insbesondere eine ausführliche Beschreibung der zum Schutz der Daten getroffenen technischen und organisatorischen Maßnahmen. Im Regelfall ist das Datenschutzkonzept damit auch Grundlage der in einem Verarbeitungstätigkeitenverzeichnis zu einem Projekt zu dokumentierenden Daten.“

[25] Thilo Weichert 2022: Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung. S.200. Gutachten für den TMF e.V.

[26] Bundesdatenschutzgesetz (BDSG); § 22 Verarbeitung besonderer Kategorien personenbezogener Daten

(2) In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Benennung einer oder eines Datenschutzbeauftragten,
5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. Pseudonymisierung personenbezogener Daten,
7. Verschlüsselung personenbezogener Daten,
8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.

Weichert fährt fort, dass mit der Datenschutzgrundverordnung (DSGVO) im Jahr 2018 der neue Begriff der Datenschutz-Folgenabschätzung (DSFA, Art. 35) eingeführt wurde, die zwingend bei umfangreichen Verarbeitungen von besonderen Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) einzuhalten ist (vgl. Art. 35 Abs. 3b) DSGVO).

Inhalte eines Datenschutzkonzeptes (den Datenschutz umfassendes Dokument) nach Th. Weichert 2022 Kap. 11.3, Kap. 11.4)	**Inhalte einer Datenschutz-Folgenabschätzung** Gemäß DSGVO Art. 35 Absatz (7)
☐ *(der Eintrag in) das Verarbeitungsverzeichnis,* ☐ *die Darstellung der technisch-organisatorischen Maßnahmen,* ☐ *die Datenschutz-Folgenabschätzung,* ☐ *die Einschränkung der Betroffenenrechte und* ☐ *die kompensierenden Garantien sowie,* ☐ *soweit es hierauf ankommt, die nötigen Interessenabwägungen enthalten.*	*a) „eine systematische **Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung**, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;* *b) eine **Bewertung** der Notwendigkeit und Verhältnismäßigkeit **der Verarbeitungsvorgänge** in Bezug auf den Zweck;* *c) eine **Bewertung der Risiken** für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und* d) *die zur Bewältigung der Risiken geplanten **Abhilfemaßnahmen**, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.“*

Besonders zu beachten ist, dass sowohl ein Datenschutzkonzept gemäß § 26 (2) des Berliner Landesdatenschutzgesetzes als auch eine **Datenschutz-Folgenabschätzung vor Aufnahme der Verarbeitungsvorgänge** erstellt werden müssen.

Ein Dokument oder zwei Dokumente?

Thilo Weichert führt aus, dass es aus rechtlicher oder ggf. auch praktischer Sicht keine Hinweise darauf gibt, dass man notwendiger Weise zwei getrennte Dokumente pflegen muss. Er betont die Möglichkeit, dass „d*ie Datenschutz-Folgenabschätzung im Rahmen eines umfassenderen Datenschutzkonzeptes vorgenommen werden kann. Möglich seien auch separate Dokumente, wobei es dann sinnvoll sei, dass aufeinander Bezug genommen wird.* (Kap. 11.4)

Klaus Pommerening schlägt als „Interner Berichterstatter“ der TMF-AG Datenschutz für das NARSE vor, *„die DSFA evtl. als Anhang auszugliedern, damit nicht bei kleinen Änderungen der Risikobewertung das ganze DS-Konzept samt Votum ungültig wird.“*

Vorgehen beim NARSE

- ☐ Die verantwortlichen Autoren für das Datenschutzkonzept (DSK) und die Datenschutz-Folgenabschätzung („Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten; DSFA“) gehen von einer sehr großen Überschneidung der Anforderungen von DSK und DSFA aus. Beide fordern mit teilweise geringfügig unterschiedlichen Begriffendie Beschreibung der Verarbeitungsvorgänge,
- ☐ die Feststellung von Risiken für Betroffenenrechte,
- ☐ Interessenabwägungen (einschließlich der Berufung auf Rechtsgrundlagen) und
- ☐ die Beschreibung von technischen und organisatorischen Abhilfemaßnahmen.

