Schablone zur Erstellung eines Datenschutzkonzepts für ein OSSE-Register

Dr. Marita Muscholl\*\*, Martin Lablans\*\*, Andreas Borg\*\*, Prof. Dr. Frank Ückert\*\*, Prof. Dr. TOF Wagner\*

\*Universitätsklinikum Frankfurt am Main

Abteilung Pneumologie

69590 Frankfurt am Main

\*\*Universitätsmedizin der Johannes Gutenberg-Universität Mainz

Institut für Medizinische Biometrie, Epidemiologie und Informatik

55101 Mainz

Hinweise zur Nutzung der Schablone

Ziel der Schablone zum Datenschutzkonzept für OSSE-Register ist es, die Erstellung eines individuellen Datenschutzkonzepts beim Einsatz der OSSE-Registersoftware zu erleichtern. Die Schablone berücksichtigt alle Komponenten, die Teil der OSSE-Registersoftware sind oder im Zusammenhang mit dieser verwendet werden, sowie die Datenflüsse zwischen diesen Komponenten. Maßnahmen zum Datenschutz, die Teil der Softwarefunktionen sind, werden beschrieben. Zu ergänzende Informationen zu organisatorischen Abläufen oder zu darüber hinaus verwendeten, eigenen IT-Komponenten sind im Text markiert. Technische Maßnahmen, die nicht Teil der Software sind, sind als Vorschläge zu sehen.

### Markierungen und ihre Bedeutung

* *Stellen im Text, an denen Information zu ergänzen ist oder Platzhalter zu ersetzen sind, sind grau markiert* [*und als Kommentare ggf. in eckige Klammern gesetzt*]
* Abschnitte im Text, für die es je nach den lokalen Gegebenheiten verschiedenen Varianten gibt, sind mit gelb unterlegten Beginn- und Ende-Markierungen geklammert oder, wenn es sich nur um einen Satz handelt, durch eine Markierung am Satzanfang gekennzeichnet:
[*#Beginn* ***Variante n*** *(hier ist die Variante beschrieben)*] … [*#Ende* ***Variante n***]
[*Gilt nur für* ***Variante m***] …
* Hinweise zu einzelnen Abschnitten sind ebenfalls in eckigen Klammern und gelb hinterlegt: [*Dieser Abschnitt soll folgendermaßen bearbeitet werden …*]
* CAVE: Textänderungen außerhalb der markierten Stellen können das Konzept datenschutzrechtlich inhaltlich verändern. Die Abweichung vom zugrundeliegenden TMF-Datenschutzkonzept[[1]](#footnote-2) führt mit großer Wahrscheinlichkeit zu einem Verlust der prinzipiellen Anerkennung durch alle bundesdeutschen Landesdatenschützer.

### Vorgehen bei der Bearbeitung

1. Ersetzen Sie in der Schablone den Platzhalter „OSSE-Register für „Seltene Erkrankung X““ durch den Namen des geplanten Registers.
2. Beantworten Sie sich folgende Fragen, die für die Auswahl der Varianten oder zu ergänzenden Informationen notwendig sind:
3. *Wer ist der Träger (üblicherweise also „Besitzer“) des Registers?*
4. *Welche Institution betreibt das OSSE-Register (hat üblicherweise die notwendige zentrale Hardware unter seiner Kontrolle)?*
5. *Welche Institutionen sind an dem Vorhaben beteiligt (erfassen Daten in das Register)?*
6. *Welche Daten werden in das OSSE-Register erfasst (z.B. Gewicht, Geburtsdatum, Diagnose als Orphacode)? (🡪 ergibt einen Anhang)*
7. *Wo ist das Identitätsmanagement zur Pseudonymisierung der Patientendaten angesiedelt und wer betreibt es? (folgende Varianten sind möglich)*
	1. *Es gibt ein Identitätsmanagement, das für alle Register für „Seltene Erkrankung X“ zentral betrieben wird (damit bei Forschungsprojekten mit anderen Registern identische Patienten in verschiedenen Registern erkannt werden können)[[2]](#footnote-3).*
	2. *Für das OSSE-Register für „Seltene Erkrankung X soll ein eigenes Identitätsmanagement betrieben werden.*
	3. *Es wird keine Komponente für das Identitätsmanagement genutzt. Das OSSE-Register wird so konfiguriert, dass es interne Patientenidentifikatoren (PID) vergibt, die ausschließlich am Behandlungsort manuell mit den identifizierenden Daten des Patienten verknüpft werden.*
8. *Welche Rollen gibt es für das Register (z.B. „Dokumentar“, „behandelnder Arzt“)? Mit welchen Zugriffsrechten müssen diese jeweils ausgestattet sein (z.B. „Lesen von xyz“, „Schreiben von abc“)?*
9. *Wie sieht der Ablauf der manuellen Dateneingabe aus (welche Zustände, z.B. „in Bearbeitung“, „abgeschlossen“, „validiert“) kann ein Eingabeformular haben und welche Benutzergruppen (Rollen) dürfen es bearbeiten)?*
10. *Werden Daten aus klinischen Systemen importiert?*
	1. *Falls ja, welche Daten aus welchen Systemen? (🡪 ergibt einen Anhang)*
11. *Werden Daten zu Biomaterialproben in das OSSE-Register importiert (und welche)?*
	1. *Falls ja, □ aus einer Biomaterialbank? □ direkt von der Probenquelle?*
12. Ersetzen Sie die Platzhalter und ergänzen Sie die abgefragten Informationen und Anhänge.
13. Löschen Sie überflüssige Abschnitte.
14. Lesen Sie dabei die gesamte Schablone sorgfältig durch und passen Sie die Texte hinsichtlich Ihrer spezifischen Umgebung (IT-Infrastruktur, Organisation, etc.) an.
15. Löschen Sie die Kommentare und Markierungen.
16. Aktualisieren Sie das Inhaltsverzeichnis.

# Logo_UKF_-_rgb

OSSE-Register für „Seltene Erkrankung X“

Datenschutzkonzept[[3]](#footnote-4)

Projekt OSSE-Register für „Seltene Erkrankung X“

Autoren [*Autor(en)*]

 [*Institution(en)*]

[*Träger (Name und Adresse)*]

Version [*Datum*]

Inhalt

[1. Einleitung 6](#_Toc395700532)

[1.1 Zielsetzung 6](#_Toc395700533)

[1.2 Überblick über die Datenverarbeitung 6](#_Toc395700534)

[1.3 Rechtsgrundlage 8](#_Toc395700535)

[1.4 Träger 8](#_Toc395700536)

[2. Datenverarbeitende Komponenten 8](#_Toc395700537)

[2.1 OSSE-Register 8](#_Toc395700538)

[Komponenten und Funktionen 8](#_Toc395700539)

[Workflow 9](#_Toc395700540)

[Benutzer, Rollen und Rechte 9](#_Toc395700541)

[2.2 Identitätsmanagement 9](#_Toc395700542)

[Pseudonyme 9](#_Toc395700543)

[Manuelles Linken 10](#_Toc395700544)

[2.3 Biomaterialbank 10](#_Toc395700545)

[2.4 Teiler (OSSE-Share) 10](#_Toc395700546)

[2.5 Metadaten-Repository 11](#_Toc395700547)

[2.6 Registerverzeichnis (Registry of Registries) 11](#_Toc395700548)

[3. Datenverarbeitende Prozesse 11](#_Toc395700549)

[3.1 Manuelle Dateneingabe 11](#_Toc395700550)

[Anlegen eines Patienten 11](#_Toc395700551)

[Auswahl von Patienten, Dateneingabe 11](#_Toc395700552)

[Workflowunterstützung 11](#_Toc395700553)

[Manuelle Freigabe von Datensätzen 11](#_Toc395700554)

[3.2 Datenimport 12](#_Toc395700555)

[3.3 Pseudonymisierung 12](#_Toc395700556)

[Manuelle Patientenregistrierung 12](#_Toc395700557)

