Datenmanagement im ILEG-Projekt

Inanspruchnahme, Leistungen und Effekte des Gemeindenotfallsanitäters

Datenschutzkonzept

Stand: 11.02.2021

Rainer Röhrig, Jonas Bienzeisler, Insa Seeger, Andrea Diana Klausen, Julia Volmerg

Ansprechpartner

Julia Volmerg
Institut für Medizinische Informatik
Uniklinik RWTH Aachen

Adresse: Pauwelsstraße 30 • D 52074 Aachen
Telefon.: +49 241 80-88870
Email: jbienzeisler@ukaachen.de

Prof. Dr. Rainer Röhrig
Institut für Medizinische Informatik
Uniklinik RWTH Aachen

Adresse: Pauwelsstraße 30 • D 52074 Aachen
Telefon.: +49 241 80-88790
Email: rroehrig@ukaachen.de

Version 1.0.4 vom 11.02.2021

Inhalt

Abkürzungs- und Symbolverzeichnis

DWH	Data Warehouse
TempID	Temporäre ID
IDAT	Patient*innen-Identifizierende Daten
MDAT	Medizinische Daten
PSN	Pseudonym

Glossar

Pseudonym/Pseudonymisierung: „die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifisch betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können." (Art. 4 Nr. 5 DSGVO)

Anonymisierung: Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann (Erwägungsgrund 26, DSGVO).

K-Anonymität: Eigenschaft von anonymisierte Datensätze. Die Daten von Individuen sind so weit verallgemeinert, dass es zu jedem Feld im Datensatz minimal k-1 Datenzwillinge gibt.

Data Warehouse: Eine für Analysezwecke optimierte zentrale Datenbank, die Daten aus mehreren, in der Regel heterogenen Quellen zusammenführt. Kurz geschrieben DWH; wörtlich „Datenlager".

Auswertestelle: Unabhängige Einrichtung zur Auswertung, Verarbeitung und datenschutzkonformen Weiterleitung der gesammelten medizinischen Daten an Forscher*innen. Stellt durch technische und organisatorische Maßnahmen sicher, dass die Daten nicht mit anderen Datenquellen verknüpft werden können. Wird von der Universitätsklinik für Unfallchirurgie an der Otto-von-Guericke-Universität Magdeburg betrieben.

Treuhandstelle: Unabhängige Einrichtung, die die Trennung von identifizierenden (IDAT) und medizinischen Daten (MDAT) umsetzt. Von der Treuhandstelle werden Patientenlisten geführt und medizinische Daten zweistufig pseudonymisiert.

Data Use and Access Committee (DUAC): W*issenschaftliches Kontrollgremium* für die Prüfung von Datenabfragen des AKTIN-Notaufnahmeregisters im Rahmen von Forschungsvorhaben. Prüft diese in Hinblick ethischer und datenschutzrechtlicher Gesichtspunkte und gibt entsprechende Datenauszüge frei.

1. Das Projekt

Im Oldenburger Land tragen Gemeindenotfallsanitäter*innen dazu bei, Rettungsdienste und Notaufnahmen zu entlasten. Gemeindenotfallsanitäter*innen sind speziell weitergebildete Notfallsanitäter*innen, die einen ressourcenschonenden Einsatz in solchen Fällen ermöglichen, bei denen in der Alarmierung der Rettungsleitstelle keine Notfall- bzw. Transportindikation zu bestehen scheint. Vor Ort greift der/die Gemeindenotfallsanitäter*in auf ein Netzwerk von verschiedenen Versorgungsmöglichkeiten zurück, indem er/sie Kontakt zu entsprechenden Institutionen, dem/der Hausarzt/Hausärztin oder dem kassenärztlichen Bereitschaftsdienst aufnimmt. Zur Einschätzung der Einsatzsituation kann der/die Gemeindenotfallsanitäter*in auf die telemedizinische Unterstützung durch Notärzte der Universitätsklinik für Anästhesiologie/Intensivmedizin/Notfallmedizin/Schmerztherapie (AINS) am Klinikum Oldenburg zurückgreifen. Als Rettungsmittel kommt ein Fahrzeug analog eines Notarzteinsatzfahrzeuges (NEF) zum Einsatz. Die Ausstattung wurde an den Bedarf des/der Gemeindenotfallsanitäters*in angepasst. Der/die Gemeindenotfallsanitäter*in ist Bestandteil des regulären Rettungsdienstes und unterliegt der medizinischen Aufsicht der ärztlichen Leiter Rettungsdienst. Das Handeln erfolgt leitlinienkonform anhand eigens erstellter Algorithmen. Der Gemeindenotfallsanitäter ist ein Pilotprojekt der Landkreise Ammerland, Cloppenburg, Vechta und der Stadt Oldenburg.

Die Effekte von Gemeindenotfallsanitätern auf die Versorgung im ländlichen Raum sollen im ILEG Projekt analysiert werden. Dabei werden Fragen zur Inanspruchnahme des Rettungsdienstes zu erbrachten Leistungen und zu möglichen Effekten auf die Versorgungsqualität und Wirtschaftlichkeit untersucht. Durch Verknüpfen von verschiedenen Datenquellen soll eine Datengrundlage geschaffen werden, um das Projekt steuern und ggf. auf weitere Landkreise ausweiten zu können. Im Forschungsvorhaben ist ein Multi-Modulares Vorgehen geplant. Es werden Leistellendaten, Gemeindenotfallsanitäter- und Rettungsdienstprotokolle, Routinedaten aus der Notaufnahmeversorgung (erhoben im AKTIN NotaufnahmeRegister), Daten einer Patientenbefragung sowie Daten einer Befragung der (ggf. nachbehandelnden) Hausärzte von teilnehmenden Patienten*innen erhoben und mithilfe einer Treuhandstelle unter einem Pseudonym verknüpft. Die gesammelten Daten können für spezifische wissenschaftliche Fragestellungen den Konsortialpartnern verfügbar gemacht werden – allerdings erst nachdem ein *wissenschaftliches Kontrollgremium,* das *Data Use and Access Committee (DUAC),* eine entsprechende Anfrage geprüft und genehmigt hat.

Für die Datenerhebung im Projekt werden zwei informierte Einwilligungen eingeholt. Während des Einsatzes des/der Gemeindenotfallsanitäters*in wird eine *erste* Einwilligung (EWE1) zum Zwecke der postalischen Kontaktierung für die Einholung einer *zweiten* informierten Einwilligung (EWE2) eingeholt. In der zweiten Einwilligung stimmt der/die Patient*in der Datenerhebung im Projekt zu. Dieses zweistufige Vorgehen ist notwendig, da in einer Notfallsituation das Einholen einer informierten Einwilligung den Patienten*innen nicht zugemutet werden kann (Vgl. Tabelle 1).

1.1 Hintergrund

Die Versorgung von Patienten*innen in Notfallsituationen ist eine der wichtigsten Aufgaben im Gesundheitswesen. In den vergangenen Jahren sind die Patientenzahlen in den Notaufnahmen und bei den Rettungsdiensten stetig angestiegen, während die Anzahl von Notfällen beim kassenärztlichen Bereitschaftsdienst immer weiter gesunken ist. Die Ausgaben für Rettungsdienste sind während dieses Zeitraums enorm gestiegen: Im Jahr 2005 wurden insgesamt 2,6 Millionen Euro für Rettungsdienste ausgegeben während es im Jahr 2015 bereits 4,6 Millionen Euro waren. Dies ist jedoch nicht mit einem Anstieg lebensbedrohlicher Notfälle begründet. Vielmehr nutzen mehr Patienten*innen den Rettungsdienst oder die Notaufnahmen, obwohl sie eigentlich vor Ort versorgt werden könnten. Im Oldenburger Land sollen „Gemeindenotfallsanitäter“ dazu beitragen, Rettungsdienst und Notaufnahmen zu entlasten. Diese beurteilen die Notlage der Patienten*innen und versorgen sie ggf.

vor Ort. Die Gemeindenotfallsanitäter*innen entscheiden, falls möglich, auch über die weitere Behandlung. Gemeindenotfallsanitäter*innen werden dann eingesetzt, wenn eine lebensbedrohliche Verletzung oder Erkrankung bereits durch die Leitstelle ausgeschlossen werden konnte, ohne einen persönlichen Kontakt mit den Patienten*innen aber nicht darüber entschieden werden kann, ob sie bei einer anderen Versorgungseinrichtung vorstellig werden sollten. Gemeindenotfallsanitäter*innen sind eine neue Qualität an Einsatzmittel. Daran werden unterschiedliche Erwartungen geknüpft, insbesondere die Entlastung des Rettungsdienstes und der Notaufnahmen durch eine Reduktion von Fehlinanspruchnahmen. Dabei gilt es sicherzustellen, das neue Einsatzmittel so einzusetzen, dass es nicht zu Verzögerungen bis zu der notwendigen und angemessenen Versorgung kommt.

Tabelle 1: Einwilligungen im ILEG Projekt

Einwilligung		Inhalt	Eingeholt durch
Einwilligung Datenverarbeitung für die Kontaktierung für Forschungsvorhaben	EWE1	• Einwilligung in die Kontaktierung für die Rekrutierung für das Forschungsvorhaben. • Entbindung der Rettungsdienste von der ärztlichen Schweigepflicht • Einwilligung in der Verarbeitung von Kontaktdaten und Einsatznummer des Gemeindenotfallsanitäter-einsatzes.	Gemeindenotfallsanitäter während des Einsatzes
Einwilligung Datenverarbeitung im Projekt	EWE2	• Einwilligung für die pseudonyme Erhebung und Verarbeitung der im Projekt erhobenen Daten. • Einwilligung für die Verknüpfung der im Projekt erhobenen Daten. Entbindung der beteiligten Institutionen von der ärztlichen Schweigepflicht	Postalisch durch das Studienzentrum

1.1 Zweck der Datenverarbeitung

Die Daten im ILEG-Projekt werden zu folgenden Zwecken erhoben:

1. Beantwortung der Forschungsfragen des ILEG Projekts
   - Ändert sich die Häufigkeit der Inanspruchnahme des Rettungsdienstes (Primäre Zielstellung)?
   - Ändert sich die Häufigkeit der Inanspruchnahme der weiter versorgenden Einrichtungen?
   - Sind Sicherheit und Versorgungsqualität gewährleistet?
   - Wie häufig und mit welchem Effekt erfolgt eine Inanspruchnahme der Telemedizin?
   - Ändert sich die Häufigkeit der Inanspruchnahme der Notrufnummer 112?
   - Ist das Modell „Gemeindenotfallsanitäter“ wirtschaftlich sinnvoll?

2. Einrichtungsübergreifendes Qualitätsmanagement
3. Einrichtungsübergreifende Versorgungsforschung in der Akutmedizin

Das Ziel dieses Forschungsvorhabens ist die Auswirkung des Rettungsmittel Gemeindenotfallsanitäter*in auf die Inanspruchnahme und Versorgung von nicht lebensbedrohlichen erkrankten Patienten*innen zu untersuchen. Es sollen erbrachte Leistungen und Effekte auf die Versorgungsqualität und Wirtschaftlichkeit untersucht werden und damit eine Datengrundlage für die Steuerung und ggf. Ausweitung des Projektes auf weitere Landkreise oder die Regelversorgung geschaffen werden.

1.2 Umfang der Datenverarbeitung

Im Rahmen des ILEG Projekts werden (vorbehaltlich der Einwilligung der Patienten*innen) Daten von allen Patienten*innen, die von Gemeindenotfallsanitäter*innen im Jahre 2021 behandelt werden, verarbeitet. Dies erfolgt für teilnehmende Patienten*innen ggf. rückwirkend für das gesamte Jahr 2021 ab dem Zeitpunkt der Einholung der Einwilligung in die Datenverarbeitung. Es ist geplant, ca. 1.000 Patienten*innen in das Projekt einzubeziehen. Es werden zwei Einwilligungen eingeholt. Mit der ersten Einwilligung – die bei den Patienten*innen durch die Gemeindenotfallsanitäter*innen eingeholt wird – stimmt der/die Patient*in einer Kontaktierung zum Zwecke von Patientenbefragungen zu. In der zweiten Einwilligung – die zu einem späteren Zeitpunkt postalisch eingeholt wird – stimmt der/die Patient*in einer Verarbeitung und Verknüpfung von Gesundheitsdaten zu.

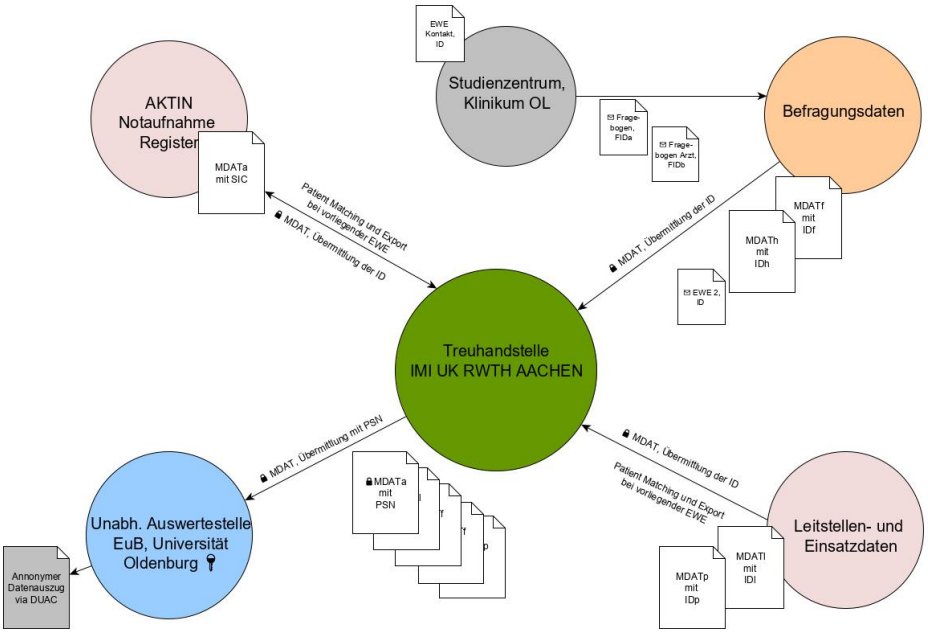

Abbildung 1: Schematischer Datenfluss von Dateneignern zur Treuhandstelle. Die Daten werden dezentral beim Dateneigner erhoben und zentral anhand von identifizierenden Merkmalen (IDAT) in der Treuhandstelle verknüpft. Die medizinischen Daten werden verschlüsselt von den Dateneignern direkt an die Auswertestelle weitergeleitet. Daten von klinischen Modulen im Sinne des organisatorischen und technischen Konzepts für Forschungsverbünde der TMF in rot, Studienmodule orange, Forschungsmodul in blau.