Während der Hauptteil des DSK als Fließtext formuliert ist, wird die tabellarische DSFA als kommentierte Liste der Verarbeitungsvorgänge dargestellt. Die Tabelle beruht auf einer Liste von Verarbeitungsvorgängen aus dem TMF-Bericht „Von der Evaluierung zur Konsolidierung: Anforderungen an Kohortenstudien und Register-IT (KoRegIT)“ aus dem Jahre 2015. In dem TMF-Bericht liegt eine hierarchische Gliederung in „Phasen“, „Top-Level-Aufgaben“ und „Use Cases“ vor, die im Prinzip übernommen wird. Allerdings erfolgt eine Umbenennung der „Top-Level-Aufgaben“ in „Verarbeitungsgruppen“ und der „Use Cases“ in „Verarbeitungsvorgänge“.

In der DSFA-Tabelle wird die Betrachtung der Risiken, die es durch Abwehrmaßnahmen zu bewältigen gilt, auf die Gefährdung der sieben Gewährleitungsziele des Standarddatenschutzmodells der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Datenschutzkonferenz DSK) fokussiert:

(1) Datenminimierung
(2) Verfügbarkeit
(3) Integrität
(4) Vertraulichkeit
(5) Nichtverkettung
(6) Transparenz
(7) Intervenierbarkeit

Die Technischen und Organisatorischen Schutzmaßnahmen, hier DSGVO-konform „Abhilfemaßnahmen“ genannt, werden mit Verweis auf das vorliegende Datenschutzkonzept benannt, aber in der Version 1.0, die sich auf den initialen Betrieb des NARSE mit manueller Datenerfassung über EDC-Clients bezieht, noch nicht ausführlich beschrieben.

Es ist vorgesehen, im Zuge der schrittweisen Weiterentwicklung des NARSE, bei der der Anschluss von Satellitendokumentationen (angestrebte Ausbauphase 2) und die Datenübernahme aus den Datenintegrationszentren der Universitätsmedizin (angestrebte Ausbauphase 3) hervorgehoben werden kann, das DSK und die angehängte Tabellarische DSFA mit gleicher Versionierung synchronisiert fortzuschreiben.

Allerdings erhält die Versionsnummer der angehängten Tabellarischen DSFA beginnend mit „a“ einen kleinen Buchstaben als Suffix, so dass Anpassungen der Tabellarischen DSFA auch zwischenzeitlich erfolgen können, wenn dies notwendig erscheint.

Exkurs II

Datenschutzkonzept und DSFA als kontinuierlicher Prozess

Das Berliner Landesdatenschutzgesetz fordert in § 26 die Wiederholung der *„Ermittlung* [und Dokumentation] *der Maßnahmen in angemessenen Abständen“*. Anpassungen des Datenschutzkonzeptes sollen *„Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken“* erfolgen.

Im gleichen Sinn hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) im Kurzpapier Nr. 5 mit dem Titel „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“ [27] die Interpretation erarbeitet, dass es sich bei der Abfassung einer DSFA nicht um einen einmaligen Vorgang handelt.

Es wird ausgeführt: „Sollten sich z.B. neue Risken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderung im Verfahren ergeben die in der DSFA bisher nicht berücksichtigt wurden, so ist die DSFA zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Prüfung und Anpassung empfohlen.

[27] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf

Dieses Kurzpapier dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Abbildung 1: Iterativ-zyklischer Prozess der Anpassung der DSFA

Diese Interpretation trifft beim NARSE mit der Absicht zusammen, eine kontinuierliche Entwicklung der Datenerhebung, der Datenimporte und des Erfahrungsaustausches zu betreiben. Wie bereits einleitend vermerkt, sind folgende Aufbau- und Ausbauphasen vorgemerkt:

- Phase 1: Manuelle Datenerfassung über die web-basierte OSSE-Benutzerschnittstelle (OSSE EDC) (~ 2023)
- Phase 2: Anschluss von NARSE-kompatiblen sekundären EDC-Systemen oder Betroffenendokumentationen (~2023/24)
- Phase 3: Datenübermittlung aus unabhängigen Datenbeständen, z.B. Datenintegrationszentren (~2024/25)