[Pseudonymisierung beim Datenimport 13](#_Toc395700558)

[Schlüsselerzeugung und Schlüsselverwaltung 13](#_Toc395700559)

[3.4 Import von Biomaterialdaten 14](#_Toc395700560)

[3.5 Datenexport 17](#_Toc395700561)

[3.6 Dezentrale Suche 17](#_Toc395700562)

[3.7 Hochladen von Informationen an das Registerverzeichnis 18](#_Toc395700563)

[4. Organisatorische Rahmenbedingungen 18](#_Toc395700564)

[4.1 Betrieb der Komponenten 18](#_Toc395700565)

[4.2 Teilnehmende Forscher 18](#_Toc395700566)

[4.3 Mitgliederversammlung 19](#_Toc395700567)

[4.4 Registerleitung 19](#_Toc395700568)

[4.5 Registerausschuss 19](#_Toc395700569)

[4.6 Zugriff durch Systemadministratoren 19](#_Toc395700570)

[5. Maßnahmen zum Datenschutz 19](#_Toc395700571)

[5.1 Informationelle Gewaltenteilung 19](#_Toc395700572)

[5.2 Autorisierung und Authentifizierung 20](#_Toc395700573)

[Autorisierung von Benutzern 20](#_Toc395700574)

[Autorisierung von Komponenten 20](#_Toc395700575)

[Authentifizierung von Benutzern 20](#_Toc395700576)

[Authentifizierung von Komponenten 20](#_Toc395700577)

[5.3 Maßnahmen in der IT-Infrastruktur 20](#_Toc395700578)

[Sicherheit der gespeicherten Daten 20](#_Toc395700579)

[Sicherheit der Kommunikation 20](#_Toc395700580)

[Protokollierung 21](#_Toc395700581)

[6. Wahrung von Betroffenenrechten 21](#_Toc395700582)

[6.1 Aufklärung und Einwilligung 21](#_Toc395700583)

[6.2 Auskunft über gespeicherte Daten 21](#_Toc395700584)

[6.3 Widerruf, Löschung, Anonymisierung 22](#_Toc395700585)

[6.4 Dauer der Speicherung 22](#_Toc395700586)

[7. Anhang 23](#_Toc395700587)

[7.1 Patienteneinwilligung OSSE-Register 23](#_Toc395700588)

[7.2 Datensätze 24](#_Toc395700589)

[Registerdefinition 24](#_Toc395700590)

[Identifizierende Daten 24](#_Toc395700591)

[7.3 Daten und Quellsysteme für den Datenimport 25](#_Toc395700592)

# Einleitung

## Zielsetzung

[*Der folgende Abschnitt stellt einen Formulierungsvorschlag dar und sollte ersetzt oder angepasst und präzisiert werden.*]

Vor dem Hintergrund eines Mangels an Wissen über die Seltene Erkrankung X verlangt die ärztliche und gesellschaftliche Verantwortung für die Betroffenen die Beobachtung von Krankheitsverläufen über lange Zeiträume. Nur durch die Forschung in standortübergreifenden Verbünden mit ausreichenden Fallzahlen kann auch bei Seltenen Erkrankungen wie bei der Seltenen Erkrankung X sinnvoll klinisch wie auf dem Gebiet der Grundlagen geforscht werden. Auch für die Versorgung und gesundheitspolitische Planung sind verlässliche Informationen zur Häufigkeit bestimmter Ausprägungsmuster, zum Gesundheitszustand, etc. von größter Wichtigkeit.

Das OSSE-Register für „Seltene Erkrankung X“ hat sich zur Aufgabe gemacht, durch den Aufbau eines Registers die Zusammenführung der Informationen zur Verbesserung der Forschungsvoraussetzungen beizutragen.

Das OSSE-Register für „Seltene Erkrankung X“ kann dazu mit anderen Registern für die Seltene Erkrankung X in einer IT-Infrastruktur vernetzt werden, die es vor allem ermöglicht, Fallzahlen registerübergreifend zu ermitteln, aber auch Probanden für klinische Studien zu rekrutieren oder den Austausch bereits vorliegender Daten für Forschungsfragestellungen zur Auswertung zu unterstützen. Dazu werden in den beteiligten Registern Daten aus der klinischen Dokumentation sowie zu dort vorhandenen Biomaterialproben erhoben und gesammelt. Um diese Daten für die Forschung nutzbar zu machen, stellt das OSSE-Register für „Seltene Erkrankung X“ eine Suchschnittstelle bereit, die ermöglicht

* abzuschätzen, ob für ein Forschungsvorhaben im OSSE-Register für „Seltene Erkrankung X“ genügend Probanden mit den betrachteten Eigenschaften auffindbar sind,
* zu ermitteln, welche Institutionen passende Patienten behandeln oder behandelt haben und
* Anfragen zur Nutzung von medizinischen Daten und Biomaterialproben dieser Patienten für Forschungsvorhaben zu stellen.

Dabei stellt das OSSE-Register für „Seltene Erkrankung X“ sicher, dass die Hoheit über die Verwendung der Daten bei den Registerverantwortlichen bleibt und Daten nur derart ausgetauscht werden, dass durch die Wahl geeigneter Pseudonyme eine Rückidentifizierung der individuellen Patienten auszuschließen ist.

## Überblick über die Datenverarbeitung

Im OSSE-Register für „Seltene Erkrankung X“ werden Daten von Patienten[[4]](#footnote-5), die in den teilnehmenden Kliniken (auch als „Standorte“ bezeichnet) behandelt werden, erhoben und verarbeitet. Die Daten werden auf folgende Weise in das Register erfasst:

[*Unzutreffendes aus den Aufzählungen streichen!*]

* manuell über die web-basierte OSSE-Benutzer-Schnittstelle
* per Datenimport aus vorhandenen Datenverarbeitungssystemen, z.B. aus Krankenhausinformations- und Dokumentationssystemen (siehe 7.3, „Daten und Quellsysteme für den Datenimport“).

Folgende Arten von Daten werden erhoben:

* Identifizierende Daten (IDAT): Sie enthalten demografische Daten (z.B. Name, Geburtsdatum, Geschlecht), die eine eindeutige Identifikation des Patienten erlauben. Sie werden nicht im Register, sondern separat in einer Patientenliste gespeichert.
* Medizinische Daten (MDAT): Dazu gehören alle Daten, die über die Erkrankung und deren Verlauf im Register erfasst werden.
* Daten zu Biomaterialproben (ProbDAT): Das OSSE-Register für die Seltene Erkrankung X enthält auch Daten zu Biomaterial (siehe 3.4 „Import von Biomaterialdaten“)

Genauere Informationen zum Umfang der Daten finden sich im Anhang unter 7.2 „Datensätze“.

Alle Datenfelder, die im Register gespeichert werden, sind in einem für alle Register zentral betriebenen Metadaten-Repository registriert und beschrieben. Die Registerstruktur (Stamm- und Verlaufsdatenformulare) wird mithilfe eines Registereditors dynamisch festgelegt (siehe 7.2 „Datensätze“ – Registerdefinition).

[*#Beginn* ***Variante 1****: Zentrales ID-Management für alle Register für die Seltene Erkrankung X*]

IDAT werden im zentralen ID-Management gespeichert, das von [*hier die Institution angeben, die die Mainzelliste treuhänderisch zentral für alle Register für die Seltene Erkrankung X betreibt*] betrieben wird.

[*#Ende Variante 1*]

[*#Beginn* ***Variante 2****: Lokal betriebenes ID-Management für dieses Register für die Seltene Erkrankung X*]

IDAT werden im ID-Management des OSSE-Registers für „Seltene Erkrankung X“ gespeichert, das von [*hier die Institution angeben, die die Mainzelliste treuhänderisch für dieses Register betreibt*] betrieben wird.