Im Forschungsvorhaben ist ein Multi-Modulares Vorgehen geplant. Es werden Daten aus verschiedenen Datenquellen verknüpft und pseudonym verarbeitet, um eine ganzheitliche Datengrundlage für Auswertungen zu schaffen. Es werden Leistellendaten, Gemeindenotfallsanitäter- und Rettungsdienstprotokolle, Routinedaten aus der Notaufnahmeversorgung und Abrechnungsdaten der Kliniken (erhoben im AKTIN NotaufnahmeRegister), Daten einer Patientenbefragung sowie Daten

einer Befragung der (ggf. nachbehandelnden) Hausärzten von teilnehmenden Patienten*innen verknüpft und erhoben.

Im Falle der Befragungen werden die Daten vom Studienzentrum primär für das Projekt erhoben. Alle medizinischen Daten (*MDAT*) werden von den entsprechenden Dateneignern selbstständig zu Dokumentationszwecken erhoben und für die Verknüpfung im Rahmen des ILEG Projekts zur Sekundärnutzung zur Verfügung gestellt. Die Daten werden zentral über Pseudonyme verknüpft und dann gesammelt ausgewertet. Dies geschieht mithilfe einer *Treuhandstelle,* die die zu den MDAT gehörende Pseudonyme an eine *Auswertestelle* unabhängig von den medizinischen Daten vermittelt. Die Treuhandstelle ist zweigeteilt in eine Patientenliste, in der patientenidentifizierende Daten verwaltet werden und einen Pseudonymisierungsdienst, der die medizinischen Daten unabhängig von den patientenidentifizierenden Daten pseudonymisiert und so eine Verknüpfung mehrerer Datenquellen ermöglicht. Die MDAT werden von den Dateneignern verschlüsselt und direkt an die Auswertestelle übermittelt.

1.2.1 Datenerhebung gemäß Leitfaden zum Datenschutz der TMF

Dieses Datenschutzkonzept folgt dem Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – generische Lösungen der TMF 2.0 [1]. Die Datenerhebung in den Rettungsdiensten erfolgt gemäß des *klinischen Moduls* im Sinne des organisatorischen und technischen Konzepts für Forschungsverbünde der TMF. Die Erhebung der Daten in den Kliniken im Rahmen des AKTIN Notaufnahme Registers erfolgt ebenfalls gemäß dem klinischen Modul. Die Infrastruktur des deutschen Notaufnahmeregisters – entstanden im Rahmen des AKTIN Notaufnahme Registers – wurde bereits von der TMF begutachtet. Im Gegensatz zu diesem werden für das ILEG Projekt allerdings pseudonyme Daten auf Basis einer Einwilligung (EWE2) der teilnehmenden Patienten*innen durchgeführt.

Die Daten der Befragungen von sowohl Patienten*innen als auch den zugehörigen Hausärzten liegen im Sinne der TMF in Studienmodulen vor. Für die pseudonymisierte Speicherung und Verarbeitung der Daten im Studienmodul ist Grundsätzlich unabhängig von der langfristigen Verarbeitung in einer Forschungsdatenbank im Gesamtprojekt und setzen als Rechtsgrundlage eine informierte Einwilligung (EWE1) der Patienten*innen voraus. Für die Befragungen von Patienten*innen und Hausärzten*innen durch das Studienzentrum des Klinikums Oldenburg (in Zusammenarbeit mit dem Fragebogenlabor der Carl von Ossietzky Universität Oldenburg) wird im Sinne der TMF ein Kontaktmanagement eingerichtet. Die Betroffenen Patienten*innen werden durch Forschungspersonal kontaktiert. Die Kontaktierung der Patienten*innen wird durch die EWE1 abgedeckt. Für ein solches Studienmodule wird keine doppelte Pseudonymisierung gemäß Modell B in der ersten Version der generischen Datenschutzkonzepte der TMF vorausgesetzt [1].

Gemäß den Vorgaben der TMF sind zusätzliche Schutzmaßnahmen dann erforderlich, wenn die Daten einer Studie oder eines Forschungsprojekts nach dessen Ende weiterhin in pseudonymisierter Form gespeichert und mit den Daten aus anderen Forschungsprojekten zusammengeführt werden sollen. Eine solche Auswertung der verschiedenen klinischen bzw. Studienmodule im ILEG Projekt erfolgt durch die Auswertestelle in der Abteilung für Epidemiologie und Biometrie an der Carl von Ossietzky Universität Oldenburg. Damit die Daten dort im Sinne eines *Forschungsmoduls* gemäß TMF zusammen verarbeitet werden können, wird ein Treuhänder im Sinne des generischen Datenschutzkonzeptes der TMF eingesetzt. Das treuhänderische Führen des Identitätsmanagements in einer *Treuhandstelle* erfolgt durch das Institut für Medizinische Informatik des Uniklinikums RWTH Aachen.

1.3 Organisationsstruktur und Verantwortlichkeiten

Das Projekt ILEG wird unter Leitung des Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin der Universität Oldenburg, der Universität Oldenburg (Fakultät VI: Abteilung für Epidemiologie und Biometrie sowie die Abteilung Organisationsbezogene Versorgungsforschung), dem Universitätsklinikum Magdeburg (Universitätsklinik für Unfallchirurgie), dem Uniklinikum RWTH

Aachen (Institut für Medizinische Informatik), der Universität Maastricht (Care and Public Health Research Institute, Faculty of Health, Medicine and Life Sciences) durchgeführt. Beteiligt sind außerdem die Oldenburger Kliniken (Pius-Hospital Oldenburg, Evangelisches Krankenhaus Oldenburg, Klinikum Oldenburg) sowie die Rettungsdienste und Leitstellen der am Projekt beteiligten Landkreise und die Telemedizinzentrale am Klinikum Oldenburg (Vgl. Anlage 1 – Beteiligte Projektpartner).

1.3.1 Dateneigner

Dateneigner stellen die im Projekt Daten für Forschungszwecke bereit und wirken bei der Verknüpfung der Daten üben den die Treuhandstelle mit. Bei diesen Daten handelt es sich um Fragebogen- und Routinedaten. Letztere werden primär zu Dokumentationszwecken gesammelt werden und im Rahmen des Projekts für sekundäre Auswertungen zur Verfügung gestellt werden. Alle Datenlieferanten verpflichten sich gegenüber dem Konsortialführer, an der Datenverarbeitung wie in dieser Vereinbarung beschrieben mitzuwirken, insbesondere an den Prozessen zur Erfüllung der Betroffenenrechte (vgl. Abschnitt 3).

Rettungsdienste

Die Rettungsdienste der am Projekt beteiligten Landkreise

- Rettungsdienst Stadt Oldenburg
- Malteser Hilfsdienst gGmbH, Landkreis Vechta
- Malteser Hilfsdienst gGmbH, Bezirk Oldenburg-Nord
- Deutsches Rotes Kreuz Cloppenburg
- Rettungsdienst Ammerland GmbH

entsenden Gemeindenotfallsanitäter*innen und erheben die Einwilligungen der Patienten*innen für eine Kontaktierung im Rahmen einer Patientenbefragung. Die Rettungsdienste stellen alle Einsatzprotokolle dem Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin anonymisiert und für das Forschungsprojekt pseudonymisiert zur Verfügung – allerdings nur Daten von Patienten*innen, die der Teilnahme an der Studie zugestimmt haben. Die Rettungsdienste erheben Gemeindenotfallsanitäter- und Rettungsdienstprotokolle und übermitteln diese dann für die digitale Erfassung an das Fragebogenlabor. Ferner wirken die Rettungsdienste bei der Pseudonymisierung und Verknüpfung dieser Daten über die Treuhandstelle mit.

Leitstellen

Die Leitstellen der am Projekt beteiligten Landkreise

- Einsatzleitstelle Vechta, Sachgebietsleitung Feuerschutz und Rettungswesen, Landkreis Vechta
- Großleitstelle Oldenburger Land

erheben Leitstellendaten und übermitteln diese pseudonymisiert an die Auswertestelle – allerdings nur von Patienten*innen, die der Teilnahme an der Studie zugestimmt haben. Ferner wirken die Leitstellen bei der Pseudonymisierung und Verknüpfung der Daten über die Treuhandstelle mit.

Kliniken

Behandlungsdaten der teilnehmenden Notaufnahmen bzw. Krankenhäuser werden in Kliniken der am Projekt beteiligten Landkreise erhoben, die der Forschungsdateninfrastruktur des AKTIN Notaufnahme Register angehören. In den Kliniken wird die klinische Dokumentation routinemäßig auf Basis des Notaufnahmeprotokolls der DIVI e. V. erfasst und im Rahmen des Nationalen Notaufnahme Register (AKTIN) für die sekundäre Analyse zur Verfügung gestellt. Am Projekt beteiligt sind

- Evangelisches Krankenhaus Oldenburg
- Pius-Hospital Oldenburg
- Klinikum Oldenburg

Die Kliniken übermitteln pseudonymisierte Routinedokumentation und Abrechnungsdaten für Forschungszwecke an die Auswertestelle. Ferner wirken die Kliniken bei der Pseudonymisierung und Verknüpfung der Daten über die Treuhandstelle mit. Es gilt das Datenschutzkonzept des AKTIN Notaufnahme Register (vgl. Anlage 3 – Datensatznotaufnahmeprotokoll).

Telemedizinzentrale

Die Telemedizinzentrale am Klinikum Oldenburg erhebt und übermittelt routinemäßige Dokumentation (Notaufnahmeprotokolls der DIVI e. V.) pseudonymisiert an die Auswertestelle – allerdings nur von Patienten*innen, die der Teilnahme an der Studie zugestimmt haben. Ferner wirkt die Telemedizinzentrale bei der Pseudonymisierung und Verknüpfung der Daten über die Treuhandstelle mit.

Studienzentrum

Das Studienzentrum des Klinikum Oldenburg kontaktiert postalisch Patienten*innen sowie Hausärzte der Patienten*innen und führt eine Patientenbefragung durch. Eine (erste) Einwilligung für die bloße postalische Kontaktierung wird für das Studienzentrum von den Gemeindenotfallsanitäter*innen bei einem Einsatz eingeholt. Das unterschriebene Einwilligungsformular wird sicher vom Studienzentrum aufbewahrt und der Umfang der Einwilligung im Kontaktmanagement gespeichert. Die Befragungen werden vom Studienzentrum nach dem Einsatz der Gemeindenotfallsanitäter*innen zusammen mit einer (zweiten) Einwilligung zur Erhebung und Verknüpfung aller weiteren Datenquellen an die Betroffenen verschickt. Die pseudonymen, wiedereingetroffenen und ausgefüllten Befragungen werden vom Studienzentrum an das Fragebogenlabor für die elektronische Erfassung weitergeleitet. Zwischen Studienzentrum und Fragebogenlabor wird eine Vereinbarung gemäß Art. 26 DSGVO geschlossen.

Das Studienzentrum registriert die Einwilligungserklärung (EWE1) und – unter Voraussetzung einer erfolgten zweiten Einwilligung (EWE2) – die ID der zweiten Einwilligung und Fragebögen-IDs im Identitätsmanagement der Treuhandstelle.

1.3.2 Fragebogenlabor

Das Fragebogenlabor der Abteilung Organisationsbezogene Versorgungsforschung erfasst im Auftrag von Dateneignern automatisiert in Papierform erhobene Dokumente, verschlüsselt und leitet über die Treuhandstelle die Daten pseudonymisiert an die Auswertestelle – allerdings nur Daten von Patienten*innen, die der Teilnahme an der Studie zugestimmt haben.

1.3.3 Treuhandstelle

Um eine informationelle Gewaltentrennung gemäß dem Leitfaden zum Datenschutz der TMF zu erreichen, wird eine von der Datenerhebung unabhängige Treuhandstelle eingerichtet. Diese ist nur für die Trennung von identifizierenden und medizinischen Daten zuständig und wird vom Institut für Medizininformatik des Uniklinikums RWTH Aachen von einem/einer zuständigen Mitarbeiter*in betrieben. Die geforderte Unabhängigkeit für eine solche Treuhandstelle wird durch die Unabhängigkeit der Person von der Datengewinnung, anderen Projekten der Uniklinik RWTH Aachen und durch Trennung der Daten von anderen Daten der Uniklinik RWTH Aachen erreicht. Die eigens für das Projekt eingerichtete VM ist nur im internen RWTH-Netz, und auch hier eingeschränkt durch ein Loginverfahren per PublicKey/PrivateKey erreichbar. Die bereitgestellte Anwendung zur IDAT-Verwaltung kann ebenso nur per Login erreicht werden, und der Zugriff wurde weiter eingeschränkt in dem die IDAT zwar eingegeben, nicht aber nochmals eingesehen werden können.