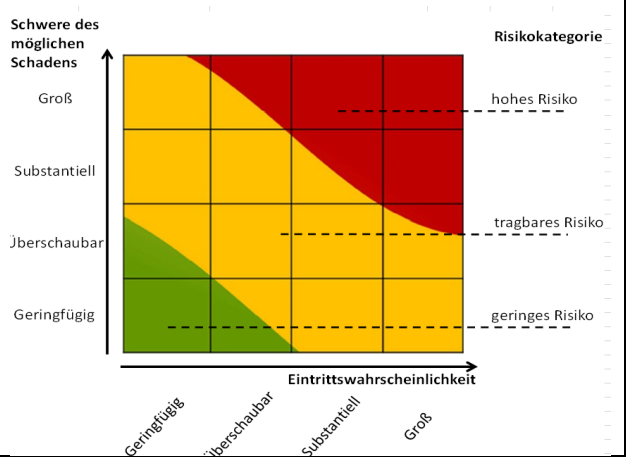
9.2 DSFA-Tabelle mit Verarbeitungsrubriken (Top-Level-Aufgaben) und Verarbeitungsvorgängen (Use Cases)

Die „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten“ orientiert sich an der Beschreibung der Verarbeitungsrubriken (Top-Level-Aufgaben, VR=TL) und Verarbeitungsvorgänge (Detailaufgaben, Use Cases, VV=UC) des TMF-Projektes KoRegIT[28].

Die initiale Folgenabschätzung beschränkt sich auf die Verarbeitungsrubriken (Top-Level-Aufgaben) der Phase 1 des NARSE-Aufbaus (= Erhebung über Web-Clients des Zentralsystems) fokussiert auf die sieben Gewährleistungsziele des Standarddatenschutzmodells der Datenschutzkonferenz des Bundes und Länder und die darin abgebildeten zentralen Datenschutzanforderungen der DSGVO.

Im Zuge des Aufbaus des NARSE und des iterativ-zyklischen DSFA-Vorgehens können einzelne Detailaufgaben und ihre Risiken stärkere Beachtung finden, was sich in der weiteren Ausgestaltung der DSFA niederschlagen wird.

Die Kategorisierung der Risiken orientiert sich am DSFA-Entwurf der TMF-AG Datenschutz (Stand November 2022)[29].

Die sieben **Gewährleistungsziele des Standarddatenschutzmodells** sind:	**Schweregrade des möglichen Schadens**	**Eintrittswahrscheinlichkeiten**	**Risikomatrix**
(1) Datenminimierung (2) Verfügbarkeit (3) Integrität (4) Vertraulichkeit (5) Nichtverkettung (6) Transparenz (7) Intervenierbarkeit	(1) Geringfügig (2) Überschaubar (3) Substantiell (4) Groß	(1) Geringfügig (2) Überschaubar (3) Substantiell (4) Groß	

[28] Aufbauend auf: Claudia Michalik M.A., Dipl.-Inform. Med. Sylvie Ngouongo, Prof. Dr. med. Jürgen Stausberg 2015: Von der Evaluierung zur Konsolidierung: Anforderungen an Kohortenstudien und Register-IT (KoRegIT). Anforderungskatalog. Version 1.0; Januar 2015. © TMF e.V.

[29] TMF AG Datenschutz 2022: DSFA Template

Tabelle 1: Tabelle der NARSE-Verarbeitungsrubriken und Verarbeitungsvorgänge mit Risikoanalyse und Abhilfemaßnahmen