[*#Ende Variante 2*]

[*#Beginn* ***Variante 3****: Manuell geführte Liste von IDAT; in diesem Fall erzeugt OSSE einen PID, der mit den IDAT in der Liste registriert wird*]

Pseudonyme werden beim Anlegen der Patienten vom OSSE-Register erzeugt. IDAT werden lokal an den Standorten manuell verwaltet und dem Pseudonym zugeordnet.

[*#Ende Variante 3*]

Daten im OSSE-Register für „Seltene Erkrankung X“ werden zu Auswertungszwecken mit nicht-rückführbaren Exportpseudonymen exportiert. Das OSSE-Register für „Seltene Erkrankung X“ unterstützt außerdem die „Dezentrale Suche“, eine Anfrage-Infrastruktur, mit der in den vernetzten OSSE-Registern nach definierten Fällen gesucht werden kann. Die Anfrage, bestehend aus einem Exposé zur Fragestellung, den Kontaktdaten des Anfragenden und den Suchkriterien, wird zusammen mit den Ergebnissen der Registerleitung elektronisch-automatisch vorgelegt. Diese hat dann die Möglichkeit, die Anfrage auf inhaltliche Kriterien und rechtliche Zulässigkeit zu prüfen und, falls beides positiv ausfällt, manuell auf diese Anfrage zu antworten und ggf. die Datensätze zu übermitteln. Diese Art der Suche kommt am ehesten einer klassischen schriftlichen Anfrage gleich, nur dass durch die Vernetzung der Register schon geklärt ist, wo eine Anfrage bezüglich geeigneter Datensätze sinnvoll sein kann und die Begutachtung und Beantwortung der Anfrage durch technische Hilfsmittel unterstützt wird. Um die Vergleichbarkeit und die gezielte Abfrage von Dateninhalten in verschiedenen Datenquellen zu ermöglichen, ist das Datenschema des OSSE-Registers mit einer formalen Definition aller Datenfelder verknüpft, die in Form von Metadaten im zentralen Metadaten Repository (MDR) registriert ist.

Eine detaillierte Beschreibung der Komponenten und Prozesse wird in den Abschnitten 2 und 3 gegeben.

## Rechtsgrundlage

Die informierte Einwilligung des Patienten (siehe Abschnitt 6.1 „Aufklärung und Einwilligung“) bildet die Rechtsgrundlage der Datenverarbeitung. Sie nennt explizit die Institutionen und Personen, die festgelegte Datenarten verarbeiten und nutzen dürfen. Auch die Weitergabe von Daten zu Forschungszwecken, die mit einem nicht-rückführbaren Exportpseudonym quasi „anonymisiert“ werden, 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 Patienten gezogen werden können. Die Anfrage an vernetzte OSSE-Registern für „Seltene Erkrankung X“ über die „Dezentrale Suche“ sind datenschutzrechtlich nicht relevant, da sie nur aggregierte Daten zurückliefert (z.B. Anzahl bestimmter Fälle) und Ergebnisse nicht automatisch übermittelt werden. Für die Weitergabe von Daten ist eine Einwilligung erforderlich.

## Träger

Träger des Vorhabens ist [hier den Träger des Vorhabens angeben]

# Datenverarbeitende Komponenten

## OSSE-Register

### Komponenten und Funktionen

Die OSSE-Register-Software dient der Erfassung und Speicherung medizinischer Stamm- und Verlaufsdaten von an Erkrankung X erkrankten Patienten. Datenfelder und Formulare sind extern in einem Metadaten-Repository bzw. Formular-Repository registriert und beschrieben und können auch nach Start des laufenden Vorhaben modifiziert und ergänzt werden.

Die Eingabe der Daten erfolgt an den Standorten über die webbasierte Benutzerschnittstelle; zusätzlich können Daten über Schnittstellen für den Datenimport erfasst werden. Alle Daten werden versioniert gespeichert, d.h. geänderte und gelöschte Werte bleiben in der Datenbank erhalten und können ggf. angezeigt werden.[[5]](#footnote-6)

[*#Beginn* ***Variante 1, Variante 2*** *(Identitätsmanagement mit zentraler oder lokaler Komponente wie in Abschnitt 2.2 definiert):*]

Identifizierende Daten werden nicht in das OSSE-Register, sondern direkt in das Identitätsmanagement erfasst. Die Kommunikation zwischen Identitätsmanagement und OSSE-Register findet über den Webbrowser statt. Für den Benutzer erscheint die Eingabemaske des Identitätsmanagements integriert in die Benutzeroberfläche des OSSE-Registers. Das zurückgelieferte Pseudonym, „PSNOSSE“ (siehe 2.2 „Identitätsmanagement“), wird mit den MDAT gespeichert, aber nicht angezeigt, so dass auch manuell keine Zuordnung der IDAT mit dem PSNOSSE außerhalb des Identitätsmanagements möglich ist. Da medizinische Daten 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 des Patienten abruft und die sicherstellen, dass die Zuordnung zwischen dem PSNOSSE und den IDAT des Patienten außerhalb des Identitätsmanagements nicht bekannt wird.

[*#Ende Variante 1, Variante 2*]

[*#Beginn* ***Variante 3*** *(Identitätsmanagement mit manuell geführter Liste)*] Identifizierende Daten werden nicht in das OSSE-Register erfasst. Das OSSE-Register zeigt zur Kennzeichnung des Datensatzes die intern erzeugten Identifikatoren (PIDOSSE) an. Die Zuordnung von den IDAT zu den PIDOSSE findet am Standort manuell statt.

[*#Ende Variante 3*]

### Workflow

Medizinische Daten werden in Formulare (Stammdaten- und Verlaufsdatenformulare) erfasst, die im Bearbeitungsablauf folgende Statuswerte annehmen können:

[*Falls zutreffend hier die Dokumenten-Status und Statusübergänge beschreiben; sonst den ganzen Abschnitt streichen*.]

### Benutzer, Rollen und Rechte

Zugriffsberechtigungen werden rollenbasiert vergeben. Jeder Benutzer besitzt entsprechend seiner Funktion eine oder mehrere Rollen, mit denen er sich jeweils anmeldet. Für die Definition der Zugriffsrechte werden Daten insbesondere nach ihrer Zuordnung zu der informationellen Einheit in der sie erhoben wurden [und nach … (*hier weitere Kriterien ergänzen*)], klassifiziert. Für das OSSE-Register für „Seltene Erkrankung X“ gibt es entsprechend der Einwilligungserklärung, den beteiligten Standorten und organisatorischen Erfordernissen folgende Rollen:

[*Liste der Rollen und ihrer Beschreibung/zugeordneten Rechte; ggf. als Anhang*]

Alle Zugriffe werden protokolliert (siehe 5.3 „Maßnahmen in der IT-Infrastruktur“).

## Identitätsmanagement

Pseudonymisierung ist ein zur Aufrechterhaltung eines hohen Datenschutzniveaus notwendiger Schritt, um den Patienten vor Rückidentifizierung zu schützen. Anstelle seiner identifizierenden Daten (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

[*#Beginn* ***Variante 1*** *(Zentrales ID-Management für alle Register für „Seltene Erkrankung X“)*]

Für die Pseudonymisierung im OSSE-Register für „Seltene Erkrankung X“ wird eine Instanz der „Mainzelliste[[6]](#footnote-7)“ genutzt, die zentral für alle OSSE-Register für „Seltene Erkrankung X“ von [*Betreiber der zentralen Mainzelliste*] betrieben wird. Sie erzeugt für jeden Patienten einen eindeutigen Identifikator (PID) und je ein unabhängiges Pseudonym zweiter Stufe (PSN*OSSE*(#)) für jedes OSSE-Register, in dem Daten des Patienten erfasst werden. Es gibt noch folgende weitere Systeme für die Forschung im Register für „Seltene Erkrankung X“, für die die Mainzelliste unabhängige Pseudonyme erzeugt:

* [Liste weiterer Systeme des Verbunds, die pseudonymisierte Daten speichern und Art der Pseudonyme]

Die Mainzelliste erzeugt außerdem nicht-rückführbare Exportpseudonyme für den Export von Patientendaten zu Forschungszwecken, wobei im Fall einer Zusammenführung von Fällen aus verschiedenen Registern für „Seltene Erkrankung X“ Daten identischer Patienten dasselbe Exportpseudonym erhalten. Das zentrale Identitätsmanagement ermöglicht eine datenschutzgerechte Zusammenführung der zu verschiedenen Zeitpunkten und von verschiedenen Standorten (und in verschiedene Register) erfassten bzw. importierten patientenbeziehbaren Daten eines Patienten.