Der Treuhänder arbeitet mandantenspezifisch und wird nur für das ILEG-Projekt eingerichtet. Der Treuhänder besteht aus

- Identitätsmanagement in Form einer Patientenliste als E-PIX Instanz [1]
- Pseudonymisierungsdienst in Form einer gPAS Instanz[2]

Vom Identitätsmanagement werden - unter Wahrung des Datenschutzes – die Pseudonyme der ersten Stufe in einer Patientenliste geführt. Es werden Software (E-PIX, gPAS) und Infrastruktur für die Verlinkung und Pseudonymisierung von medizinischen Daten für die Dateneigner bereitgestellt (vgl. Abschnitt 2.3). Es wird eine Software für die lokale Verschlüsselung der MDAT zur Verfügung gestellt.

Der Pseudonymisierungsdienst führt und verwaltet unter Wahrung des Datenschutzes Pseudonyme der zweiten Stufe (PSN). Diese dienen dazu, die Pseudonyme zwischen den Dateneignern und der Auswertestelle zu vermitteln (siehe Abbildung 3). Der Pseudonymisierungsdienst stellt Software (gPAS) und Infrastruktur für die Verlinkung und Weiterleitung von medizinischen Daten bereit (vgl. Abschnitt 2.3). Die Software wird für die Erzeugung von Pseudonymen zweiter Stufe (PSN) für die Zuordnung der Datensätze genutzt (vgl. Abb. 3).

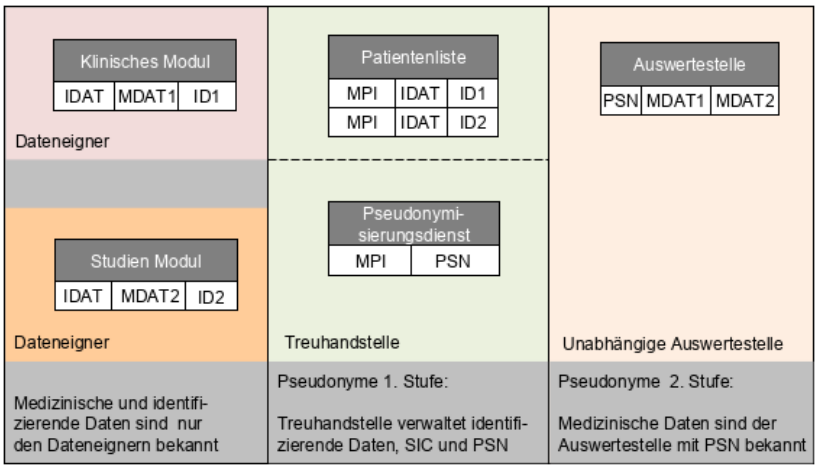

Abbildung 3: Prinzip der Pseudonymgenerierung. Die Treuhandstelle am Institut für Medizinische Informatik des Uniklinikum RWTH Aachen vermittelt Pseudonyme 1. (ID) und 2. Stufe (PSN) an die Auswertestelle im ILEG Projekt.

1.3.4 Auswertestelle

Die Abteilung für Epidemiologie und Biometrie an der Carl von Ossietzky Universität Oldenburg richtet eine Auswertestelle ein, die die pseudonymisierten Daten verwaltet. Die Auswertestelle führt Analysen durch und stellt durch technische und organisatorische Maßnahmen sicher, dass die Daten nicht mit anderen Datenquellen verknüpft werden können. Sollten Konsortialpartner anonyme Datenauszüge für Forschungsfragen benötigen, so werden diese von der Auswertestelle aufbereitet, ggfs. vergröbert und in Zusammenarbeit mit dem Data-Use-and-Access-Komitee an Konsortialpartner übermittelt. An Dritte, nicht an dem Projekt beteiligte Partner, können aggregierten Daten in Rahmen von Forschungsanfragen übermittelt werden.

1.3.5 Data Use and Access Committee

Es wird ein Data-Use-and-Access-Komitee (DUAK) unter der Leitung der Konsortialführung und unter Beteiligung der Treuhandstelle, der Auswertestelle, eines Vertreters der Rettungsdienste und eines Vertreters der Modellkliniken eingerichtet. Die Bereitstellung eines anonymen Datensatzes kann dort von Konsortialpartnern beantragt werden. Das Komitee prüft den Antrag und teilt eine positive Bewertung der Auswertestelle mit, die dann den jeweiligen Datenauszug entsprechend der Vorgaben

[1] https://www.ths-greifswald.de/forscher/e-pix/
[2] https://www.ths-greifswald.de/forscher/gpas/

(bspw. bezüglich K-Annonymität und i-Diversität) des DUAK erstellt. Das genaue Vorgehen wird in einer Verfahrensordnung festgelegt.

1.3.6 Dateninterpreten

Interpretierende Konsortialpartner können Datenauszüge auf der Grundlage einer formulierten Fragestellung und bezugnehmend auf ein *Data Dictionary* für alle Datenquellen des Projektes über das Data-Use-and-Access-Komitee beantragen.

1.3.7 ILEG Geschäftsstelle

Die ILEG Geschäftsstelle wird vom Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin der Universität Oldenburg betrieben. Die ILEG Geschäftsstelle betreut die (nicht-technischen) organisatorischen Vorgänge im ILEG-Projekt und stellt die Projektleitung.

1.3.8 Finanzierung

Das Projekt wird vom Innovationsfonds finanziert, Förderkennzeichen 01VSF19017.

1.4 Anfallende Daten

Im ILEG Projekt sollen Daten von n = 1.000 Patienten*innen die von Gemeindenotfallsanitäter*innen behandelt wurden, ausgewertet werden. Es fallen Einsatzdaten des Rettungsdienstes, Leitstellendaten, Behandlungsdaten von Kliniken bzw. Notaufnahmen sowie Daten einer Patientenbefragung und Daten einer Hausarztbefragung an. Sämtliche Daten werden auf Fall- und Patientenebene mit einem Pseudonym erster Stufe für das Projekt zur Verfügung gestellt, dass auf Patienten*innen zurückgeführt werden kann.

Daten	**Datenquelle**	**Pseudonym (1.Stufe)**
Einwilligungsmanagement		
Einwilligung in Kontaktaufnahme	Einwillligungserklärung 1	EWE_ID1
Einwilligung in Projektteilnahme	Einwillligungserklärung 2	EWE_ID2
Kontaktdaten	Einwillligungserklärung 1	-
Einsatzdaten des Rettungsdienstes		
Gemeindenotfallsanitäterprotokoll	Gemeindenotfallsanitäterprotokoll ausgefüllt durch Gemeindenotfallsanitäter	Einsatznummer, PID_RD
Rettungsdienstprotokoll	Rettungsdienstprotokoll DIVI, ausgefüllt durch Rettungsdienst	Einsatznummer
Notarzteinsatzprotokoll	Notarzteinsatzprotokoll DIVI, ausgefüllt durch Notarzt	Einsatznummer
Telemedizinzentrale		

Telenotarzteinsatzprotokoll	DIVI-Notaufnahmeprotokoll, ausgefüllt durch Telenotarzt in der Telemedizinzentrale am Klinikum Oldenburg	Einsatznummer
Leitstellendaten		
Einsatzdokumentation	Leitstellendaten auf Einsatzebene	Einsatznummer
Klinische Daten		
Klinische Routinedokumentation auf Individualebene	Datensatz Notaufnahme DIVI, AKTIN Notaufnahmeregister	SIC
Leistungsdaten Krankenhaus	Entlassdaten der Krankenhäuser in einem Standardformat analog zum §21-Datensatz, AKTIN Notaufnahmeregister	SIC
Befragungen		
Patientenbefragung	Fragebogen Patientenbefragung	FID_Pat
Hausarztbefragung	Fragebogen Hausarztbefragungen	FID_Doc

1.4.1 Einsatzdaten des Rettungsdienstes

Die Archivierung aller medizinisch relevanten Behandlungsunterlagen gehört zu den allgemeinen Dokumentations- und Aufbewahrungspflichten der teilnehmenden Rettungsdienste. Routinemäßig erhobene Einsatzdaten werden von den Rettungsdiensten für die Sekundärnutzung im ILEG Projekt zur Verfügung gestellt. Bei jedem Rettungsdiensteinsatz wird ein DIVI-Rettungsdienstprotokoll von jedem Einsatzmittel ausgefüllt (vgl. Anlage 9 – Datensatzbeschreibung Datensatz Rettungsdienst). Der Datensatz besteht aus Stamm-, Rettungstechnischen-, Befund-, Diagnose- und Vitaldaten. Die Daten der DIVI-Rettungsdienstprotokolle werden digital und strukturiert von den Rettungsdiensten in einer Datenbank mit Einsatznummer und identifizierenden Daten (Name, Vorname, Geburtsdatum) erfasst. Wird ein Notarzt eingesetzt, so erfolgt eine Dokumentation im DIVI-Notarzteinsatzprotokoll mit Einsatznummer. Der Datensatz besteht aus Stamm-, Rettungstechnischen-, Befund-, Diagnose- und Vitaldaten. Die Daten der DIVI- Notarzteinsatzprotokolle werden digital und strukturiert von den Rettungsdiensten in einer Datenbank mit Einsatznummer und identifizierenden Daten (Name, Vorname, Geburtsdatum) erfasst.

Wird ein/e Gemeindenotfallsanitäter*in eingesetzt, erfolgt eine Dokumentation auf einem gesonderten Bogen (vgl. Anlage 9 – Datensatzbeschreibung Datensatz Rettungsdienst). Dieser Bogen als Formular ausgefüllt, welches von den Rettungsdienstengescannt und sowohl in anonymisierter wie in pseudonymisierter Form (teilnehmende Patienten*innen) im Fragebogenlabor (Uni OL-OVF) in eine Datenbank eingelesen wird.

Die Telemedizinzentrale am Klinikum Oldenburg stellt Daten von Gemeindenotfallsanitätereinsätzen mit Beteiligung des Telenotarztes zur Verfügung. Wird ein Telenotarzt eingesetzt, so erfolgt eine Dokumentation im DIVI- Notaufnahmeprotokoll mit XXX-Nummer. Der Datensatz besteht aus Stamm-, Rettungstechnischen, Befund-, Diagnose- und Vitaldaten. Die Daten der DIVI- Notaufnahmeprotokolls werden digital von der Telemedizinzentrale am Klinikum Oldenburg in einer Datenbank mit XXX-Nummer und identifizierenden Daten (Name, Vorname, Geburtsdatum) erfasst.

1.4.2 Leitstellendaten

Die Speicherung und Archivierung der medizinisch relevanten Einsatzdaten gehört zu den allgemeinen Dokumentations- und Aufbewahrungspflichten der teilnehmenden Leitstellen. Routinemäßig erhobene Einsatzdaten werden von den Leitstellen für die Sekundär-Nutzung im ILEG Projekt zur Verfügung gestellt (vgl. Anlage 11). Ein Datensatz besteht aus Orts-, Dispositions- und Zeitdaten sowie aus den Einsatzrückmeldungen, dem PZC-Code und ggf. der Zielklink. Die Daten werden digital und strukturiert von den Leitstellen in einer Datenbank mit einer Haupt- und ggf. Untereinsatznummer und ggf. mit identifizierenden Daten (Name) erfasst. Klinische Daten

Die Archivierung aller medizinisch relevanten Behandlungsunterlagen gehört zu den allgemeinen ärztlichen Dokumentations- und Aufbewahrungspflichten der teilnehmenden Kliniken. Für die Auswertung von möglichen klinischen Behandlungen von Patienten*innen sollen die klinische Routinedokumentation auf Individualebene in der Notaufnahme, stationäre Abrechnungsdaten und Daten der Telemedizinzentrale am Klinikum Oldenburg ausgewertet werden. Die beteiligten Kliniken stellen diese Daten für die Sekundärnutzung im ILEG Projekt zur Verfügung. Sowohl Notaufnahme- als auch Abrechnungsdaten werden über die Infrastruktur des AKTIN Notaufnahmeregisters zur Verfügung gestellt. Datenquelle für die klinischen Daten aller teilnehmenden Patienten*innen ist der Datensatz Notaufnahme der DIVI, der im Notaufnahme-Informationssystem erfasst wird (siehe Anlage 3 – Datensatzbeschreibung Datensatz Notaufnahmeprotokoll). Die teilnehmenden Kliniken stellen Entlassdaten der Krankenhäuser in einem Standardformat analog zum §21-Datensatz zur Verfügung (siehe Anlage 11 – Datensatzbeschreibung Entlassdaten).

1.4.3 Befragungsdaten

Das Studienzentrum des Klinikums Oldenburg führt sowohl eine Patienten- als auch eine Hausarztbefragung durch. Es werden Fragen zur Behandlung durch die Gemeindenotfall-sanitäter*innen sowie zur Inanspruchnahme von medizinischer Versorgung gestellt. Zufriedenheit als weiterer patientenrelevanter Endpunkt wird als *patient-reported outcome* erhoben. Die Patientenbefragung erfolgt ca. zwei Wochen nach Inanspruchnahme der Gemeindenotfallsanitäter*innen (siehe Anlage 12 – Patientenbefragung). Die Befragung der Hausärzte der jeweilige Patient*innen erfolgt nach ca. 1 bis 3 Wochen nach Inanspruchnahme der Gemeindenotfallsanitäter*innen.