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
3. Betrieb / Umsetzung								
145	**TL= VR**	**TL022**	**Probandenmanagement** Details zur Verarbeitungsrubrik Probandenmanage-ment finden sich in der nachfolgenden Auflistung der Verarbeitungsvorgänge [Use Case].	(1) Gef. Datenminimier. **(2) Gef. Verfügbarkeit** **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Verfügbarkeit** c. Datenerhebungskommunikation (ZSE, Krankenhäuser, Niedergelassene, Patienten-gruppen, weitere) d. proaktive Entwicklung der Datenzugänge (z.B. Satellitendokum.) e. proaktive Probandenkommunikation f. Gewährleistung der Verfügbarkeit und Be-lastbarkeit der Server durch Dienstleister (Hetzner TOMs) g. regelmäßige Backups entsprechend eines Backup-Konzepts (OSSE TOMs 5b) **Spez. TOM wg. Vertraulichkeit** h. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen i. Informationelle Gewaltenteilung mit Ver-trauensstelle (UTHS) j. Pseudonymisierung und Trennung von I-DAT und MDAT k. Zutritts- und Zugangskontrolle zu Servern (Hetzner TOMs) l. Zugangskontrolle: Authentifizierung in OSSE-Software mit Passwort + 2FA (OSSE TOMs 3b) m. Zugriffskontrolle innerhalb der OSSE-Software über modulares Berechtigungs-konzept (OSSE TOMs 3c) **Spez. TOM wg. Integrität**	Über-schaubar	Über-schaubar	**Tragbares Risiko**

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
					n. Protokollierung aller Änderungen inner-halb der OSSE-Software (OSSE TOMs 4b) o. Dokumentation aller manuellen Änderun-gen in der OSSE-Datenbank (OSSE TOMs 4b)			
146	UC=VV	UC0080	Informationsmaterial an potentielle Probanden versenden		Siehe TOM zu Verarbeitungsrubrik TL022			
147	UC=VV	UC0081	Eignung potentieller Probanden prüfen		Siehe TOM zu Verarbeitungsrubrik TL022			
148	UC=VV	UC0084	Probanden aufklären und Einwilligungen einholen		Siehe TOM zu Verarbeitungsrubrik TL022			
149	UC=VV	UC0250	Screeningliste führen		Siehe TOM zu Verarbeitungsrubrik TL022			
150	UC=VV	UC0179	Probanden einschließen		Siehe TOM zu Verarbeitungsrubrik TL022			
151	UC=VV	UC0085	Probandenpass erstellen		Siehe TOM zu Verarbeitungsrubrik TL022			
152	UC=VV	UC0075	Probandenpass ausgeben		Siehe TOM zu Verarbeitungsrubrik TL022			
~~153~~	~~UC=VV~~	~~UC0251~~	~~Dezentrale Probandenliste führen~~		~~Siehe TOM zu Verarbeitungsrubrik TL022~~			
154	UC=VV	UC0244	Zentrale Probandenliste führen		Siehe TOM zu Verarbeitungsrubrik TL022			
155	UC=VV	UC0100	Widerruf einer Einwilligungserklärung bearbeiten		Siehe TOM zu Verarbeitungsrubrik TL022			
156	UC=VV	UC0235	Einwilligungserklärung des Probanden modifizieren		Siehe TOM zu Verarbeitungsrubrik TL022			
157	**TL=VR**	**TL037**	**Unterstützung und Betreuung von Probanden**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen d. Rekontaktierung von Probanden nur mit Opt-in Einwilligung unter Einbindung der UTHS	Über-schaubar	Über-schaubar	**Tragbares Risiko**
158	UC=VV	UC0070	Termine mit Probanden vereinbaren		Siehe TOM zu Verarbeitungsrubrik TL037			
159	UC=VV	UC0071	Benachrichtigung bei Terminverschiebung erstellen		Siehe TOM zu Verarbeitungsrubrik TL037			
160	UC=VV	UC0073	Probanden auf Basis vereinbarter Termine einbestellen		Siehe TOM zu Verarbeitungsrubrik TL037			
161	UC=VV	UC0086	Zentrumswechsel eines Probanden verarbeiten		Siehe TOM zu Verarbeitungsrubrik TL037			
162	UC=VV	UC0206	Probanden Über Befunde informieren		Siehe TOM zu Verarbeitungsrubrik TL037			
163	UC=VV	UC0207	Informationsveranstaltung für Probanden ausrichten		Siehe TOM zu Verarbeitungsrubrik TL037			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
164	TL= VR	TL021	Datenerhebung und Datenerfassung	**(1) Gef. Datenminimier.** **(2) Gef. Verfügbarkeit** **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Datenminimierung** c. Erfassung eines abgestimmten Minimal-datensatzes d. Erfassung von genetischen Informationen nur mit Opt-in Einwilligung **Spez. TOM wg. Verfügbarkeit** e. Ergonomie und Usability der Datenerfas-sung f. proaktive Entwicklung der Datenzugänge (z.B. Satellitendokum.) g. Gewährleistung der Verfügbarkeit und Belastbarkeit der Server durch Dienstleister (Hetzner TOMs) h. regelmäßige Backups entsprechend eines Backup-Konzepts (OSSE TOMs 5b) **Spez. TOM wg. Integrität** i. Identitätsmanagement mit Vertrauens-stelle UTHS Dresden j. Protokollierung aller Änderungen inner-halb der OSSE-Software in Audit Trail (OSSE TOMs 4b) k. Dokumentation aller manuellen Änderun-gen in der OSSE-Datenbank (OSSE TOMs 4b) l. Datenübertragung zwischen Browser und Server mit sicherer Verschlüsselung (OSSE TOMs 4a) **Spez. TOM wg. Vertraulichkeit** m. informationelle Gewaltenteilung mit UTHS n. Pseudonymisierung und Trennung von I-DAT und MDAT	Über-schaubar	Über-schaubar	**Tragbares Risiko**