[*#Ende Variante 1*]

[*#Beginn* ***Variante 2*** *(Lokal betriebenes ID-Management für dieses Register für „Seltene Erkrankung X“)*]

Für die Pseudonymisierung im OSSE-Register für „Seltene Erkrankung X“ wird eine Instanz der „Mainzelliste“ genutzt, die von [*Betreiber der Mainzelliste*] betrieben wird. Sie erzeugt für jeden Patienten einen eindeutigen Identifikator (PID) und ein Pseudonym zweiter Stufe (PSN*OSSE*). Es gibt noch folgende weitere Systeme für die Forschung im Register für „Seltene Erkrankung X“, für die die Mainzelliste unabhängige Pseudonyme erzeugt:

* [Liste weiterer Systeme des Verbunds, die pseudonymisierte Daten speichern und Art der Pseudonyme. ]

Die Mainzelliste erzeugt außerdem nicht-rückführbare Exportpseudonyme für den Export von Patientendaten zu Forschungszwecken, wobei im Fall einer Zusammenführung von Fällen aus verschiedenen Registern oder Brückenköpfen für „Seltene Erkrankung X“ Daten identischer Patienten, unterschiedliche Exportpseudonyme erhalten. Das lokal für das OSSE-Register für „Seltene Erkrankung X“ betriebene Identitätsmanagement ermöglicht also eine datenschutzgerechte Zusammenführung der zu verschiedenen Zeitpunkten und von mehreren Standorten erfassten bzw. importierten patientenbeziehbaren Daten, jedoch ohne dass Daten identischer Patienten aus verschiedenen Registern einander zugeordnet werden können.

[*#Ende Variante 2*]

[*#Beginn* ***Variante 3*** *(Manuell geführte Liste von IDAT; in diesem Fall erzeugt OSSE einen PID, der mit den IDAT in der Liste registriert wird)*]

Das OSSE-Register für „Seltene Erkrankung X“ erzeugt interne Identifikatoren (PIDOSSE) beim Anlegen eines Patienten. Der PID wird im Behandlungskontext **am Standort** manuell in einer Liste mit den IDAT geführt.

[*#Ende Variante 3*]

### Manuelles Linken [*Nur für Variante 1 und Variante 2*]

Eine Schnittstelle erlaubt einem Menschen, Ergebnisse des automatischen Matching 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 Patienten) angezeigt und es besteht die Möglichkeit, zur Entscheidungsfindung auf medizinische Daten zuzugreifen.

## Biomaterialbank

[*Falls Daten aus einer Biomaterialbank importiert werden: hier Beschreibung der Biomaterialbank, Betreiber, darin gespeicherte Daten etc., ggf. als Anhang*]

## Teiler (OSSE-Share)

Der Teiler ist das Client-Interface für die dezentrale Suche (siehe 3.6 „Dezentrale Suche“). Er ruft über den Suchbroker gestellte Anfragen ab, kommuniziert mit dem OSSE-Store und zeigt einem berechtigten Benutzer (z.B. aus der Registerleitung) Anfrage und Ergebnis an. Hierbei werden nur pseudonymisierte und aggregierte Daten angezeigt. Der Datenverantwortliche kann mit dem Teiler-Interface einen Datenexport anstoßen. Die exportierten Daten enthalten nicht-rückführbare Exportpseudonyme anstelle der in OSSE gespeicherten Pseudonyme. Über die Weitergabe von derart „quasi anonymisierten“ Forschungsdaten an Dritte entscheidet [*hier das zuständige Gremium angeben*]. Es muss sichergestellt werden, dass die Weitergabe der exportierten Daten mit der in den Einwilligungen beschriebenen Datennutzung konform ist, da speziell im Bereich seltener Erkrankungen allein durch die medizinischen Daten ein hohes Risiko einer Reidentifizierung besteht.

## Metadaten-Repository

Das Metadaten-Repository (MDR) speichert die Bedeutung (Semantik) sämtlicher im OSSE-Register für „Seltene Erkrankung X“ verwendeten (Nutz-)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 (7.2 Datensätze) definiert. Da das MDR keine personenbezogenen Daten verarbeitet, wird innerhalb dieses Datenschutzkonzepts nicht weiter darauf eingegangen.

## Registerverzeichnis (Registry of Registries)

Im Registerverzeichnis registrieren sich alle OSSE-Register und ‑Brückenköpfe[[7]](#footnote-8) mit einer Kurzbeschreibung des Registers, den Ansprechpartnern und ggf. zusätzlich den Metadaten des Registers und interessanten Kerndaten (z.B. Anzahl der Fälle insgesamt). Die Daten werden von den Verantwortlichen aktiv hochgeladen. Es werden keine Patientendaten übertragen. Das Registerverzeichnis wird von [*Hier den Betreiber des Registerverzeichnisses angeben*] betrieben.

# Datenverarbeitende Prozesse

## Manuelle Dateneingabe

### Anlegen eines Patienten

1. Der Benutzer gibt die IDAT in die im OSSE-Register integrierte Maske der Mainzelliste ein.
2. Das OSSE-Register erhält ein Pseudonym (detailliert siehe 3.3 „Pseudonymisierung“), das mit dem Datensatz gespeichert wird. Dabei erhält der Benutzer keine Rückmeldung, ob der Patient in der Mainzelliste bereits vorhanden war oder neu angelegt wurde.

### Auswahl von Patienten, Dateneingabe

Der Benutzer erhält eine Liste der Patienten (mit Klartextnamen) entsprechend seiner Nutzerrechte. Nach Auswahl eines Patienten können Formulare bearbeitet werden; im Browserfenster werden IDAT des ausgewählten Patienten angezeigt.

### Workflowunterstützung

[*Hier ist der Datenerfassungs-Prozess zu beschreiben: Welchen Statuswert hat ein Dokumente wann? Wer darf welche Dokumente sehen und bearbeiten?*]

### Manuelle Freigabe von Datensätzen

In begründeten Fällen, z.B. für eine Referenzbefundung, können Datensätze an definierte Personen und Rollen freigegeben werden. Die Freigabe umfasst einzelne Formulare oder ganze Fälle (alle Formulare eines Patienten des betreffenden Standorts). Der Benutzer, der die Freigabe durchführt, muss dazu explizit berechtigt sein. Eine Freigabe wird zeitlich befristet. Zur Freigabe wählt der Benutzer einen Patientendatensatz aus. Im Dialog „Datensatz freigeben“ legt er den zu berechtigenden User bzw. Rolle fest und bestimmt die Gültigkeitsdauer. Die Datenfreigabe muss durch die in der Einwilligung beschriebenen Zugriffe abgedeckt sein.

[*Falls kein Datenimport aus anderen Systemen stattfindet, folgenden Abschnitt bitte löschen*]

## Datenimport

Daten aus vorhandenen Systemen werden in regelmäßigen Zeitintervallen in das OSSE-Register für „Seltene Erkrankung X“ übernommen und dort neu angelegt bzw. aktualisiert. Die Aufstellung der zu importierenden Daten und ihrer Quellsysteme findet sich im Anhang 7.3 „Daten und Quellsysteme für den Datenimport“. Die Datenübernahme durchläuft folgende Schritte eines sogenannten ETL[[8]](#footnote-9)-Prozesses, wobei sich die Daten bis zum Import in das OSSE-Register immer auf den lokalen Systemen am jeweiligen Standort befinden:

1. Identifizierende, medizinische und Probendaten werden aus den Quellsystemen extrahiert.
2. Identifizierende Daten werden innerhalb des Transformationsschrittes durch ein Pseudonym ersetzt (Details siehe 3.3 „Pseudonymisierung“).
3. Der ETL-Prozess lädt die Daten über eine Web-Schnittstelle in das OSSE-Register.