1.5 Risikobewertung der vorgesehenen Verarbeitungsvorgänge

Die Verarbeitung im Rahmen des ILEG Projektes hat 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.

1.5.1 Datenkategorien

Bei den Daten (vgl. Tabelle 1) handelt es sich i. S. d. Artikel 9 Abs. 1 bzw. Artikel 4 Nr. 15 DSGVO um Gesundheitsdaten. Alle aufgeführten Datenkategorien sind im Sinne der Datenvermeidung und Datensparsamkeit für die Beantwortung der Forschungsfragen nötig: Benötigte medizinische Daten werden zum Zwecke der Evaluierung der Forschungsfragen gesammelt. Die genauen Inhalte der Datensätze wurden von einer Experten*innenrunde ausgewählt, denen sowohl Rettungsdienste, Wissenschaftler, Ärztliche Leiter der Rettungsdienste und Ärzte angehörten. Eine detaillierte Datensatzbeschreibung findet sich in den Anlagen. Diese wird entsprechend des aktuellen Stands laufend fortgeschrieben. Die Nutzung der Daten ist ausschließlich für das Forschungsprojekt vorgesehen. Eine andere Nutzung dieser Daten als zum beschriebenen Forschungszweck findet nicht statt. Es ist gewährleistet, dass die Bestimmungen des Datenschutzes eingehalten und ausschließlich die Daten ausgewertet werden, die für den Forschungszweck erforderlich sind.

1.5.2 Schutzbedarf und Risikoklassifizierung

Bei den im Projekt erhobenen Gesundheitsdaten handelt es sich im Sinne der DSGVO um personenbezogene Daten der besonderen Kategorie. Für diese Daten gilt ein hoher Schutzbedarf bzw. sehr hoher Schutzbedarf. Insbesondere Daten mit sehr hohem Schutzbedarf werden von der Treuhandstelle verwaltet. Für alle weiteren Daten, die gesammelt erhoben werden, gelten Maßnahmen entsprechend des höchsten Schutzbedarfs der enthaltenen Daten. Technische und organisatorische Maßnahmen - passend zum jeweiligen Schutzbedarf bzw. der Schutzklassen - finden sich in Kapitel 2.

Tabelle 2: Schutzbedarf und Risikoklassifizierung nach DIN 66399

Daten	Schutzbedarf	Risikoklasse
Einsatzdaten des Rettungsdienstes		
Gemeindenotfallsanitäterprotokoll	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Rettungsdienstprotokoll	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Notarzteinsatzprotokoll	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Telemedizinzentrale		
Telenotarzteinsatzprotokoll	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Leitstellendaten		
Einsatzdokumentation	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Klinische Daten		
Klinische Routinedokumentation auf Individualebene	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Leistungsdaten Krankenhaus	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Befragungen		
Patientenbefragung	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Hausarztbefragung	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Kontaktdaten zum Zwecke der Kontaktierung	Normaler Schutzbedarf, ein möglichen Schaden kann den Betroffenen beeinträchtigen	1
Organisatorische Daten (Treuhandstelle)		
Patienten-Listen	Sehr hoher Schutzbedarf, Schwere eines möglichen Schadens ist groß	3

Pseudonymisierungslisten	Sehr hoher Schutzbedarf, Schwere eines möglichen Schadens ist groß	3
Kontaktdaten zum Zwecke der Kontaktierung	Normaler Schutzbedarf, ein möglichen Schaden kann den Betroffenen beeinträchtigen	1

1.5.3 Re-Identifizierungsmöglichkeiten

Die Daten liegen für die Auswertung in pseudonymisierter Form i. S. d. Artikel 4 Nr. 5 DSGVO in der Auswertestelle vor. Die Pseudonyme (PSN) des Auswerte-Datensatzes können nur durch das Zusammenwirken der Treuhandstelle und eines Dateneigners einer spezifischen Person zugeordnet werden. Eine vollkommen anonyme Verarbeitung ist nicht möglich, da die Daten verschiedener Dateneigner zu verschiedenen Zeitpunkten auf Personenebene zusammengeführt werden müssen, um Verlaufsbetrachtungen für Patienten*innen zu ermöglichen. Die pseudonymen Daten werden in einer gesicherten Umgebung von der Auswertestelle aufbewahrt. Von DUAC und Auswertestelle wird sichergestellt, dass im Falle einer Weitergabe von anonymen Daten an auswertende Projektpartner die Kriterien der k-Anonymisierung und l-Diversität eingehalten werden.

Bezüglich der verarbeiteten Einzelangaben sind auch in der zusammengeführten Form keine besonderen Re-Identifizierungsrisiken bekannt. Insbesondere besteht durch Hinzufügen von bzw. Vergleich mit öffentlich zugänglichen Informationen eine geringe Wahrscheinlichkeit, die Daten einer Person zuordnen zu können.

Die Daten werden generell ohne Personenbezug veröffentlicht. Es werden ausschließlich aggregierte Informationen veröffentlicht, die insbesondere keine Rückschlüsse zulassen auf einzelne:

- Patienten*innen
- Krankenhausmitarbeiter*innen
- Krankenhäuser
- Rettungsdienstmitarbeiter*innen
- Notärzte*innen
- Hausärzte*innen
- Leitstellenmitarbeiter*innen

1.6 Ethische und regulatorische Anforderungen

Zu jedem Zeitpunkt des Projektes werden die Datenschutzbestimmungen der Europäischen Union (EU), des Bundes und des Landes eingehalten. An den Stellen, an denen ein bereichsspezifisches Gesetz den Eingriff in das informationelle Selbstbestimmungsrecht spezifischer als ein allgemeineres Datenschutzgesetz regelt, wird auf die entsprechende Rechtsgrundlage hingewiesen. Das Projektkonsortium verpflichtet sich, die Datenschutzvereinbarung mittels neuer Anlagen zu aktualisieren, wenn dies durch technische Entwicklungen oder eintretende Gesetzesänderungen nötig wird. Für den Datenschutz finden die EU-Datenschutzgrundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG) Anwendung. Bezüglich der Verarbeitung von Sekundärdaten der Krankenkassen gelten die Regelungen des SGB V und SGB X.

Es werden bzgl. der wissenschaftlichen Qualität die Richtlinien zur Sicherung der guten wissenschaftlichen Praxis der Deutschen Forschungsgemeinschaft [3] eingehalten. Über die Medizinische Ethikkommission der Universität Oldenburg wird ein koordiniertes Verfahren beantragt, um ein gemeinsames Ethik-Votum für alle relevanten Kommissionen zu erhalten. Die im Projekt

genutzte Infrastruktur des AKTIN Registers wurde bereits von den Ethikkommissionen der Universitäten Magdeburg begutachtet (siehe Anlage 13 – Ethikvotum AKTIN).

Bei schwerwiegenden Störungen des Verarbeitungslaufs, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten werden die Dateneigner sowie die Aufsichtsbehörde unverzüglich von der Treuhandstelle informiert. Im Falle der Verletzung des Schutzes personenbezogener Daten werden außerdem die Voraussetzungen und Bestimmungen des Art. 34 DSGVO geprüft und ggf. die betroffenen Personen entsprechend vom Datenmanager kontaktiert und informiert. Betroffene Personen, die nicht kontaktiert werden können, werden über eine Website informiert.

1.6.1 Rechtgrundlage für die Datenverarbeitung

Eine informierte Einwilligung in einer Notfallsituation, d.h. im Rahmen eines Rettungsdiensteinsatzes mit Beteiligung von Gemeindenotfallsanitäter*innen, ist den Patienten*innen nicht möglich. Eine informierte Einwilligung als Rechtsgrundlage (DSGVO Art. 6 (1) lit. a bzw. DSGVO Art. 9 (2) lit a und gemäß NDSG §33(4)) ist im Vorhaben allerdings unabdingbar, da pseudonyme Daten aus mehreren Quellen gesammelt und verknüpft werden. Insbesondere deshalb findet (wie z.B. im AKTIN NotaufnahmeRegister) DSGVO Art 9 (2) lit. i keine Anwendung. Im Projekt werden daher Daten aufgrund einer zweistufigen Rechtsgrundlage zu verarbeitet. In einer ersten Einwilligung – die von den Gemeindenotfallsanitäter*innen im Auftrag des Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin beim Einsatz eingeholt wird – stimmt der/die Patient*in der Verarbeitung der Kontaktdaten und Einsatznummer zum Zwecke einer Kontaktierung für weitere Forschungsvorhaben zu. Hierbei ist durch den/die Gemeindenotfallsanitär*in sicherzustellen, dass der Patient einwilligungsfähig ist. In einer zweiten Einwilligung, die postalisch an den/die Patienten*in verschickt wird, stimmt der/die Patient*in der Teilnahme am Forschungsprojekt und der pseudonymisierten Erhebung und Verknüpfung der benötigten Daten zu.

*Rechtsgrundlage für die Kontaktierung von Patienten*innen (EWE 1)*

Der/die Patient*in stimmt der Verarbeitung der Kontaktdaten und Einsatznummer zum Zwecke einer Kontaktierung für Forschungsvorhaben zu und entbindet den/die Gemeindenotfallsanitäter*in (zählen zum schweigepflichtigen Personenkreis des § 203 StGB) von der ärztlichen Schweigepflicht (siehe Anlage 7 – Einwilligungserklärung EWE 1). Die Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten zum Zwecke der Kontaktierung für weitere Forschungsvorhaben ist somit die freiwillige schriftliche Einwilligung gemäß DSGVO Art. 6 (1) lit. a. Für die Verarbeitung und Archivierung der Daten gilt Art. 89 DSGVO und § 27 BDSG (neue Fassung, 2018).

Die gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung treffen die Treuhandstelle (Institut für Medizinische Informatik, Uniklinik RWTH Aachen), das Studienzentrum (Klinikum Oldenburg) und Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin. Die Genannten sind im Sinne des Art. 26 der DSGVO gemeinsam verantwortlich. Es wird ein Vertrag zur Vereinbarung zur gemeinsamen Verantwortlichkeit geschlossen, der gemäß Art. 26 Abs. 1 Satz 2 i.V.m. Erwägungsgrund 79 eine Zuteilung der Verantwortlichkeiten beinhaltet. Weitere unter Punkt 1.3. genannte Organisationen haben keinen bestimmenden tatsächlichen Einfluss auf die Datenverarbeitung.

Rechtsgrundlage für die Verknüpfung der Daten (EWE 2)

In der zweiten Einwilligung stimmt der/die Patient*in der Erhebung von Gesundheitsdaten im Forschungsprojekt, der Verknüpfung von Gesundheitsdaten gemäß NDSG §13(2), der Entbindung der Dateneigner von der ärztlichen Schweigepflicht und der Kontaktierung des/der Hausarztes/Hausärztin zu (siehe Anlage 8 – Einwilligungserklärung EWE 2). Die Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten ist die freiwillige schriftliche Einwilligung gemäß DSGVO Art. 6 (1) lit. a. Für die Verarbeitung und Archivierung der Daten gilt Art. 89 DSGVO und § 27 BDSG (neue Fassung, 2018). Im Falle der Daten des Evangelischen Krankenhauses Oldenburg gilt nachrangig DSG-EKD.

Die gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung treffen die Auswertestelle (Abteilung Epidemiologie und Biometrie, Carl von Ossietzky Universität Oldenburg) und die Treuhandstelle (Institut für Medizinische Informatik, Uniklinik RWTH Aachen) sowie das Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin. Daten werden von den datenbereitstellenden Projektpartnern - sog. Dateneignern – erhoben und von der Auswerte- und Treuhandstelle verarbeitet. Die Genannten sind im Sinne des Art. 26 der DSGVO gemeinsam verantwortlich. Es wird ein Vertrag zur Vereinbarung zur gemeinsamen Verantwortlichkeit geschlossen, der gemäß Art. 26 Abs. 1 Satz 2 i.V.m. Erwägungsgrund 79 eine Zuteilung der Verantwortlichkeiten beinhaltet. Weitere unter Punkt 1.3. genannte Organisationen haben keinen bestimmenden tatsächlichen Einfluss auf die Datenverarbeitung.

1.7 Datenlöschung

Die Datenübermittlungen bzw. -erhebungen ist für das Jahr 2021 vorgesehen. Die Pseudonymisierungslisten (für die jeweiligen Zuordnungen zwischen SIC und PSN) werden für den Fall, dass im Rahmen der primären Auswertung noch grundsätzliche Rückfragen gegenüber den Dateneignern entstehen, bis zum Ende der Projektlaufzeit am 31.12.2023 durch die Treuhandstelle vorgehalten und zu diesem Datum gelöscht.

Die Patientenlisten werden bis zum Ende der Projektlaufzeit am 31.12.2023 durch die Treuhandstelle vorgehalten und zu diesem Datum gelöscht. Die anfallenden Dokumente (Einwilligungen, Fragebögen, etc.) werden von den zuständigen Datenlieferanten gemäß den gesetzlichen Bestimmungen aufbewahrt. Es ist den Daten-auswertenden Stellen erlaubt, die (nach dem Ende der Projektlaufzeit) anonymisierten) Daten bis zu 4 Jahre nach Ende der Projektförderung durch den Innovationsfonds auszuwerten.

Die anonymisierten Gesundheitsdaten, die der Universität Oldenburg vorliegen, werden gemäß den Vorschriften der „Guten Praxis Sekundärdatenanalyse“ (GPS, [2]) mindestens 10 Jahre nach der Auswertung in einer Form aufbewahrt, die eine Reproduzierbarkeit der Ergebnisse gewährleistet. Es ergibt sich somit eine endgültige Löschfrist zum 31.12.2033. Die Aufbewahrung und fristgerechte Löschung der Daten obliegt der Verantwortung der Universität Oldenburg.