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
					o. Zutritts- und Zugangskontrolle zu Servern (Hetzner TOMs) p. Zugangskontrolle: Authentifizierung in OSSE-Software mit Passwort + 2FA (OSSE TOMs 3b) q. Zugriffskontrolle innerhalb der OSSE-Software über modulares Berechtigungskonzept (OSSE TOMs 3c) r. Trennungskontrolle innerhalb der OSSE-Software über modulares Berechtigungskonzept (OSSE TOMs 3d)			
165	UC=VV	UC0088	Daten erheben		Siehe TOM zu Verarbeitungsrubrik TL021			
~~166~~	~~UC=VV~~	~~UC0089~~	~~Daten importieren~~		~~Siehe TOM zu Verarbeitungsrubrik TL021~~			
167	UC=VV	UC0090	Probanden registrieren		Siehe TOM zu Verarbeitungsrubrik TL021			
~~168~~	~~UC=VV~~	~~UC0208~~	~~Probanden zu Kollektiv zuordnen~~		~~Siehe TOM zu Verarbeitungsrubrik TL021~~			
169	UC=VV	UC0092	Probandendatensatz bearbeiten		Siehe TOM zu Verarbeitungsrubrik TL021			
170	UC=VV	UC0093	Probandendatensatz deaktivieren/sperren		Siehe TOM zu Verarbeitungsrubrik TL021			
171	UC=VV	UC0094	Probandendatensatz endgültig löschen		Siehe TOM zu Verarbeitungsrubrik TL021			
~~172~~	~~UC=VV~~	~~UC0095~~	~~Visiten anzeigen~~		~~Siehe TOM zu Verarbeitungsrubrik TL021~~			
~~173~~	~~UC=VV~~	~~UC0096~~	~~Visite anlegen~~		~~Siehe TOM zu Verarbeitungsrubrik TL021~~			
~~174~~	~~UC=VV~~	~~UC0099~~	~~Visite löschen~~		~~Siehe TOM zu Verarbeitungsrubrik Nr. 164~~			
175	UC=VV	UC0242	Probandenberichte implementieren		Siehe TOM zu Verarbeitungsrubrik Nr. 164			
176	**TL=VR**	**TL023**	**Monitoring**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen	Über-schaubar	Gering-fügig	**Geringes Risiko**
177	UC=VV	UC0101	Monitore schulen		Siehe TOM zu Verarbeitungsrubrik TL023			
178	UC=VV	UC0102	Monitoring vor Ort vorbereiten		Siehe TOM zu Verarbeitungsrubrik TL023			
179	UC=VV	UC0103	Monitoring vor Ort durchführen		Siehe TOM zu Verarbeitungsrubrik TL023			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
180	UC=VV	UC0104	Zentrales Monitoring durchführen		Siehe TOM zu Verarbeitungsrubrik TL023			
181	UC=VV	UC0105	Monitoringbericht erstellen		Siehe TOM zu Verarbeitungsrubrik TL023			
182	UC=VV	UC0209	Monitoringbericht abstimmen		Siehe TOM zu Verarbeitungsrubrik TL023			
183	UC=VV	UC0210	Monitoringbericht an Zentrum versenden		Siehe TOM zu Verarbeitungsrubrik TL023			
184	UC=VV	UC0106	Umsetzung der Maßnahmen zur Behebung oder Vorbeugung von Auffälligkeiten kontrollieren		Siehe TOM zu Verarbeitungsrubrik TL023			
185	**TL=VR**	**TL024**	**Bereitstellung von probandenbezogenen Informationen**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen d. Rekontaktierung von Probanden nur mit Opt-in Einwilligung unter Einbindung der UTHS	Über-schaubar	Gering-fügig.	**Geringes Risiko**
186	UC=VV	UC0108	Befunddokumentation generieren		Siehe TOM zu Verarbeitungsrubrik TL024			
187	UC=VV	UC0109	Gutachten/Briefe erstellen		Siehe TOM zu Verarbeitungsrubrik TL024			
188	UC=VV	UC0110	Dokument verschicken		Siehe TOM zu Verarbeitungsrubrik TL024			