## Pseudonymisierung

[*#Beginn* ***Variante 1*** *und* ***Variante 2*** *(lokale oder zentrale Mainzelliste)*]

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

### Manuelle Patientenregistrierung

Gleichermaßen für die Registrierung eines neuen Patientendatensatzes wie auch für das Wiederfinden eines vorhandenen gibt der Benutzer die identifizierenden Daten in eine Eingabemaske der Mainzelliste, die im Browserfenster der OSSE-GUI angezeigt wird, ein. Die identifizierenden Daten 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 der Patient bereits in der Mainzelliste registriert ist. Falls nicht, so wird der Patient neu angelegt, indem die IDAT gespeichert und ein nicht-sprechender PID sowie das PSNOSSE als Pseudonym zweiter Stufe erzeugt werden. Der Benutzer wird automatisch auf eine Webseite des OSSE-Registers zurückgeleitet, auf der MDAT zum neu angelegten oder ausgewählten Patienten eingegeben werden können. Browser und OSSE-Register kommunizieren dabei mittels temporärer Identifikatorens. Das PSNOSSE 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 PSNOSSE 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 identifizierende Daten der Patienten im Browser angezeigt. Diese werden allerdings erst im Browser mit den MDAT zusammengeführt, so dass das OSSE-Register zu keinem Zeitpunkt Zugriff auf IDAT bekommt. Dazu ruft die Registersoftware für jedes PSNOSSE bei der Mainzelliste eine sessionbasierte temporäre ID ab, mit der der Browser die zugehörigen IDAT von der Mainzelliste erhält.

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

[*#Ende Variante 1, Variante 2*]

[*#Beginn Variante 3 (OSSE erzeugt eigene PIDs)*]

Bei der Registrierung eines neuen Patienten generiert das Register einen eindeutigen Patientenidentifikator (PID). Die Zuordnung des PID zu den IDAT wird jeweils lokal am Behandlungsort in einer manuell geführten Liste wie folgt separat erfasst.

[*Hier beschreiben, wie der Vorgang organisatorisch geregelt ist und wie die Liste vor Zugriffen Unberechtigter geschützt wird.*]

[*#Ende Variante 3*]

### Pseudonymisierung beim Datenimport

Beim Datenimport aus den [klinischen Systemen oder der Biobank/Probenquelle *(Unzutreffendes streichen!)*] werden die IDAT vor dem Laden der Datensätze (siehe 3.2 „Datenimport“) durch Pseudonyme ersetzt. Datenextraktion und -transformation werden durch eine Datenintegrations-Software (Talend Open Studio) unterstützt. Dabei ist die Pseudonymisierung Teil der Daten-Transformation 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 PSNOSSE (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, (PSNOSSE)tr, an die Transformationskomponente, wo die IDAT durch das (PSNOSSE)tr ersetzt werden.
4. Die Importschnittstelle entschlüsselt das (PSNOSSE)tr und speichert die Daten mit dem PSNOSSE

Durch dieses Verfahren ist sichergestellt, dass auch beim Datenimport keine Pseudonyme zugeordnet werden können, da die Daten liefernde Seite, die den Patientenbezug herstellen kann, nur das verschlüsselte (PSNOSSE)tr sieht.

### Schlüsselerzeugung und Schlüsselverwaltung

Das Schlüsselpaar für die geschützte Übertragung der OSSE-Pseudonyme wird im OSSE-Register bei Systemstart erzeugt und 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 Identitätsmanagement) jederzeit über eine Webschnittstelle beim OSSE-Register abgerufen werden.

[*Dieser Abschnitt (Import von Biomaterialdaten) wird benötigt, falls Bioprobendaten in das Register importiert werden sollen. Dabei wird unterschieden, ob die Probendaten direkt von der Probenquelle stammen oder der Verbund eine separate Biomaterialbank nutzt. Im zweiten Fall wird vorausgesetzt, dass die Biomaterialbank, gemäß dem „Datenschutzkonzept der TMF für Biomaterialbanken“[[9]](#footnote-10), die LabID von der Probenquelle nicht im Klartext sondern in verschlüsselter Form weitergibt und selbst keinen Patientenbezug speichert. Abweichende Realisierungen sind im folgenden Abschnitt entsprechend anzupassen.)*]

## Import von Biomaterialdaten[[10]](#footnote-11)

[#Beginn Biomaterialbank existiert]

Durch die Anbindung einer Biomaterialbank sollen Information über Bioproben zur Verfügung gestellt werden, die es ermöglichen, aus dem Register geeignete Patienten für Forschungsvorhaben zu ermitteln. Daten zu Bioproben (IDAT, PID, LabID, weitere Charakteristika der Probe) werden im Behandlungszusammenhang erfasst (Probenquelle) und an die Biomaterialbank übertragen. Der an der Probenquelle erzeugte eindeutige Identifikator der Probe, LabID, wird in der Biomaterialbank verschlüsselt (LabID)tr. Die Biomaterialbank speichert Proben ohne Patientenbezug; deshalb soll der Patientenbezug der Probe für die Weitergabe an das Register nur temporär (bis zur Übertragung der Probendaten) gespeichert werden. Die Probendaten im Register erlauben keinen direkten Abruf von Informationen zur Probe von der Probenquelle. Folgende Daten aus der Biomaterialbank werden in das OSSE-Register importiert:

[*Unzutreffendes aus der Aufzählung streichen!*]

* Existenz bzw. Anzahl der Proben
* Charakteristika zur Probe
* sowie die (LabID)tr

Beim Import von Biomaterialdaten werden folgende Schritte durchlaufen:

1. Der Patient wird durch die Probenquelle in der Mainzelliste registriert: Die Probenquelle schickt IDAT und erhält das verschlüsselte OSSE-Pseudonym (PSNOSSE)tr und falls erforderlich, den allgemein gültigen PID.
2. Der Patient wird durch einen Benutzer im OSSE-Register erfasst.
3. Die Probe wird an die Biobank verschickt: Das Adressetikett enthält das (PSNOSSE)tr, das für die Datenübermittlung an das Register zwischengespeichert wird.
4. Die Probe wird im Biobankenmodul registriert: Das Biobankenmodul speichert die LabID und alle notwendigen Daten zur Probe (OrgDat). Aus der LabID wird durch eine kryptografische Operation die LabIDtr erzeugt, damit eine direkte Zuordnung von MDAT und Probe vermieden werden kann. Eine Zuordnung von (PSNOSSE)tr und LabIDtr wird temporär gespeichert.
5. Übertragung der Probendaten an das OSSE-Register: Das OSSE-Register erhält zu jeder Probe einen Datensatz bestehend aus (PSNOSSE)tr, LabIDtr und weiteren Information zur Probe (siehe oben), die übermittelt werden sollen. Die Daten werden, wie unter 3.2 „Datenimport“ beschrieben, transformiert und in das OSSE-Register geladen. Nach erfolgreicher Übertragung wird die Zuordnung (PSNOSSE)tr und LabIDtr gelöscht. Dadurch wird verhindert, dass in der Biomaterialbank dauerhaft eine Zuordnung zwischen Probe und Patient hergestellt wird.