2 Technische und organisatorische Maßnahmen

Für die verarbeiteten Daten gilt ein sehr hoher Schutzbedarf. Sämtliche Datenverarbeitung fußt deshalb auf einem Rollen- und Rechtekonzept. Sämtliche Daten werden pseudonymisiert unter der Datenhoheit der erhebenden Einrichtung gesammelt - gemäß Art. 32 Abs. 1a DSGVO unterstützt die Verwendung von Pseudonymen dabei, ein angemessenes Schutzniveau der Datenverarbeitung zu gewährleisten. Die Daten werden zweifach pseudonymisiert, mithilfe eines Treuhänders gesammelt und verbleiben in einer Forschungsdatenbank in der Auswertestelle; dies entspricht den Vorgaben des Leitfadens zum Datenschutz in medizinischen Forschungsprojekten – generische Lösungen der TMF 2.0 [1]. Die Daten werden bei der Auswertestelle so geführt, dass die Re-Identifizierung nur durch die Zusammenarbeit von Dateneigner bzw. Auswertestelle und Treuhandstelle erfolgen könnte. Insbesondere kann durch die Löschung der Zuordnungstabelle beim Pseudonymisierungsdienst eine spätere Re-Identifizierung wirksam ausgeschlossen werden. Für Datenanfragen zu Forschungszwecken können die gesammelten Daten verfügbar gemacht werden. Es gelten dafür die Anweisungen des DUAC, welches datenschutzrechtliche und ethische Standards garantiert.

Die technisch-organisatorischen Maßnahmen bei den datenbereitstellenden Projektpartnern (bspw. Kliniken und Rettungsdienste) selbst sind nicht Bestandteil der Datenschutzvereinbarung, da der Schutzbedarf dort unabhängig vom Projekt besteht und bereits entsprechend umgesetzt ist (siehe Anlage 1 - Studienzentren). Insbesondere handelt es sich dabei um Datenverarbeitungen mit anderen Zwecken und Rechtsgrundlagen außerhalb der Regelungskompetenz des ILEG-Projekts (bspw. allgemeine Dokumentations- und Aufbewahrungspflichten).

2.1 Rollen und Rechte

Für alle Daten, die im Rahmen des AKTIN-Notaufnahmeregisters erhoben werden, gelten Maßnahmen entsprechend eines sehr hohen Schutzbedarfs. Die Daten werden deshalb lokal gespeichert und nur nach einem standardisierten Freigabeprozess durch das DUAC an Dritte übermittelt. Es gilt ein striktes Rollenkonzept. Mit Hilfe der technischen und organisatorischen Maßnahmen werden insbesondere die durch Art. 32 DSGVO (Sicherheit der Verarbeitung) vorgegebenen Grundsätze eingehalten.

2.1.1 Dateneigner

Die Dateneigner (Kliniken, Rettungsdienste und Leitstellen) verantworten das lokale Datenmanagement und die Bereitstellung der Daten für die Verarbeitung im Forschungsprojekt. Sie sind dementsprechend für die Umsetzung und Einhaltung aller ethischen, rechtlichen, vertraglichen und organisatorischen Vorgaben der eigenen Institution zum Datenmanagement verantwortlich. Sie verantworten eine lokale Prüfung der Bereitstellung der benötigten Daten Abfrage (bspw. durch die lokalen Datenschutzbeauftragten), sowie die Festsetzung und Prüfung der Einhaltung der geltenden Kriterien der Anonymität durch die eigene Institution.

2.1.2 Treuhandstelle

Die informationelle Trennung gemäß dem Leitfaden zum Datenschutz der TMF wird durch die Einrichtung einer Treuhandstelle am Institut für Medizininformatik des Uniklinikum RWTH Aachen erreicht. Diese setzt lediglich eine Trennung von MDAT und IDAT um, und ist unabhängig von Datengewinnung in diesem und anderen Projekten der Uniklinik RWTH Aachen. Die Treuhandstelle hat keine Einsicht in die medizinischen Daten MDAT, sondern ist für das Führen einer Patientenliste (IDAT zu MPI) und Zuordnungslisten erster Stufe (IDAT zu den verschiedenen Pseudonymen erster Stufe) und die zweistufige Pseudonymisierung (Pseudonymen erster Stufe zu Pseudonym zweiter Stufe) zuständig. Dafür wird von der Treuhandstelle die Software E-PIX und die Software gPAS bereitgestellt. Die Treuhandstelle fordert außerdem Daten bei Dateneignern an, wenn Patienten*innen nicht mithilfe eines ID Managements identifiziert werden können (z.B. in den AKTIN Notaufnahmeregister Datensätzen). Dafür wird von der Treuhandstelle eine datenschutzkonforme Patientmatching-Software entwickelt. Für die Verarbeitung und die Verwaltung der Zuordnungslisten erster Stufe, die Verwaltung der Zuordnungslisten zweiter Stufe von SIC und PSN und die Einrichtung und den Betrieb der technischen Infrastruktur für Pseudonymisierungsdienst, Patientenliste und Patientmatching werden ausgewählte Mitarbeiter*innen des Institut für Medizininformatik des Uniklinikum RWTH Aachen benannt. Diese Mitarbeiter*innen werden in einer Liste geführt, die kontinuierlich aktualisiert wird. Abgesehen vom Patientmatching und den Prozessen zur Erfüllung der Betroffenenrechte erteilt die Treuhandstelle den anderen Projektteilnehmern keine Auskünfte über gespeicherte Datensätze einzelner Patienten*innen. Es können ggf. aggregierte und anonyme Daten wie z.B. Rekrutierungszahlen zur Verfügung gestellt werden.

2.1.3 Auswertestelle

Die Aufgabe der Mitarbeiter*innen der Auswertestelle ist die Prüfung, Aufbereitung, Aggregation und Auswertung der gesammelten Anfrageergebnisse. Die Verarbeitung des Gesamtdatensatzes ist nur der Auswertestelle gestattet. Beim Konsortialführer wird eine Liste derjenigen Personen geführt, die zum Umgang mit den Daten berechtigt sind sowie eines internen Ansprechpartners in datenschutzrechtlichen Angelegenheiten (Anlage 2 – Ansprechpartner Datenschutz). Alle Personen, die Datenzugang erhalten, unterschreiben eine Schweigepflichterklärung. Sie unterliegen auch nach dem Ende des Projekts der Geheimhaltungspflicht. Die Auswertestelle stellt gemäß der Vorgaben des DUAC (Punkt 2.1.5) sicher, dass im Falle einer Weitergabe von Daten an Forscher*innen im Rahmen von Forschungsanfragen die Kriterien der k-Anonymisierung und l-Diversität eingehalten werden. Die Daten werden von der Auswertestelle für jede Forschungsanfrage erneut zufällig verschlüsselt.

2.1.4 Dateninterpreten

Forscher*innen aus dem Projektkonsortium können über die ILEG Geschäftsstelle Forschungsanfragen anmelden und so Datenauszüge beantragen. Alle Anfragen werden protokolliert.

2.1.5 Data Use and Access Committee (DUAC)

Die Bereitstellung eines Datensatzes kann beim *Data-Use-and-Access-Komitee* des ILEG-Projektes von Konsortialpartnern für die Beantwortung ihrer Fragestellungen mittels eines Antrages beantragt werden. Dem DUAC gehört mindestens ein Mitarbeiter der Auswertestelle an. Das DUAC prüft den Antrag im Hinblick auf seinen Bezug zum Projektantrag, auf Wissenschaftlichkeit sowie auf datenschutzrechtliche Konformität der Bereitstellung und sendet - bei positiver Bewertung - die Informationen über den jeweiligen Datenauszug an die Auswertestelle, die die Daten dann dem jeweiligen Projektteilnehmer zur externen Berechnung bereitstellt. Die Auswahl der Fälle, Variablen und Ausprägungen erfolgt anhand der konkreten Fragestellung und unter Berücksichtigung des Antragstellers bzw. dessen bisheriger Anträge, so dass den auswertenden Stellen jeweils nur ein reduzierter bzw. aggregierter Datensatz bereitgestellt wird[3].

Vollständige Rohdatensätze werden nicht an Dateninterpreten versandt. Sollten solche Datensätze benötigt werden (bspw. für explorative Datenanalysen), so stehen diese nur über eine Remote-Desktop-Verbindung zur Verfügung. Das entsprechende physikalische System gehört zur Auswertestelle. Benötigte Ergebnisse werden vor Herausgabe an die jeweiligen Projektpartner erneut in Bezug auf datenschutzrechtliche Aspekte (K-Annonymität, I-Diversität) begutachtet. Es können von den Dateninterpreten keine Datensätze aus dem System exportiert werden.

2.1.6 Rollenkonflikte

Alle genannten Rollen schließen sich gegenseitig aus, d. h. eine Vereinigung mehrerer Rollen in einer Institution bzw. Person ist nicht zulässig.

2.2 IT Infrastruktur

Die Forschungsinfrastruktur des ILEG-Projektes besteht aus einer dezentralen Datenerhebung bei den Dateneignern unter deren Verantwortung und über eine zentrale IT-Komponente, die für das Record Linkage (zusammenführen der Daten über das Führen einer Patientenliste) und einem Pseudonymisierungsdienst besteht.

2.2.1 Hardware

Für den Betrieb der Patientenliste zum Zwecke des Recordlinkage (E-PIX), der Pseudonymisierung (gPAS) und der Identifizierung von Patienten*innen beim Dateneigner (Patientmatching-Software) wird von der Treuhandstelle ein virtueller Server im Rechenzentrum des Uniklinikum RWTH Aachen eingesetzt. Datensätze der Auswertestelle stehen gemäß den Anweisungen des DUAC über eine Remote-Desktop-Verbindung zur Verfügung (siehe Punkt 2.1.5). Zu diesem Zwecke wird von der Auswertestelle ein virtueller Server im Rechenzentrum der Universität Oldenburg eingesetzt.

2.2.2 Software

Es wird in verschiedenen Stufen des Projekts Software eingesetzt. Software, die bei den Dateneignern eingesetzt wird, unterliegt den jeweils dortig gültigen Vorgaben.

Patientmatching Software

Die Treuhandstelle fordert Daten bei Dateneignern an, wenn Patienten*innen nicht mithilfe eines ID Managements identifiziert werden können (z.B. in den AKTIN Notaufnahmeregister Datensätzen). Um die Daten von Patienten*innen, die eingewilligt haben an der Studie teilzunehmen, zu filtern, wird von der Treuhandstelle eine Patientmatching Software entwickelt. Die Software soll es ermöglichen

[3] Insbesondere die (verkürzte oder vollständige) Postleitzahl wird nur übermittelt, wenn sichergestellt ist, dass die Postleitzahl in Verbindung mit den anderen angeforderten Variablen keine Re-Identifizierung zulässt.

anhand von IDAT (Name, Nachname, Geburtstdatum) Patienten*innen beim Dateneigner zu identifizieren, ohne andere Patienten*innen zu offenbaren. Um dies umzusetzen, sollen Hashwerte aus den IDAT berechnet werden, die verglichen werden können. Als Ausgabe werden sowohl für Treuhandstelle als auch Dateneigner von der Software Patientenlisten mit einem Subject Identification Code generiert, die eine Verknüpfung der Daten erlaubt (einen schematischen Ablauf findet sich in Abbildung 2). Das genaue Verfahren wird während der Entwicklung im Laufe des Projektes gemäß diesen Anforderungen ausgearbeitet.

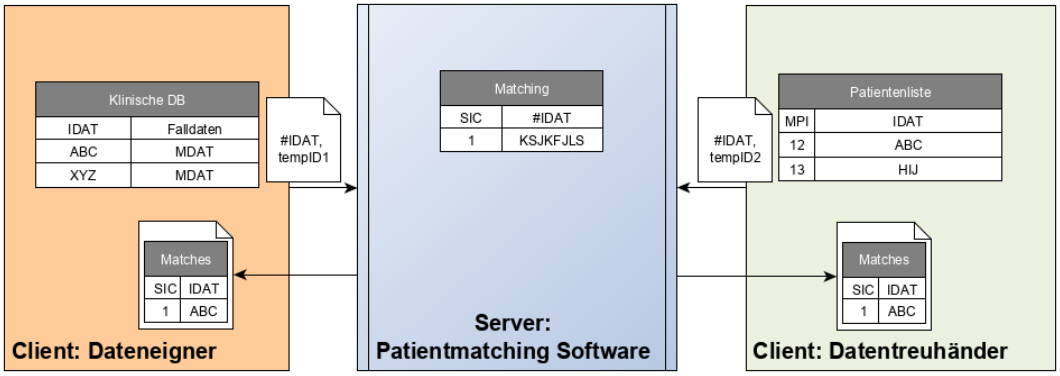

Abbildung 2: Schematischer Aufbau der Patientmatching Software

Recordlinkage mit E-PIX

Für das Recordlinkage wird von der Treuhandstelle eine Instanz der E-PIX Software eingesetzt. Um Forschungsdaten aus mehreren Projekten und Studien zusammenführen, ist sowohl ein Dublettenverfahren als auch eine eineindeutige systemweite Kennung erforderlich, der sowohl die personenidentifizierenden Daten, als auch die einzelnen lokalen Kennungen des Quellsystems (z.B. Rettungsdienst, Notaufnahme, etc.) zugeordnet sind. Da dies auch bei unvollständigen oder fehlerhaften Personendaten fehlertolerant und nachvollziehbar erfolgen muss, ist ein nachhaltiges Record Linkage und Identitäten-Management erforderlich. Der E-PIX ermöglicht ein probabilistisches Record Linkage und setzt das Konzept eines Master Patient Index um. Das integrierte Identitätenkonzept erlaubt potentielle Synonymfehler automatisch zu erkennen und unterstützt bei deren grafischer Auflösung. Die Erkennung von Dubletten erfolgt auf Basis frei definierbarer Parameter und der Levensthein-Distanz. Mögliche Synonymfehler werden so protokolliert und können im Nachhinein über entsprechende Funktionen aufgelöst werden [5].