189	**TL=VR**	**TL025**	~~**Abrechnung mit Erhebungszentren und Probanden**~~ **(zurückgestellt)**	~~(1) Gef. Datenminimier.~~ ~~(2) Gef. Verfügbarkeit~~ ~~(3) Gef. Integrität~~ ~~(4) Gef. Vertraulichkeit~~ ~~(5) Gef. Nichtverkettung~~ ~~(6) Gef. Transparenz~~ ~~(7) Gef. Intervenierbark.~~	~~**Allgemeine TOM**~~ ~~a. Umsetzung durch geschultes Personal~~ ~~b. DV in Geschützten Räumen~~ ~~**Spez. TOM wg. Vertraulichkeit**~~ ~~c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen~~	~~Gering-fügig.~~	~~Über-schaubar~~	~~**Geringes Risiko**~~
190	UC=VV	UC0113	~~Umfang und Qualität der von den Zentren erbrachten Leistungen prüfen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL025~~			
191	UC=VV	UC0114	~~Abrechnung erstellen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL025~~			
192	UC=VV	UC0115	~~Abrechnung verschicken~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL025~~			
193	UC=VV	UC0116	~~Auszahlungen prüfen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL025~~			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
194	TL=VR	TL045	~~Abrechnung von Dienstleistungen~~ (Zurückgestellt)	~~(1) Gef. Datenminimier.~~ ~~(2) Gef. Verfügbarkeit~~ ~~(3) Gef. Integrität~~ ~~(4) Gef. Vertraulichkeit~~ ~~(5) Gef. Nichtverkettung~~ ~~(6) Gef. Transparenz~~ ~~(7) Gef. Intervenierbark.~~	~~Allgemeine TOM~~ ~~a. Umsetzung durch geschultes Personal~~ ~~b. DV in Geschützten Räumen~~ ~~Spez. TOM wg. Vertraulichkeit~~ ~~c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen~~	~~Gering-fügig.~~	~~Über-schaubar~~	~~Geringes Risiko~~
~~195~~	~~UC=VV~~	~~UC0213~~	~~Abrechnung erstellen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL045~~			
~~196~~	~~UC=VV~~	~~UC0214~~	~~Abrechnung verschicken~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL045~~			
~~197~~	~~UC=VV~~	~~UC0215~~	~~Zahlungseingang prüfen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL045~~			
198	TL=VR	TL026	Datenmanagement (Organisation und Pflege der Daten)	(1) Gef. Datenminimier. **(2) Gef. Verfügbarkeit** **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	Allgemeine TOM a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen	Über-schaubar.	Gering-fügig	Geringes Risiko
199	UC=VV	UC0122	Datensicherheit entsprechend dem Datenschutzkonzept umsetzen		Siehe TOM zu Verarbeitungsrubrik TL026			
200	UC=VV	UC0118	Datenbestand einfrieren		Siehe TOM zu Verarbeitungsrubrik TL026			
201	UC=VV	UC0119	Daten exportieren und bereitstellen		Siehe TOM zu Verarbeitungsrubrik TL026			
202	UC=VV	UC0121	Zentrales Monitoring unterstützen		Siehe TOM zu Verarbeitungsrubrik TL026			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
4. Betrieb / Nutzung								
204	**TL=VR**	**TL028**	**Studienunterstützung**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen d. Prüfung und Freigabe durch Data Access Committee (erg. durch EK und DSB) e. reguläre Beschränkung auf Daten mit Einwilligung f. reguläre Beschränkung auf Daten auf vorgegebene Nutzungszwecke g. reguläre Beschränkung auf Auswertung pseudonymisierter Daten **Spez. TOM wg. Integrität** h. Export aus OSSE-Software in pseudonymisierter Form (OSSE TOMs 4a) i. weitere Verarbeitung und Bereitstellung der Daten nach SOPs mit Dokumentation für Nachvollziehbarkeit	Über-schaubar	Über-schaubar	**Tragbares Risiko**