Abbildung : Datenflüsse beim Import von Biomaterialdaten

[#*Ende Biomaterialbank existiert*]

[*#Beginn Biomaterialbank existiert nicht*]

Im OSSE-Register für „Seltene Erkrankung X“ sollen Information über Bioproben zur Verfügung gestellt werden, die ermöglichen, aus dem Register geeignete Patienten für Forschungsvorhaben zu ermitteln. Daten zu Bioproben (IDAT, PID, LabID, weitere Charakteristika der Probe) werden im Behandlungszusammenhang erfasst (Probenquelle). Folgende Daten werden in das OSSE-Register importiert:

[*Unzutreffendes aus der Aufzählung streichen!*]

* Existenz bzw. Anzahl der Proben
* Charakteristika zur Probe

Beim Import von Biomaterialdaten werden folgende Schritte durchlaufen:

1. Der Patient wird durch die Probenquelle in der Mainzelliste registriert: Die Probenquelle schickt IDAT und erhält das verschlüsselte OSSE-Pseudonym (PSNOSSE)tr und falls erforderlich, den allgemein gültigen PID.
2. Der Patient wird durch einen Benutzer im OSSE-Register erfasst.
3. Übertragung von Probendaten aus der Probenquelle an das OSSE-Register: Das OSSE-Register erhält zu jeder Probe einen Datensatz bestehend aus (PSNOSSE)tr und weiteren Information zur Probe (siehe oben), die übermittelt werden sollen. Daten von der Probenquelle werden, wie unter 3.2 „Datenimport“ beschrieben, transformiert und in das OSSE-Register geladen.
[*Falls es nicht möglich ist*, *das (PSNOSSE)tr in der Probenquelle zwischenzuspeichern, kann es mithilfe der IDAT über den Pseudonymisierungsschritt im ETL-Prozess abgerufen werden*. *Der Abschnitt ist entsprechend anzupassen.*]

Abbildung 1: Datenflüsse beim Import von Biomaterialdaten

[*#Ende Biomaterialbank existiert nicht*]

## Datenexport

Daten können zu Auswertungszwecken exportiert werden. Dafür wird das interne Pseudonym des OSSE-Registers im Exportschritt durch ein Exportpseudonym ersetzt.

[*#Beginn* ***Variante 1*** *(zentrales Identitätsmanagement)*]

Werden im Rahmen der dezentralen Suche Daten aus verschiedenen Registern zusammengeführt, so werden beim Export einheitliche nicht-rückführbare Exportpseudonyme beim zentralen Identitätsmanagement abgefragt. Diese erlauben, in den zusammengeführten Datenbeständen Datensätze identischer Patienten zuzuordnen, die in verschiedenen Registern erfasst wurden, sowie die konsistente Aktualisierung der zusammengeführten Datensätze. Folgende Schritte werden beim Export durchlaufen:

1. OSSE schickt das interne Pseudonyme PSNOSSE(#) zusammen mit einer Projektkennung an das Identitätsmanagement.
2. Das Identitätsmanagement liefert ein einheitliches projektspezifisches Exportpseudonym (PSNProjekt) zurück.
3. Der Datensatz wird mit dem PSNProjekt ausgegeben.

[*#Ende Variante 1*]

[*#Beginn* ***Variante 2*** *(lokales Identitätsmanagement)*]

Werden im Rahmen der dezentralen Suche Daten aus verschiedenen Registern zusammengeführt, so werden beim Export einheitliche nicht-rückführbare Exportpseudonyme beim lokalen Identitätsmanagement abgefragt. Diese erlauben die konsistente Aktualisierung der zusammengeführten Datensätze, identische Patienten verschiedener Register werden dabei aber nicht erkannt. Folgende Schritte werden beim Export durchlaufen:

1. OSSE schickt das interne Pseudonyme PSNOSSE zusammen mit einer Projektkennung an das Identitätsmanagement.
2. Das Identitätsmanagement liefert ein projektspezifisches Exportpseudonym (PSNProjekt) zurück.
3. Der Datensatz wird mit dem PSNProjekt ausgegeben.

[*#Ende Variante 2*]

Besonders bei Erkrankungen mit geringen Fallzahlen lassen sich medizinische Daten bei Kenntnis des Krankheitsverlaufs oder zusätzlicher Daten auch ohne Kenntnis der identifizierbaren Daten konkreten Patienten zuordnen. Auch bei der Verwendung nicht-rückführbarer Exportpseudonyme kann nicht immer sicher von faktischer Anonymität ausgegangen werden.

Deshalb wird auch der Export pseudonymisierter Daten und der Zweck ihrer Nutzung in der informierten Einwilligung berücksichtigt.

## Dezentrale Suche

Mit der dezentralen Suche können Forscher die Datenbestände der OSSE-Register oder Brückenköpfe durchsuchen, um die Register zu ermitteln, in denen Daten und Proben vorhanden sind, die für ein Forschungsvorhaben relevant sein könnten. Der Suchbroker stellt für die Suche ein Webformular bereit, in dem Suchanfragen erfasst werden können, die Datenelemente nach vorgegebenen Werten oder per Freitextsuche filtern. Mehrere Suchattribute können durch logische Operatoren frei kombiniert werden. Mit dem Suchformular werden außerdem ein Exposé des geplanten Forschungsvorhabens und die Kontaktdaten des anfragenden Forschers übermittelt.

Die Suchanfrage wird zunächst gespeichert und dem anfragenden Forscher lediglich die Speicherung der Suchanfrage mitgeteilt. Die Teiler der beteiligten Register rufen in regelmäßigen Abständen neu hinzugekommene Suchanfragen vom Suchbroker ab und ermitteln, welche Datensätze im OSSE-Register den Suchkriterien entsprechen. Der Inhalt der Anfrage sowie die gefundenen Datensätze können für jedes Register von einer dazu berechtigten Person eingesehen werden. Diese kann nun den anfragenden Forscher kontaktieren, um eine mögliche Weitergabe von Daten oder Proben zu vereinbaren. Dieser Vorgang und die damit verbundenen datenschutzrechtlichen Fragen, wie z.B. die Notwendigkeit, weitere Einwilligungen einzuholen, müssen im Einzelfall von den beteiligten Personen geklärt werden. Eine Übermittlung von Daten findet kontrolliert außerhalb des OSSE-Registers statt.

## Hochladen von Informationen an das Registerverzeichnis

Durch eine Menüfunktion, die von einem berechtigten Benutzer ausgeführt wird, können Informationen über das OSSE-Register für „Seltene Erkrankung X“ an das Registerverzeichnis hochgeladen werden (Neuregistrierung und Aktualisierungen). Der Umfang der hochzuladenden Informationen kann in der Registerkonfiguration eingestellt werden. Inhaltsdaten des Registers betrifft dies nicht (siehe 2.6 „Registerverzeichnis (Registry of Registries)“).

# Organisatorische Rahmenbedingungen

[*In Verbindung mit den organisatorischen Rahmenbedingungen sind auch die vertraglichen Regelungen des Trägers (z.B. eine Satzung oder Vergleichbares) zu nennen, die im Falle eines Rechtsstreits belastbar sind.*]

## Betrieb der Komponenten

Der Betrieb des OSSE-Registers erfolgt durch [*hier den Standort/die Institution angeben, die das OSSE-Register betreibt und administriert*]. Daten erfassende Standorte des Registers für „Seltene Erkrankung X“ sind

* [*Hier Liste der Institutionen/Standorte einfügen*]

Den Betrieb der zentralen Komponenten des OSSE-Registers für „Seltene Erkrankung X“ übernehmen ausgewählte Institutionen, die in Absprache mit dem Lenkungsgremium (Registerleitung) des OSSE-Registers für „Seltene Erkrankung X“ bestimmt werden. Dabei wird zum Zweck der informationellen Gewaltenteilung der organisatorisch unabhängige Betrieb von Identitätsmanagement und OSSE-Register gewährleistet (vgl. Abschnitt 5.1, „Informationelle Gewaltenteilung“).

## Teilnehmende Forscher

*Teilnehmende Forscher* sind die Personen, die über die dezentrale Suche Anfragen stellen können. Generell können alle Mitglieder der Registerstandorte als teilnehmende Forscher das OSSE-Register für „Seltene Erkrankung X“ nutzen, wobei jeder Standort selbst entscheidet, welche seiner Mitglieder eine Zugangsberechtigung erhalten (siehe auch Abschnitt 5.2, „Autorisierung und Authentifizierung“).