Für die erste Pseudonymisierungsstufe bei den jeweiligen Dateneignern, werden zufällige IDs auf alle Dokumente bzw. Protokolle gedruckt. Die IDs können dann in E-PIX dokumentiert werden. Für die erste Pseudonymisierungsstufe der Daten, die über das AKTIN Notaufnahmeregister gesammelt werden, wird der in der *AKTIN Consentmanager* eingesetzt. Dieser erzeugt eine klinikinterne laufende Nummer als *Subject Identification Code* (SIC) und speichert diese in einer Tabelle im lokalen Data Warehouse zusammen mit einer Identifikationsnummer (ggf. Patientennummer, Fallnummer, Notaufnahme-Besuchs-ID), um damit Einwilligungen zu dokumentieren.

Pseudonymisierung mit g-PAS

Für die zweite Stufe der Pseudonymisierung der gesammelten Daten wird von der Treuhandstelle eine Instanz der g-PAS Software eingesetzt. G-PAS dient der Generierung und Verwaltung von Pseudonymen. Das Domänenkonzept sowie die freie Definition von Alphabeten als auch Generatoralgorithmen erlauben unterschiedliche Pseudonyme je Datenquelle, Anwendungskontext (Erhebung, Herausgabe) oder Standort zu generieren. Durch die spezielle Ausgestaltung des Pseudonymisierungsprozesses werden die Bedingungen der Definition aus Art. 4 Nr. 5 der DSGVO erfüllt und insbesondere die folgenden Schutzziele erreicht:

- Keine Offenbarung identifizierender Daten

- Keine Offenbarung personenbezogener Daten zwischen den Dateneignern
- Keine Offenbarung personenbezogener Daten gegenüber dem Pseudonymisierungsdienst
- Eine Rückrechnung der Auswerte-Pseudonyme ist ausgeschlossen, dadurch sichere Umsetzung der Anonymisierung durch Löschen der Zuordnungsliste beim Pseudonymisierungsdienst

Datenübermittlung und sicherer Datenspeicher

Für die Übertragung der MDAT von den Dateneignern an die Auswertestelle wird ein nach dem Stand der Technik sicherer Datenspeicher eingerichtet (cryptshare o.ä.). Der Treuhänder pseudonymisiert die Datensätze und leitet die MDAT ohne inhaltliche Kenntnisnahme an die Auswertestelle weiter. Die medizinischen Daten, die nicht für die Pseudonymisierung benötigt werden, werden hybrid verschlüsselt (AES und RSA). Die verschlüsselten Daten können von der Auswertestelle mit einem nur ihr zugänglichen RSA Schlüssel und einem AES Schlüssel entschlüsselt werden.

Verschlüsselung

Für die Verschlüsslung der MDAT durch die Dateneigner an die Auswertestelle wird ein nach dem Stand der Technik sichere Software zur Verfügung gestellt. Die Software verschlüsselt alle Inhalte eines tabellarischen Datensatzes mit Ausnahme der identifizierenden Daten. Ziel ist es MDAT und IDAT zu trennen. Die medizinischen Daten, die nicht für das Record Linkage benötigt werden (d.h. sämtliche Daten außer den IDAT), werden hybrid verschlüsselt (AES und RSA), so dass sie von der Treuhandstelle nicht gelesen, sondern nur an die Auswertestelle, versehen mit einem neuen Pseudonym PSN (anstelle des SIC), durchgeleitet werden. Die verschlüsselten Daten können von der Auswertestelle mit einem nur ihr zugänglichen RSA Schlüssel und einem AES Schlüssel entschlüsselt werden.

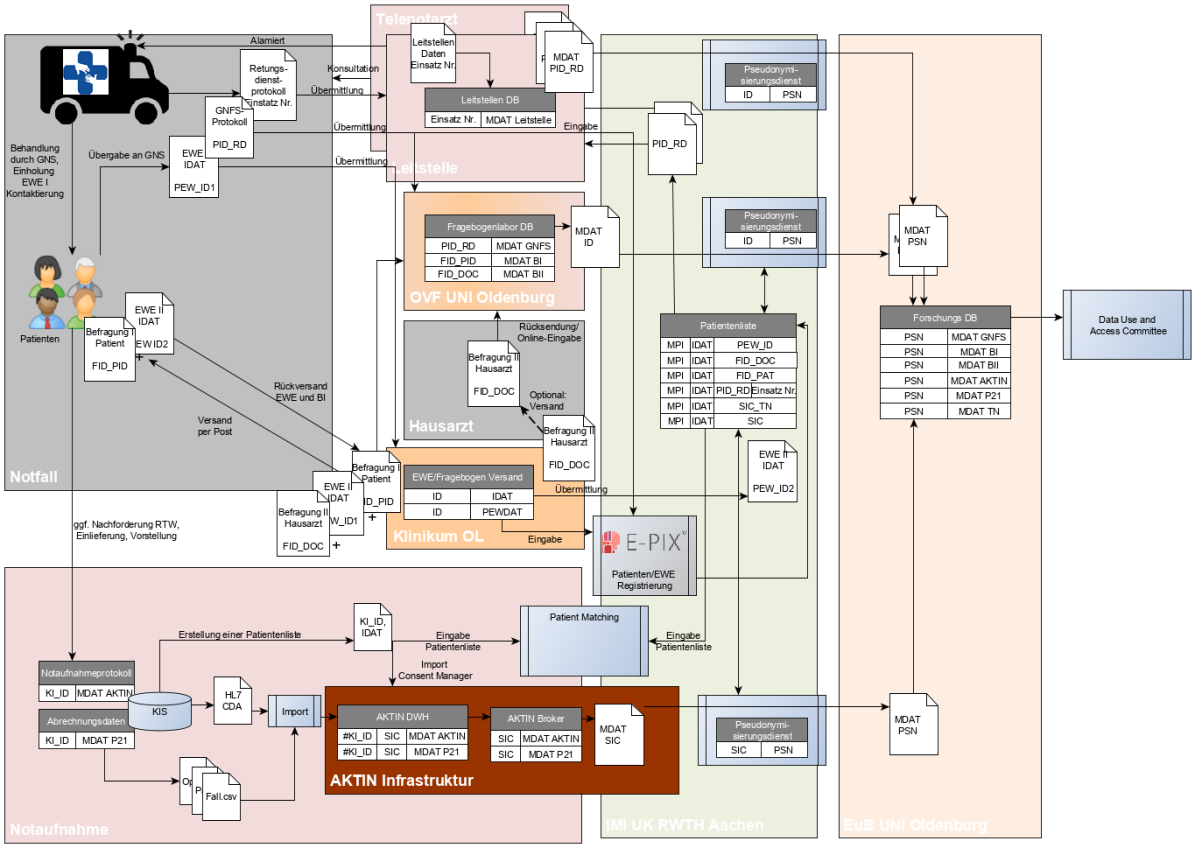

Abbildung 3: Datenfluss im ILEG Projekt

2.3 Datenflüsse

Im Forschungsvorhaben ist ein Multi-Modulares Vorgehen geplant. Es werden Daten aus verschiedenen Datenquellen verknüpft und pseudonym verarbeitet, um eine ganzheitliche Datengrundlage für Auswertungen zu schaffen. Der Datenfluss im Projekt setzt eine Trennung von MDAT und IDAT als Garantie für eine rechtmäßige Verarbeitung der Daten im Sinne von Art. 6 DSGVO (4) lit. e voraus.

Die Pseudonymisierung und Weiterleitung der medizinischen Daten ohne Kenntnisnahme der Inhalte von den Dateneignern zur Auswertestelle wird von der Treuhandstelle vorgenommen. Die Treuhandstelle stellt zusätzlich sicher, dass Daten nur übermittelt werden, wenn eine Einwilligung für die Datenverarbeitung im Rahmen des ILEG Projekts vorliegt (EWE2). Auf diese Weise ist sichergestellt, dass medizinische Daten und Fragebögen nur von Patienten*innen verknüpft werden, bei denen zum Zeitpunkt der Weiterleitung der medizinischen Daten eine gültige Einwilligung vorliegt.

2.3.1 Erhebung der Einwilligungserklärungen

Im Projekt werden zwei Einwilligungen im Auftrag des Studienzentrums bzw. des Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin eingeholt.

Einholung EWE 1

Im Projekt wird eine erste Einwilligung (EWE1) von dem/der Gemeindenotfallsanitäter*in im Auftrag des Studienzentrums bzw. des Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin beim Einsatz eingeholt. In dieser stimmt der/die Patient*in die Verarbeitung der Kontaktdaten und Einsatznummer zum Zwecke einer Kontaktierung durch das Studienzentrum bzw. dem Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin für Forschungsvorhaben zu. Auf der Einwilligung ist eine eindeutige ID die dem jeweiligen Rettungsdienst durch ein Prefix zugewiesen werden kann (EWE_ID1) aufgedruckt. Die ID wird zusammen mit der Einsatznummer, EWE_ID1, Namen, Vornamen und Geburtsdatum des/der Patienten*in von dem/der Gemeindenotfallsanitäter*in in E-PIX eingegeben. Der/die Gemeindenotfallsanitäter*in hat keinen Einblick in die Patientenliste, sondern kann lediglich die Daten eines Patienten*in eingeben. Die originale Einwilligung wird anschließend an das Studienzentrum (verschlüsselt digital oder postalisch) übermittelt und geprüft. Das Studienzentrum verwahrt die Einwilligung und nutzt die Kontaktdaten für ein Kotaktmanagement in E-PIX im Rahmen einer Re-Kontaktierung zum Zwecke der Einholung von weiteren Einwilligungen im Rahmen von Forschungsprojekten (EWE2). Die Treuhandstelle hat keinen Einblick in die Daten der Einwilligungserklärung (abgesehen von den Eingaben in E-PIX).

Sollten Patienten*innen mehr Bedenkzeit benötigen, so kann die Einwilligung EWE1 auch Postalisch von Patienten*innen an die Studienzentrale verschickt werden. In diesem Fall werden die Rettungsdienste von der Studienzentrale kontaktiert und über die Einwilligung mit Name, Vorname und Geburtsdatum informiert. Die Einsatznummer, EWE_ID1, Namen, Vornamen und Geburtsdatum des/der Patienten*in werden dann von der Rettungsdienst in E-PIX eingegeben. Das Studienzentrum verwahrt die Einwilligung.

Einholung EWE 2

Im Projekt wird eine zweite informierte Einwilligung (EWE2) vom Studienzentrum bzw. dem Oldenburger Forschungsnetzwerk Notfall- und Intensivmedizin postalisch eingeholt. In dieser Einwilligung stimmen die Patienten*innen der Erhebung ihrer Gesundheitsdaten im Rahmen des ILEG Projekts zu. Zusätzlich zur Einwilligungserklärung wird an die Patienten*innen eine schriftliche Aufklärung verschickt. Die Einwilligung wird per Rückumschlag an das Studienzentrum zurückgeschickt. Auf der Einwilligung ist eine eindeutige ID (EWE_ID2) aufgedruckt. Diese wird *nach* dem Eingang und Prüfung der Ausgefüllten Einwilligung in E-PIX zusammen mit Namen, Vornamen und Geburtsdatum des/der Patienten*in eingegeben. Mitarbeiter des Studienzentrums haben keinen Einblick in die Patientenliste, sondern können lediglich die Daten eines Patienten*in eingeben. Im Anschluss wird die Einwilligungserklärung (EWE2) vom Studienzentrum an die Treuhandstelle

geschickt (gesammelt für jeden Kalendermonat). Die Treuhandstelle verwahrt die Einwilligungen. Das Studienzentrum hat keinen Einblick in Daten der Einwilligungserklärung (EWE2) nach abgeschlossener Übermittlung.

2.3.2 Erhebung der Patientenbefragung

Das Studienzentrum verschickt die Patientenbefragung und einen Rücksendeumschlag an den/die Patienten*in zusammen mit der zweiten Einwilligungserklärung (EWE2). Auf dem Fragebogen ist eine eindeutige ID (FID_PID) aufgedruckt. Diese wird *nach* dem Eingang des ausgefüllten Fragebogens und bei vorliegender Einwilligung (EWE2) in E-PIX zusammen mit Namen, Vornamen und Geburtsdatum des/der Patienten*in eingegeben. Mitarbeiter des Studienzentrums haben keinen Einblick in die Patientenliste, sondern können lediglich die Daten eingeben. Im Anschluss wird der Fragebogen vom Studienzentrum an das Fragebogenlabor mit dem Auftrag zur digitalen Erfassung geschickt (gesammelt für jeden Kalendermonat). Für die Pseudonymisierung, Verknüpfung und Auswertung durch die Auswertestelle werden die digitalisierten Daten mit FID_PID verschlüsselt, mittels des Pseudonymisierungsdienstes (gPAS) pseudonymisiert (FID_PID wird zu PSN getauscht) und über den sicheren Datenspeicher an die Auswertestelle weitergeleitet. Die Daten liegen in der Auswertestelle unter dem Pseudonym PSN vor. Sind zu einer Person mehrere Datenarten verfügbar, können diese anhand des Pseudonyms miteinander verknüpft werden.