205	UC=VV	UC0127	Studienanfragen prüfen		Siehe TOM zu Verarbeitungsrubrik TL028			
206	UC=VV	UC0128	Feasibility-Analysen erstellen		Siehe TOM zu Verarbeitungsrubrik TL028			
207	UC=VV	UC0129	Daten bereitstellen		Siehe TOM zu Verarbeitungsrubrik TL028			
208	UC=VV	UC0131	Berichterstattung/statistische Analyse unterstützen		Siehe TOM zu Verarbeitungsrubrik TL028			
209	UC=VV	UC0224	Zentren potentielle Probanden melden		Siehe TOM zu Verarbeitungsrubrik TL028			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
210	**TL=VR**	**TL029**	**Statistische Analyse**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** **(5) Gef. Nichtverkettung** (6) Gef. Transparenz **(7) Gef. Intervenierbark.**	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Freigabe nur durch Data Access Committee **Spez. TOM wg. Integrität** d. weitere Verarbeitung und Bereitstellung der Daten nach SOPs mit Dokumentation für Nachvollziehbarkeit	Über-schaubar	Über-schaubar	**Tragbares Risiko**
211	UC=VV	UC0134	Daten für Analyse aufbereiten		Siehe TOM zu Verarbeitungsrubrik TL029			
212	UC=VV	UC0135	Analyse durchführen		Siehe TOM zu Verarbeitungsrubrik TL029			
213	UC=VV	UC0136	Analysebericht erstellen		Siehe TOM zu Verarbeitungsrubrik TL029			
214	UC=VV	UC0139	Zentrenbezogene Auswertung erstellen		Siehe TOM zu Verarbeitungsrubrik TL029			
215	**TL=VR**	**TL030**	**Berichterstattung**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen d. Veröffentlichung von Daten nur in aggregierter Form	Über-schaubar	Über-schaubar	**Tragbares Risiko**
216	UC=VV	UC0141	Berichte vorbereiten		Siehe TOM zu Verarbeitungsrubrik TL030			
217	UC=VV	UC0142	Berichte erstellen		Siehe TOM zu Verarbeitungsrubrik TL030			
218	UC=VV	UC0143	Berichte abstimmen		Siehe TOM zu Verarbeitungsrubrik TL030			
219	UC=VV	UC0237	Berichte finalisieren		Siehe TOM zu Verarbeitungsrubrik TL030			
220	UC=VV	UC0144	Berichte veröffentlichen		Siehe TOM zu Verarbeitungsrubrik TL030			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
221	**TL=VR**	**TL031**	**Organisation von Publikationen und Präsentationen**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
222	UC=VV	UC0145	Relevante Journals und Kongresse recherchieren		Siehe TOM zu Verarbeitungsrubrik TL031			
223	UC=VV	UC0146	Publikationen und Präsentationen planen		Siehe TOM zu Verarbeitungsrubrik TL031			
224	UC=VV	UC0148	Autorenschaft abstimmen		Siehe TOM zu Verarbeitungsrubrik TL031			
225	UC=VV	UC0147	Publikationen und Präsentationen erstellen		Siehe TOM zu Verarbeitungsrubrik TL031			
226	UC=VV	UC0226	Publikationen und Präsentationen abstimmen		Siehe TOM zu Verarbeitungsrubrik TL031			
227	**TL=VR**	**TL033**	**Datenintegration, Datenzusammenführung** Ausarbeitung folgt vor der Inangriffnahme der Stufe 2 des NARSE: Import aus Satellitendokumentationen.	(1) Gef. Datenminimier. **(2) Gef. Verfügbarkeit** **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** **(5) Gef. Nichtverkettung** **(6) Gef. Transparenz** **(7) Gef. Intervenierbark.**	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