Wissenschaftler, die nicht Mitglieder eines OSSE-Register für „Seltene Erkrankung X“-Standorts sind, können auf Antrag vom Registerausschuss (siehe auch Abschnitt 4.5) eine Zugangsberechtigung erhalten. Diese ist angemessen zu befristen.

## Mitgliederversammlung

Teilnehmende Forscher/Kliniker bzw. ihre Einrichtungen, die sich mit ihren Daten am OSSE-Register für „Seltene Erkrankung X“ beteiligen, sind mit einer Stimme an der Mitgliederversammlung des OSSE-Registers für „Seltene Erkrankung X“ beteiligt.

## Registerleitung

Die Registerleitung: wird von der Mitgliederversammlung des OSSE-Registers für „Seltene Erkrankung X“ zur Führung der Geschäfte des Registers gewählt.

## Registerausschuss

Von der Registerleitung des OSSE-Registers für „Seltene Erkrankung X“ wird ein Registerausschuss berufen. Dieser erfüllt u. a. folgende Aufgaben:

* Prüfung und Bewilligung von Anträgen externer Forscher[[11]](#footnote-12) für die Nutzung der OSSE-Register für „Seltene Erkrankung X“ (dezentrale Suche).
* Prüfung und Bewilligung von Anträgen auf Export medizinischer Daten für externe Forschungsprojekte.
* Prüfung und Bewilligung von Anträgen auf die Benachrichtigung betroffener Patienten über Forschungsergebnisse.

Darüber hinaus ist der Registerausschuss erster Ansprechpartner für datenschutzrechtliche Angelegenheiten.

Der Registerausschuss wird so besetzt, dass jeder der Standorte des OSSE-Registers für „Seltene Erkrankung X“ darin vertreten ist. Zu den Mitgliedern zählen mindestens:

* Ein Arzt, der vorwiegend in der Behandlung betroffener Patienten tätig ist.
* Ein Wissenschaftler, der mit den in dem OSSE-Register für „Seltene Erkrankung X“ verwalteten Daten (oder Daten ähnlichen Typs) forscht.
* Ein Datenschutzbeauftragter oder ein mit dem Thema Datenschutz vertrauter Jurist.

Zusätzlich kann ein Vertreter der Mitentwickler des OSSE-Registers für „Seltene Erkrankung X“ in beratender Funktion hinzugezogen werden.

## Zugriff durch Systemadministratoren

Die im OSSE-Register für „Seltene Erkrankung X“ gespeicherten Daten können prinzipiell von den Administratoren der verwendeten IT-Infrastruktur eingesehen werden. Zugriffe auf die Daten durch Administratoren dürfen nur erfolgen, wenn dies zur Erfüllung ihrer Aufgaben zwingend erforderlich ist. Das Vorgehen beim Datenzugriff ist durch folgenden Prozess geregelt: [*Hier ist zu beschreiben, wie ein derartiger Zugriff abläuft, und wie der Zugriff beispielsweise über die übliche Protokollierung hinaus unter Angabe von Gründen dokumentiert wird*]. Alle Administratoren sind entsprechend zu instruieren und zur Verschwiegenheit zu verpflichten[[12]](#footnote-13).

# Maßnahmen zum Datenschutz

## Informationelle Gewaltenteilung

Das Identitätsmanagement wird logisch, physikalisch und organisatorisch getrennt von allen Komponenten betrieben, die MDAT oder Daten zu Bioproben speichern. [*Der Betreiber des Identitätsmanagements* *(hier bitte den Betreiber angeben)*] steht unter eigener rechtlicher Verantwortung und ist dem Registerbetreiber gegenüber nicht weisungsgebunden. So ist sichergestellt, dass Personen, die im OSSE-Register für „Seltene Erkrankung X“ außerhalb des Behandlungszusammenhangs Zugriff auf klinische oder Biomaterial-Daten haben, keine Zuordnung von Daten zu realen Patienten treffen können.

## Autorisierung und Authentifizierung

### Autorisierung von Benutzern

Die Autorisierung von Benutzern (Zuweisung zu definierten Rollen) des OSSE-Registers erfolgt durch lokale Administratoren der jeweiligen Standorte entsprechend den lokalen Strukturen und Erfordernissen. Dabei können lokale Regelungen des Datenschutzes (zum Beispiel Sichtbarkeit bestimmter Patienten in bestimmten Abteilungen) berücksichtigt werden.

### Autorisierung von Komponenten

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

### Authentifizierung von Benutzern

Die Authentifizierung von Benutzern gegenüber dem OSSE-Register für „Seltene Erkrankung X“ erfolgt über Benutzername und Passwort.

### Authentifizierung von Komponenten

Zugriffe zwischen verschiedenen IT-Komponenten über das Internet finden nur nach erfolgreicher Authentifizierung statt. Die Authentifizierung erfolgt serverseitig über Serverzertifikate und clientseitig (je nach technischer Möglichkeit) über IP-Adresse und Nutzername /Passwort oder über Clientzertifikate.

## Maßnahmen in der IT-Infrastruktur

[*Der folgende Abschnitt enthält neben Angaben zu den Sicherheitsmaßnahmen, die Teil der OSSE-Implementierung sind, auch Vorschläge/Vorgaben, die die Organisation und die Konfiguration der IT-Umgebung betreffen. Die Aussagen sind im Einzelnen der tatsächlichen Umsetzung anzupassen.*]

### Sicherheit der gespeicherten Daten

Alle in den zentralen Komponenten dem OSSE-Register für „Seltene Erkrankung X“ erhobenen Daten werden auf verschlüsselten Festplattenpartitionen gespeichert. Der zugehörige Schlüssel befindet sich jeweils auf einem getrennten Medium pro Server (z.B. Papier, USB-Stick). Dieses Medium wird nur während des Mount- bzw. Bootvorgangs benötigt und wird ansonsten sicher verwahrt. Nur der Administrator des jeweiligen Servers hat Zugriff auf „sein“ Schlüsselmedium. Der Schlüssel kann nicht errechnet werden. Alle Server befinden sich in Rechenzentren, die über eine Zugangskontrolle per Chipkarte oder ähnlich sichere Token für jeweils berechtigte Personen verfügen.

### Sicherheit der Kommunikation

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

* Die Kommunikation zwischen den Komponenten 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. Schlüssellänge). Aktuelle Anforderungen können den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik entnommen werden (<https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html>).
* 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 Forschern 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, ggfls. 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.

# Wahrung von Betroffenenrechten

## Aufklärung und Einwilligung

[*Zur Breite der Einwilligung:* *Sofern die Einwilligung unbestimmte Angaben beispielsweise zur Dauer der Speicherung und dem Verwendungszweck der Daten macht, muss dies in der Patienteninformation zum Zweck der Aufklärung explizit angesprochen und erklärt sein.*]

Die informierte Einwilligung (Volltext siehe Anhang) ist Rechtsgrundlage der Datenverarbeitung. Mit der Einwilligung erklärt sich der Patient insbesondere dazu bereit, dass

* [***Variante 1 und Variante 2*** *(es gibt ein Identitätsmanagement)*] seine identifizierenden Daten an das Identitätsmanagement übermittelt und dort gespeichert werden,
* [***Variante 3*** *(IDAT werden am jeweiligen Standort manuell zugeordnet)*] seine identifizierenden Daten manuell in einer Liste zusammen mit dem internen PIDOSSE geführt werden,
* medizinische Daten und Daten zu Biomaterialproben gemäß Registerdefinition im OSSE-Register erfasst werden,
* diese Daten von Forschern des OSSE-Register für „Seltene Erkrankung X“ lokal ausgewertet und gemäß der Funktionsweise der dezentralen Suche durchsucht werden können und
* medizinische Daten und Daten zu Biomaterialproben des Patienten aus dem OSSE-Register mit einem nicht-rückführbaren Exportpseudonym exportiert und für Forschungszwecke, die in der Einwilligung näher definiert sind, an externe Forscher, die benannt sind, übermittelt werden.