2.3.3 Erhebung der Hausarztbefragung

Das Studienzentrum verschickt bei vorliegender Einwilligung (EWE2) die Hausarztbefragung und einen Rücksendeumschlag an den/die Hausarzt/Hausärztin zusammen mit einer Kopie der zweiten Einwilligungserklärung (EWE2). Auf dem Fragebogen ist eine eindeutige ID (FID_DOC) aufgedruckt. Diese wird *nach* dem Eingang des ausgefüllten Fragebogens in E-PIX zusammen mit Namen, Vornamen und Geburtsdatum des/der Patienten*in eingegeben. Mitarbeiter des Studienzentrums haben keinen Einblick in die Patientenliste, sondern können lediglich die Daten eingeben. Im Anschluss wird der Fragebogen vom Studienzentrum an das Fragebogenlabor mit dem Auftrag zur digitalen Erfassung geschickt (gesammelt für jeden Kalendermonat). Für die Pseudonymisierung, Verknüpfung und Auswertung durch die Auswertestelle werden die digitalisierten Daten mit FID_PID werden lokal verschlüsselt, mittels des Pseudonymisierungsdienstes (gPAS) pseudonymisiert (FID_DOC wird zu PSN getauscht) und über den sicheren Datenspeicher an die Auswertestelle weitergeleitet. Die Daten liegen in der Auswertestelle unter dem Pseudonym PSN vor. Sind zu einer Person mehrere Datenarten verfügbar, können diese anhand des Pseudonyms miteinander verknüpft werden.

2.3.4 Erhebung der Einsatzdaten des Rettungsdienstes

Die Einsatzdaten des Rettungsdienstes werden in Form von Gemeindenotfallsanitäter- und Rettungsdienstprotokollen gesammelt.

Gemeindenotfallsanitäterprotokoll

Das Gemeindenotfallsanitäterprotokoll wird von den Gemeindenotfallsanitäter*innen im Anschluss an den Einsatz ausgefüllt. Auf dem Gemeindenotfallsanitäterprotokoll ist eine eindeutige ID (PID_RD) aufgedruckt, die dem jeweiligen Rettungsdienst durch ein Prefix zugewiesen werden kann. Die ID wird – vorausgesetzt einer erfolgten Einwilligung (EWE1) zusammen mit der Einsatznummer, Namen, Vornamen und Geburtsdatum des/der Patienten*in vom Gemeindenotfallsanitäter*in in E-PIX eingegeben. Im Anschluss wird das Gemeindenotfallsanitäter-protokoll vom Rettungsdienst an das Fragebogenlabor geschickt. Das Fragebogenlabor erfasst im Auftrag des Oldenburger Forschungsnetzwerks Notfall- und Intensivmedizin die Protokolle digital. Für die Pseudonymisierung, Verknüpfung und Auswertung durch die Auswertestelle werden die digitalisierten Daten mit FID_PID werden lokal verschlüsselt, mittels des Pseudonymisierungsdienstes (gPAS) pseudonymisiert (FID_DOC wird zu PSN getauscht) und über den sicheren Datenspeicher an die Auswertestelle weitergeleitet. Die Treuhandstelle stellt sicher, dass Daten nur übermittelt werden, wenn eine Einwilligung für die Datenverarbeitung im Rahmen des ILEG Projekts vorliegt (EWE2). Dafür werden die Fälle die im sicheren Datenspeicher liegen, vor Weiterleitung von der Treuhandstelle geprüft. Fälle für die keine

Einwilligung vorliegt, werden ohne Kenntnisnahme der medizinischen Daten gelöscht. Die Daten liegen anschließend in der Auswertestelle unter dem Pseudonym PSN vor. Sind zu einer Person mehrere Datenarten verfügbar, können diese anhand des Pseudonyms miteinander verknüpft werden.

Rettungsdienstprotokoll

Die Rettungsdienste sind in der Lage, Patienten*innen anhand von Einsatznummern in den relationalen Datenbanken, in denen die Daten vorliegen, zu identifizieren. Um Daten eingewilligte Patienten*innen liefern zu können, wird die in EPIX registrierte Einsatznummer mit Pseudonym 1. Stufe (PID_RD) von der Treuhandstelle an die Rettungsdienste übermittelt. So ist sichergestellt, dass nur Daten von eingewilligten Patienten*innen gesendet werden. Die Rettungsdienste erstellen dann einen Datenauszug von allen Einsätzen, in denen die eingewilligten Patienten*innen behandelt wurden. Die Datenauszüge werden lokal verschlüsselt, im sicheren Datenspeicher gespeichert, mittels des Pseudonymisierungsdienst (gPAS) pseudonymisiert (PID_RD wird zu PSN getauscht) und über den sicheren Datenspeicher an die Auswertestelle weitergeleitet. Die Daten liegen anschließend in der Auswertestelle unter dem Pseudonym PSN vor. Sind zu einer Person mehrere Datenarten verfügbar, können diese anhand des Pseudonyms miteinander verknüpft werden.

2.3.5 Erhebung der Leitstellendaten

Leitstellendaten werden für jeden Einsatz des Rettungsdienstes erhoben (identifiziert durch Einsatznummer). Eine digitale Aufzeichnung wird von der Leitstelle verwahrt. Im ILEG Projekt wird angestrebt, alle Leitstellendaten von Einsätzen 2021, in denen die eingewilligten Patienten*innen behandelt wurden, zu verarbeiten. Nach Ablauf des Jahres 2021 werden gesammelt von der Treuhandstelle von den Leitstellen diese Daten angefordert. Die Leitstellen sind in der Lage, Patienten*innen anhand von Einsatznummern (und sämtliche weitere Einsätze) in den relationalen Datenbanken in denen die Daten vorliegen zu identifizieren. Die Datenauszüge werden lokal verschlüsselt, im sicheren Datenspeicher gespeichert, mittels des Pseudonymisierungsdienst (gPAS) pseudonymisiert (Einsatznummer wird zu PSN getauscht) und über den sicheren Datenspeicher an die Auswertestelle weitergeleitet. Die Daten liegen anschließend in der Auswertestelle unter dem Pseudonym PSN vor. Sind zu einer Person mehrere Datenarten verfügbar, können diese anhand des Pseudonyms miteinander verknüpft werden.

2.3.6 Erhebung der Telemedizinzentrale

Ein Telenotarzteinsatzprotokoll wird für jeden Telenotarzteinsatz erhoben. Eine digitale Aufzeichnung wird von der Telemedizinzentrale verwahrt. Im ILEG Projekt wird angestrebt, alle Telenotarzteinsatzprotokolle von Einsätzen 2021, in denen die eingewilligten Patienten*innen behandelt wurden, zu verarbeiten. Nach Ablauf des Jahres 2021 werden diese Daten gesammelt von der Treuhandstelle angefordert. Um eingewilligte Patienten*innen zu identifizieren, wird von den Kliniken und der Treuhandstelle die Patientmatching Software eingesetzt. Die Datenauszüge werden lokal verschlüsselt, im sicheren Datenspeicher gespeichert, mittels des Pseudonymisierungsdienst (gPAS) pseudonymisiert (Einsatznummer wird zu PSN getauscht) und über den sicheren Datenspeicher an die Auswertestelle weitergeleitet. Die Daten liegen anschließend in der Auswertestelle unter dem Pseudonym PSN vor. Sind zu einer Person mehrere Datenarten verfügbar, können diese anhand des Pseudonyms miteinander verknüpft werden.

2.3.7 Erhebung der Klinischen Daten

Klinische Daten werden während des Behandlungsprozesses in Notaufnahmen erhoben, die als Modellkliniken im AKTIN-Projekt zum Aufbau eines elektronischen Notaufnahmeregisters einen einheitlichen Dokumentationsstandard in den Notaufnahmen etabliert haben. Grundlage für die elektronische Dokumentation ist der Datensatz Notaufnahme der DIVI. Zusätzlich können Abrechnungsdaten über die Infrastruktur erhoben werden.

Im ILEG Projekt wird angestrebt, alle Behandlungen von eingewilligten Patienten*innen im Jahre 2021 zu verarbeiten. Die Daten werden in regelmäßigen Intervallen von der Treuhandstelle angefordert. Um

eingewilligte Patienten*innen zu identifizieren, wird von den Kliniken und der Treuhandstelle die Patientmatching Software eingesetzt. Dabei wird für jede/n Patienten*in ein Pseudonym 1. Stufe (SIC_AKTIN) generiert. Die Patienten*innen können dann im Consent Manager mit Patientennummer und SIC_AKTIN registriert werden. Über den SIC_AKTIN können die Patientendaten anschließend zusammengeführt werden. Für Datenauszüge wird die Infrastruktur des AKTIN Notaufnahme Register gemäß den Vorgaben des Datenschutzkonzeptes des AKTIN Notaufnahme Register genutzt (siehe Anlage 4 – Datenschutzkonzept AKTIN). Die Datenauszüge werden lokal verschlüsselt, im sicheren Datenspeicher gespeichert, mittels des Pseudonymisierungsdienstes (gPAS) pseudonymisiert (SIC_AKTIN wird zu PSN getauscht) und über den sicheren Datenspeicher an die Auswertestelle weitergeleitet. Die Daten liegen anschließend in der Auswertestelle unter dem Pseudonym PSN vor. Sind zu einer Person mehrere Datenarten verfügbar, können diese anhand des Pseudonyms miteinander verknüpft werden.

2.3.8 Sammlung der Daten in einer Forschungs DB

Der Gesamtdatensatz wird von der Treuhandstelle allein an die Auswertestelle übermittelt. Die Auswertestelle prüft sämtliche Daten, die von der Treuhandstelle übermittelt wurden, nach Eingang auf Lesbarkeit, Übereinstimmung mit der konsentierten Datensatzbeschreibung, Vollständigkeit und Plausibilität, soweit diese Prüfalgorithmen a-priori festgelegt werden können. Die Auswertestelle speichert alle Daten in einer Forschungs-Datenbank; dafür wird ein virtueller Server im Rechenzentrum der Universität Oldenburg eingesetzt.

2.4 Verschlüsselung

Die Übertragung der Daten zwischen den Beteiligten geschieht grundsätzlich mit Transport-Verschlüsselung (TLS 1.2 mit SHA2). Es werden niemals Pseudonyme, (temporäre) IDs oder personenbezogene Daten über eine unverschlüsselte Internetverbindung oder ein anderes Medium übertragen. Die zu entwickelnde Patientmatching-Software baut eine zertifikatsbasierte verschlüsselte HTTPS-Verbindung (mindestens TLS 1.2) zum Pseudonymisierungsserver der Universität Oldenburg auf. Der gesamte Datenverkehr im Projekt ist verschlüsselt und eine Kenntnisnahme durch Dritte nach dem Stand der Technik ausgeschlossen.

Zusätzlich zur Transportverschlüsselung werden die Daten durch ein asymmetrisches Verfahren derart verschlüsselt (AES und RSA), dass sie nur von der Auswertestelle entschlüsselt werden können. Der private Schlüssel (RSA) für die Entschlüsselung der Daten darf nur der Auswertestelle bekannt sein und der öffentliche Schlüssel wird für den Versand der Daten in die Software konfiguriert.

2.5 Gewährleistung der Vertraulichkeit

Die Vertraulichkeit der Pseudonymisierungsliste wird technisch gewährleistet, indem der Webserver und die Datenbank im entsprechend gesicherten und zertifizierten Rechenzentrum der Universität Oldenburg betrieben werden. Dort gibt es insbesondere Schließ- und Alarmanlagen nach gängigen Standards, restriktiv konfigurierte Firewalls und Überwachungssoftware. Zugang zu den Zuordnungslisten haben nur entsprechend geschulte und der Geheimhaltung verpflichtete Administratoren.

2.6 Gewährleistung der Integrität

Bei der Übertragung aller Daten wird anhand von Checksummen geprüft, ob die Daten korrekt übermittelt wurden. Dazu wird über die gesamte Datenmenge (Nutzdaten und IDs) ein Message Digest-Verfahren angewendet, das jede Form von Übertragungsfehlern (Anzahl der Zeilen, fehlerhafte Übertragung der Inhalte etc.) detektiert. Bei Fehlern werden die empfangenen Daten gelöscht und der Versand wird erneut durchgeführt.

Die Auswertestelle prüft die Daten nach Eingang auf Lesbarkeit, Übereinstimmung mit der konsentierten Datensatzbeschreibung, Vollständigkeit und Plausibilität, soweit diese Prüfalgorithmen a-priori festgelegt werden können. Binnen zwei Wochen erfolgt eine Rückmeldung der Auswertestelle

an die Treuhandstelle über das Ergebnis dieser Eingangsprüfung. Sind die Daten in einem Umfang fehlerhaft, dass eine Nutzung für die Zwecke der Evaluation nicht möglich ist, wird eine Neulieferung der fehlerhaften Daten durch die Treuhandstelle veranlasst. Diese wird innerhalb von weiteren drei Wochen nach Mitteilung über das Prüfergebnis durchgeführt, sofern der Fehler allein auf Prozessen der Datenselektion und -aufbereitung für Zwecke der Datenbereitstellung beruht. Es müssen nur die fehlerbereinigten Daten erneut gesandt werden. Es erfolgt eine Bestätigung über die Entgegennahme der Datenlieferung.

2.7 Gewährleistung der Verfügbarkeit

Am Standort des Uniklinikums RWTH Aachen ist die Verfügbarkeit der Pseudonymisierungsliste und Patientenliste und an der Universität Oldenburg die Verfügbarkeit der Daten durch den Betrieb im jeweiligen Rechenzentrum gesichert. Es gibt bzgl. der Not-Stromversorgung, redundanter Klimatisierung, Netzanbindung etc. umfassende Vorkehrungen.