228	UC=VV	UC0249	Anfragen nach Datenintegration oder Datenzusammenführung prüfen		Siehe TOM zu Verarbeitungsrubrik TL033			
229	UC=VV	UC0152	Datenkompatibilität prüfen		Siehe TOM zu Verarbeitungsrubrik TL033			
230	UC=VV	UC0153	Datenformat abstimmen		Siehe TOM zu Verarbeitungsrubrik TL033			
231	UC=VV	UC0154	Datenintegration/Datenzusammenführung durchführen		Siehe TOM zu Verarbeitungsrubrik TL033			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
232	**TL= VR**	**TL046**	**Unterstützung der Patientenversorgung**	(1) Gef. Datenminimier. **(2) Gef. Verfügbarkeit** (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Verfügbarkeit** c. vollständige Minimaldatensätze d. breite Kommunikation der Registernut-zung d. Standardisierung von Satellitendokumen-tation **Spez. TOM wg. Vertraulichkeit** e. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen f. Informationelle Gewaltenteilung	Über-schaubar	Über-schaubar	**Tragbares Risiko**
233	UC=VV	UC0218	Qualitätssicherung unterstützen		Siehe TOM zu Verarbeitungsrubrik TL046			
234	UC=VV	UC0219	Diagnose und Therapie unterstützen		Siehe TOM zu Verarbeitungsrubrik TL046			
5. Betrieb / Weiterentwicklung								
236	**TL= VR**	**TL032**	**Weiterentwicklung Register/Kohorte**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
237	UC=VV	UC0149	Aktualisierungen und Projekte abstimmen		Siehe TOM zu Verarbeitungsrubrik TL032			
238	UC=VV	UC0245	Change Request bearbeiten		Siehe TOM zu Verarbeitungsrubrik TL032			
239	UC=VV	UC0247	Datenbank versionieren		Siehe TOM zu Verarbeitungsrubrik TL032			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
6. Abschluss								
241	**TL= VR**	**TL034**	**Archivierung**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
242	UC=VV	UC0157	Archivierung der Datenbank vorbereiten		Siehe TOM zu Verarbeitungsrubrik TL034			
243	UC=VV	UC0158	Abschließende Datenexporte durchführen		Siehe TOM zu Verarbeitungsrubrik TL034			
244	UC=VV	UC0159	Daten bzw. Dokumente archivieren		Siehe TOM zu Verarbeitungsrubrik TL034			
245	UC=VV	UC0160	Auf archivierte Dokumente zugreifen		Siehe TOM zu Verarbeitungsrubrik TL034			
246	UC=VV	UC0161	Archivierte Dokumente vernichten		Siehe TOM zu Verarbeitungsrubrik TL034			
247	**TL= VR**	**TL035**	**Vernichtung der Daten, Anonymisierung**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
248	UC=VV	UC0162	Daten vernichten		Siehe TOM zu Verarbeitungsrubrik TL035			
249	UC=VV	UC0163	Daten anonymisieren		Siehe TOM zu Verarbeitungsrubrik TL035			
250	UC=VV	UC0246	Daten an Nachfolge-Organisation weitergegeben		Siehe TOM zu Verarbeitungsrubrik TL035			
251	UC=VV	UC0164	Daten deaktivieren		Siehe TOM zu Verarbeitungsrubrik TL035			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
225	**TL= VR**	**TL036**	**Close Out**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
253	UC=VV	UC0165	Schließung eines Zentrums vorbereiten		Siehe TOM zu Verarbeitungsrubrik TL036			
254	UC=VV	UC0166	Zentrum schließen		Siehe TOM zu Verarbeitungsrubrik TL036			
255	UC=VV	UC0167	Schließung Zentrum nachbereiten und dokumentieren		Siehe TOM zu Verarbeitungsrubrik TL036			