Mit Einholen der Einwilligung wird der Patient über sein Recht auf Auskunft und Widerruf informiert.

## Auskunft über gespeicherte Daten

Patienten des OSSE-Registers für „Seltene Erkrankung X“ haben das Recht, Auskunft über die im Register über sie gespeicherten Daten zu erhalten. Der Antrag auf Auskunft ist schriftlich an die behandelnde Klinik zu stellen. Diese fordert über die Benutzerschnittstelle einen Datenexport an und erhält ein Exportpseudonym für den Patienten. Der Registeradministrator führt den Export durch und erzeugt einen menschenlesbaren Ausdruck der Daten, den er in einem versiegelten Umschlag markiert mit dem Exportpseudonym der zuständigen Klinik zustellt, wo er dem Patienten ausgehändigt werden kann. Enthalten die Daten genetische Befunde, so ist die Aushändigung der Daten verpflichtend an ein Beratungsgespräch durch einen behandelnden Arzt gebunden.

## Widerruf, Löschung, Anonymisierung

Patienten haben das Recht, die Einwilligung in die Verarbeitung ihrer Daten im OSSE-Register für „Seltene Erkrankung X“ zu widerrufen. Der Widerruf ist schriftlich an die behandelnde Klinik zu richten, die diesen an die Registerleitung weiterleitet. Der betroffene Patient kann mit dem Widerruf zusätzlich die vollständige Löschung seiner Daten beantragen. Fehlt dieser Antrag, so erfolgt eine Anonymisierung, sofern der Datenbestand eine faktische Anonymisierung zulässt. Kann aufgrund der geringen Fallzahlen und der spezifischen Ausprägungen keine „sinnvolle“[[13]](#footnote-14) Anonymisierung durchgeführt werden, werden die Daten gelöscht. Ausgenommen von der Löschung sind Daten, die bereits Grundlage einer veröffentlichten Studie sind[[14]](#footnote-15). Diese Daten werden dann besonders geschützt (z.B. gesondert archiviert) und der Zugriff auf sie gesperrt.

[*Die hier genannten (oder weitere) Optionen und Regelungen im Zusammenhang mit Widerruf, Anonymisierung und Löschung von Daten, sind entsprechend in der Einwilligung aufzuführen und in der Patienteninformation zu erklären.*]

Nach Prüfung des Widerrufs wird der Antrag auf Löschung entschieden. Im Falle einer Löschung werden alle dem Patienten zugeordneten Datensätze in der Mainzelliste und dem OSSE-Register gelöscht. Im Falle der Anonymisierung werden die Datensätze in der zentralen Patientenliste gelöscht und das PSNOSSE des Patienten 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 Pseudonymerzeugung ist sichergestellt, dass die Pseudonyme eines gelöschten oder anonymisierten Patienten nicht mehr für neue Patienten verwendet werden.

Die Löschung bzw. Anonymisierung ist von den zuständigen Betreibern zeitnah, maximal innerhalb von 14 Werktagen, vorzunehmen[[15]](#footnote-16). Der Abschluss der Löschung oder Anonymisierung wird dem Patienten schriftlich bestätigt.

## Dauer der Speicherung

Die erhobenen Daten bleiben im OSSE-Register gespeichert, so lange es für sie eine sinnvolle wissenschaftliche Verwendung im Rahmen der Patienteneinwilligung gibt. Falls die Daten nicht mehr in der vorgesehenen Form genutzt werden können, prüft der Registerausschuss, ob eine Rechtsgrundlage für eine anderweitige Verwendung der Daten, gegebenenfalls in anonymisierter Form, besteht. Falls diese Prüfung negativ ausfällt, sind die Daten zu löschen.

# Anhang

## Patienteneinwilligung OSSE-Register

[Schablone für die Einwilligung wird hier eingefügt]

## Datensätze

### Registerdefinition

### Identifizierende Daten

## Daten und Quellsysteme für den Datenimport

1. Der Leitfaden zum Datenschutz in der medizinischen Forschung ist unter <http://www.tmf-ev.de/Themen/Projekte/V039_01_WS_DS_Review.aspx> abrufbar. Zu dieser Version des Leitfadens hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.3.2014 in Hamburg einstimmig folgenden Beschluss gefasst: "*Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt medizinischen Forschungseinrichtungen und Forschungsverbünden den von der TMF entwickelten 'Leitfaden zum Datenschutz in der medizinischen Forschung. Generische Lösungen der TMF – Version 2' als Basis zu nehmen für die konkrete Ausgestaltung der Datenschutzkonzepte.*" [↑](#footnote-ref-2)
2. Für eine optimale Nutzung der dezentralen Suche sollten alle Teilnehmer (OSSE-Register und OSSE-Brückenköpfe) ein gemeinsames Identitätsmanagement nutzen, das zu den unabhängigen Pseudonymen der verschiedenen Teilnehmer einheitliche Exportpseudonyme erzeugen kann. Gerade im Bereich der Seltenen Erkrankungen ist es entscheidend, identische Patienten in verschiedenen Registern nicht mehrfach zu zählen. [↑](#footnote-ref-3)
3. Dieses Konzept basiert auf dem OSSE-DSK v1.2 von M. Muscholl, M. Lablans, A. Borg, F. Ückert und TOF Wagner. [↑](#footnote-ref-4)
4. Gemeint sind grundsätzlich entsprechende Personen beiden Geschlechts; auf eine neutrale Formulierung wurde aus sprachlichen Gründen verzichtet. [↑](#footnote-ref-5)
5. Ausgenommen ist die Löschung auf Wunsch eines Patienten, siehe Anmerkungen zum Widerrufsrecht in Abschnitt 6.3. [↑](#footnote-ref-6)
6. „Mainzelliste“ steht hier wie auch im Folgenden für ein Identitätsmanagement, das die Schnittstelle der Mainzelliste erfüllt, nähere Informationen zur Mainzelliste unter [www.mainzelliste.de](http://www.mainzelliste.de). [↑](#footnote-ref-7)
7. Mit einem OSSE-Brückenkopf können Register, die nicht mit der OSSE-Register-Software realisiert wurde, in das Verfahren der dezentralen Suche eingebunden werden. [↑](#footnote-ref-8)
8. 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. [↑](#footnote-ref-9)
9. Pommerening, K, „Das Datenschutzkonzept der TMF für Biomaterialbanken“. **it – Information Technology** 49 (2007), 352–359 [↑](#footnote-ref-10)
10. Der Import von Biomaterialdaten folgt im Wesentlichen den Vorgaben im Datenschutzkonzept der TMF für Biomaterialbanken. [↑](#footnote-ref-11)
11. D.h. Personen, die nicht zu den Standorten des OSSE-Registers für „Seltene Erkrankung X“ gehören. [↑](#footnote-ref-12)
12. Dies sollte in der Regel im Rahmen des Arbeitsverhältnisses an der zuständigen Institution ohnehin geschehen sein. [↑](#footnote-ref-13)
13. Bei der Anonymisierung muss erreicht werden, dass eine Mindestanzahl von Fällen mit gleichen Merkmalsausprägungen existiert, damit Patienten nicht anhand ihrer medizinischen Daten erkannt werden können. Das wird beispielsweise durch Vergröberung von Merkmalsausprägungen in Form von Kategorien (z.B. Alterskohorten) realisiert. Eine solche Vergröberung ist nur sinnvoll, wenn das ursprüngliche Ziel der Datenverarbeitung damit weiterhin erreicht wird. [↑](#footnote-ref-14)
14. §20 BDSG [↑](#footnote-ref-15)
15. Die meist impraktikable Löschung oder Anonymisierung in Datensicherungen ist verzichtbar, sofern die Sicherungen nur durch den zuständigen Systemadministrator eingesehen werden können und alte Sicherungen regelmäßig gelöscht werden. [↑](#footnote-ref-16)