2.8 Gewährleistung der Belastbarkeit der Systeme

Die Belastbarkeit der Hardware bzw. des Rechenzentrums der Universität Oldenburg und des Uniklinikums RWTH Aachen genügt höchsten Anforderungen. Bezüglich der Anwendungsebene wird ebenfalls technisch über den Einsatz professioneller Technik (z. B. Reverse-Proxy-Anbindung) eine hohe Belastbarkeit und eine minimale Angriffsfläche realisiert. Während der Entwicklung der Pseudonymisierungssoftware werden Belastungstests mit Datenmengen ausgeführt, die oberhalb der geplanten Nutzung liegen, um die ausreichende Dimensionierung der Server zu erproben und Last-probleme weitgehend auszuschließen. Außerhalb dieses Belastungstestes ist eine hohe Belastung der Systeme nicht zu erwarten und auch kurzzeitige Ausfälle würden die Projektziele nicht gefährden.

2.9 Verfahren zur Wiederherstellung der Verfügbarkeit der Daten nach einem physischen oder technischen Zwischenfall

Die Zuordnungslisten des Pseudonymisierungsdienstes und die pseudonymisierten Daten der Auswertestelle werden durch regelmäßige Backups gesichert. Im Bedarfsfall können die bei der Auswertestelle vorliegenden Daten aus einem Backup wiederhergestellt werden. Die Backups werden für einen Monat gespeichert und anschließend automatisch gelöscht. Für den zentralen Pseudonymisierungsdienst wird eine Betriebsdokumentation erstellt, die auch Anleitungen zum Neu-Aufsetzen des Dienstes enthält. Zusammen mit den gesicherten Zuordnungslisten kann somit der Pseudonymisierungsdienst nach einem technischen Zwischenfall wiederhergestellt werden. Sollten Fehler bei einer Übertragung/Pseudonymisierung auftreten, können die gesendeten Daten verworfen und von den Dateneignern erneut verschickt werden.

2.10 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Eine jährliche Überprüfung (zu Beginn eines Kalenderjahrs, dokumentiert durch die Treuhandstelle) der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen ist Bestandteil des Betriebskonzepts. Die Standorte werden über die Überprüfung und das Ergebnis der Überprüfung informiert. Dabei werden die folgenden Aspekte geprüft und ggf. Maßnahmenergriffen:

- Release-Stände der verwendeten Betriebssysteme und Anwendungssoftware inkl. Prüfung, ob Patches regelmäßig installiert wurden
- Einsatz von Updateverfahren von Firewall und Virenschutz
- Evaluation von Sicherheitsvorfällen und Störungen
- Entsprechen die Maßnahmen noch dem Stand der Technik (insbesondere Entwicklungen bzgl. der Verschlüsselungstechnologien u. ä.)
- Wirksamkeit der Backup-Verfahren (ggf. Recovery-Test)
- Schulung der mit der Datenverarbeitung betrauten Personen

2.11 Schriftliche Dokumentation von sonstigen Maßnahmen

Für das Rechenzentrum des Uniklinikums RWTH Aachen existieren diverse technische und prozessorientierte Dokumentationen, die auf der Ebene der technischen Infrastruktur einen Betrieb nach dem Stand der Technik gewährleisten.

3 Betroffenenrechte

Betroffene Personen können ihre Betroffenenrechte gegenüber dem Projektkonsortium im Rahmen des Projektes geltend machen. Für die Wahrnehmung dieser Rechte sollte die Treuhandstelle kontaktiert werden, da diese Zugriff auf die identifizierenden Daten und Zuordnungslisten hat.

3.1 Erfüllung der Informationspflicht nach Art. 13/14 DSGVO

Für die Erhebung von personenbezogenen Daten beim Betroffenen im Rahmen der Patientenbefragung gilt Artikel 13 DSGVO. Für die Erhebung von personenbezogenen Daten bei Dritten im Rahmen der Nutzung von aller Daten im ILEG Projekt gilt Artikel 14 DSGVO. In beiden Fällen werden die Befragten gemäß Art. 13 und Art. 14 DSGVO entsprechend aufgeklärt (siehe auch Aufklärung über die Teilnehmerinformation/-aufklärung (Anlage 7 – Einwilligungserklärung EWE 1, Anlage 8 – Einwilligungserklärung EWE 2).

Darüber hinaus werden die Informationen nach Artikel 14 Abs. 1 und 2 bzw. Art. 9 Abs. 2 lit. a DSGVO für die Öffentlichkeit auf der Webseite des Projekts zur Einsicht gestellt. Für die Wahrnehmung dieser Rechte kann zusätzlich die ILEG Geschäftsstelle kontaktiert werden.

3.2 Erfüllung der Auskunftspflicht nach Art. 15 DSGVO

Die betroffenen Personen haben das Recht, Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden.

Eine Auskunft ist möglich, so lange die Pseudonym-Zuordnung beim Pseudonymisierungsdienst noch besteht, also gemäß der in Abschnitt 3.3 definierten Löschfrist. Ist diese Liste gelöscht, sind die Daten bei der Auswertestelle auch mit Hilfe des Pseudonymisierungsdienstes nicht mehr einer Person zuzuordnen und eine Auskunft kann nicht erteilt werden.

Die Anfrage zur Datenauskunft sollte über die Treuhandstelle erfolgen, da diese Zugriff auf die identifizierenden Daten und Zuordnungslisten hat. Sollten sich Betroffene direkt an die Auswertestelle oder die Dateneigner wenden, bekommen sie die Informationen nach Art. 13 bzw. 14 DSGVO (z. B. Kategorien der Daten, Rechtsgrundlage, Kontaktdaten). Da der Auswertestelle keine direkt personenidentifizierbaren Merkmale vorliegen, kann eine Anfrage dort nicht direkt bearbeitet werden und wird deshalb an die Treuhandstelle weitergeleitet. Die im Rahmen der Patientenbefragung Kontaktierten erhalten über die Teilnehmerinformation die dafür notwendigen Kontaktdaten.

Negativ-Auskünfte (wenn keine Verarbeitung im Projekt stattgefunden hat) werden direkt an den Betroffenen zurückgegeben. Eine weitere Kommunikation unter den Projektpartnern ist dann nicht erforderlich.

Für die Erteilung einer Auskunft nach Anfrage über die Treuhandstelle gilt folgendes Verfahren:

a) **Anfrage bei der Treuhandstelle** (schriftlich oder elektronisch)
b) **Weiterleitung der Anfrage an die Auswertestelle**
   Falls bestimmte Daten angefragt sind, muss ein erklärender Freitext vom Dateneigner an die Auswertestelle übermittelt werden; bei der Erteilung einer Standard-Auskunft muss nur die Information „Artikel-15-Auskunft“ zusammen mit dem Pseudonym (PSN) übermittelt werden. Damit die Auswertestelle den Betroffenen anhand des ihr vorliegenden Pseudonyms (PSN) identifizieren kann, wird analog zum Verfahren bei der Datenübermittlung die Anforderung über den Pseudonymisierungsdienst kommuniziert. Der Auswertestelle werden keine identifizierenden Daten übermittelt.
c) **Rückleitung der Daten an die betroffene Person**
   Die Daten werden ebenfalls analog zum normalen Datenversand über den Pseudonymisierungsdienst zurück kommuniziert. Die Daten werden tabellarisch gedruckt in einem versiegelten Umschlag an die Treuhandstelle verschickt.

d) **Beantwortung der Anfrage durch die Treuhandstelle** (schriftlich)

3.3 Verfahren bei Widerspruch nach Art. 21 bzw. Löschanfragen nach Art. 17 DSGVO

Die Betroffenen können eine Löschung der sie betreffenden personenbezogenen Daten bei der Auswertestelle verlangen. Da der wissenschaftliche Forschungszweck bei der zu erwartenden geringen Fallzahl an Löschungen bzw. Widersprüchen nicht „unmöglich oder ernsthaft beeinträchtigt“ werden würde (Art. 17 Abs. 3 lit. d DSGVO), bleibt bei den Betroffenen das Widerspruchsrecht nach Art. 17 bzw. Art 21 DSGVO bestehen.

Ebenso wie die Erfüllung der Auskunftspflicht ist die Möglichkeit zur Löschung nur so lange gegeben, wie die Pseudonym-Zuordnung beim Pseudonymisierungsdienst vorliegt. Ist diese Liste gemäß der in Abschnitt 3.3 definierten Frist gelöscht, sind die Daten bei der Auswertestelle faktisch nicht einem Betroffenen zuzuordnen und eine Löschung kann nicht mehr durchgeführt werden.

Die Anfrage zur Löschung sollte über die Treuhandstelle erfolgen, da nur diese Zugriff auf die identifizierenden Daten und Zuordnungslisten hat.

Negativ-Auskünfte (wenn die Person nicht betroffen oder die Zuordnung nicht mehr möglich ist) werden direkt an den Betroffenen zurückgegeben. Eine weitere Kommunikation unter den Projektpartnern ist dann nicht erforderlich.

Sollten sich Betroffene entgegen des etablierten Verfahrens direkt an die Auswertestelle oder den Dateneigner wenden, bekommen sie die Informationen nach Art. 13 bzw. 14 und werden gebeten die Anfrage ggf. erneut gegenüber der Treuhandstelle zu stellen.

Für die Durchführung der Löschung nach Anfrage über die Treuhandstelle, gilt folgendes Verfahren:

a) **Anfrage bei der Treuhandstelle** (schriftlich oder elektronisch)
b) **Datenlieferungen werden gestoppt**
   zuständige Mitarbeiter*innen werden informiert. Datenlieferungen werden gestoppt.
c) **Weiterleitung der Anfrage an die Auswertestelle und Dateneigner**
   Es muss nur die Information „Lösch-Anfrage“ an die Auswertestelle übermittelt werden. Die Anforderung wird analog zum Verfahren bei der Datenübermittlung über den Pseudonymisierungsdienst kommuniziert. Der Auswertestelle werden keine identifizierenden Daten übermittelt. An die Dateneigner wird der das Pseudonym erster Stufe übermittelt.
d) **Löschung und anschließende Bestätigung von der Auswertestelle und den Dateneignern an die Treuhandstelle**
   Die Auswertestelle bestätigt das Löschen der Daten. Die Dateneigner bestätigen das Löschen der Einwilligung im AKTIN Consent Manager.
e) **Löschung des SIC durch den Datenmanager.**
   Löschung des SIC aus der Patienten-Liste. Wiederaufnahme von Datenlieferungen.
f) **Beantwortung der Anfrage durch die Treuhandstelle** (schriftlich oder elektronisch)

3.3.1 Widerrufsfolgen bzw. Folgen von Löschanfragen

Ein Widerruf führt zu einer Löschung des Eintrages des/der Patienten*in in der Patientenliste, des Eintrages des/der Patienten*in in den Pseudonymisierungslisten, der bei den Dateneignern gespeicherten medizinischen Daten inklusive den registrierten Einwilligungen und der von der Auswertestelle gesammelten medizinischen Daten. Digitalisierte Kontaktdaten werden gelöscht. Daten für die eine Dokumentations- und Aufbewahrungspflicht gilt werden nicht gelöscht.

3.4 Verantwortung für die Umsetzung der Betroffenenrechte

Für die Erfüllung der Betroffenenrechte übernehmen die Auswertestelle und die Treuhandstelle die Verantwortung im Sinne von Art. 26 DSGVO. Die Treuhandstelle und die unabhängige

Auswertungsstelle werden vertraglich verpflichtet, entsprechend des hier definierten Prozesses an der Erteilung der Auskunft mitzuwirken. Die Dateneigner verpflichten sich ebenfalls zur Mitwirkung.

4 Vereinbarung zur gemeinsamen Verantwortlichkeit und Inkrafttreten

Das vorliegende Datenschutzkonzept wurde von allen Projektleitern der Konsortiumsmitglieder geprüft, die in den Prozess der Datenverarbeitung einbezogen sind. Das Datenschutzkonzept wird über einen Vertrag zur Vereinbarung zur gemeinsamen Verantwortlichkeit (gem. Art 26 DSGVO) in Kraft gesetzt.

6 Anlagen

Anlage 1 – Beteiligte Projektpartner

Anlage 2 – Ansprechpartner Datenschutz

Anlage 3 – Datensatzbeschreibung Datensatz Notaufnahmeprotokoll

Anlage 4 – Datenschutzkonzept AKTIN

Anlage 5 – Publikationsordnung

Anlage 7 – Einwilligungserklärung EWE 1

Anlage 8 – Einwilligungserklärung EWE 2

Anlage 9 – Datensatzbeschreibung Datensatz Rettungsdienst

Anlage 10 – Datensatzbeschreibung Datensatz Leitstelle

Anlage 11 – Datensatzbeschreibung Entlassdaten

Anlage 12 – Patientenbefragung

Anlage 13 – Hausarztbefragung

Literatur

[1] K. Pommerening and T. Müller, *Leitfaden zum Datenschutz in medizinischen Forschungsprojekten: Generische Lösungen der TMF 2.0,* MWV Med. Wiss. Verl.-Ges, Berlin, 2014.

[2] M. Kulla, M. Baacke, T. Schöpke, F. Walcher, A. Ballaschk, R. Röhrig, J. Ahlbrandt, M. Helm, L. Lampl, M. Bernhard, and D. Brammen, Kerndatensatz „Notaufnahme“ der DIVI. Notfall Rettungsmed **17** (2014), 671–681.

[3] Deutsche Forschungsgemeinschaft, Guidelines for Safeguarding Good Research Practice. Code of Conduct (2019).

[4] World Medical Association Declaration of Helsinki: ethical principles for medical research involving human subjects. JAMA **310** (2013), 2191–2194.