Datenschutzkonzept

Evaluierung der Qualitätsindikatoren von Notaufnahmen auf Outcome-Relevanz für den Patienten

Inhalt

Abkürzungs- und Symbolverzeichnis

DFG	Deutschen Forschungsgemeinschaft
DWH	Data Warehouse
FID	Temporäre Fragebogen ID
IDAT	Patienten-Identifizierende Daten
MDAT	Medizinische Daten
$MDAT_k$	Medizinische Daten Klinik
$MDAT_{sd}$	Medizinische Sekundärdaten der Krankenversicherung
Org DAT	Organisatorische Daten
PEWDAT	Einwilligungs-Daten
PID_k	Patienten-Identifikator Klinik
SIC	Subject Identification Code
PSN	Pseudonym
TK	Techniker Krankenkasse
TLS	Transportverschlüsselung (Transport Layer Security)

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)

Record Linkage: Die personen- bzw. patientenbezogene Verknüpfung von Daten verschiedener Datenquellen mittels geeigneter Schlüsselvariablen zur Beantwortung von wissenschaftlichen Fragestellungen (z. B. Daten der Sozialversicherung mit Daten aus der medizinischen Routineversorgung).

Vertrauensstelle: Unabhängige Einrichtung zur Annahme, Pseudonymisierung und Weiterleitung von Daten sowie Ausgabestelle für die Fragebögen zur Patientenbefragung.

Auswertestelle: Unabhängige Einrichtung zur Auswertung, Verarbeitung und datenschutzkonformen Weiterleitung der gesammelten medizinischen Daten an die Konsortialpartner

1. Beschreibung des Forschungsprojekts

1.1. Hintergrund

Jedes Jahr werden über 20 Millionen Patienten und Patientinnen in deutschen Notaufnahmen versorgt, Tendenz steigend. Das Forschungsprojekt *Evaluierung der Qualitätsindikatoren von Notaufnahmen*, kurz *ENQuIRE*, dient der Validierung von Indikatoren für die Beschreibung der Versorgungsqualität in Notaufnahmen.

Qualitätsindikatoren (QI) für unterschiedliche Bereiche der medizinischen Versorgung basieren häufig auf einem niedrigen Evidenzlevel. Gleichermaßen wurde ihre Validität in Bezug auf das patientenrelevante Outcome bislang kaum bzw. ungenügend untersucht. Indikatoren, die die tatsächliche Ergebnisqualität von Notaufnahmen widerspiegeln, sind aktuell aus Routinedaten nicht zu ermitteln und nur prospektiv zu erheben. Insbesondere sind Studien zur Lebensqualität als weiterer patientenrelevanter Endpunkt neben Morbidität und Mortalität im Setting Notaufnahme kaum vorhanden.

Im ENQuIRE Projekt werden Routinedaten auf Basis des Notaufnahmeprotokolls der Deutsche Interdisziplinäre Vereinigung für Intensiv- und Notfallmedizin e.V. (DIVI) mit Routinedaten der Techniker Krankenkasse auf der Individualebene verknüpft. Erstere Routinedaten werden über das Verbundforschungsprojekt *Verbesserung der Versorgungsforschung in der Akutmedizin in Deutschland durch den Aufbau eines Nationalen Notaufnahmeregisters*, kurz *AKTIN*, verfügbar gemacht. Mittels einer Patientenbefragung werden außerdem ergänzend Daten über die gesundheitsbezogene Lebensqualität (*patient reported outcome*) erhoben.

Aus dieser Datenbasis, die den Verlauf der Notfallversorgung auf Ebene der Versicherten und Leistungserbringer übergreifend sichtbar macht, werden QI abgeleitet, die als Grundlage für Verbesserungen bei Organisation, Finanzierung, Anreizen und Folgen der Notfallversorgung dienen sollen.

1.2. Ziele

Das Projekt hat die Evaluierung von QI für Notaufnahmen zum Ziel. Dazu sollen Daten aus Notaufnahmen mit Outcome-relevanten Daten aus der sich im Verlauf eines Jahres anschließenden ambulanten und stationären Versorgung datenschutzkonform auf Individualebene verknüpft und die gesundheitsbezogene Lebensqualität direkt erhoben werden.

Es lässt sich so prüfen, ob einige der bislang erhobenen, publizierten bzw. empfohlenen QI zur Beurteilung von Prozessen und Strukturen in Notaufnahmen neben ihrer prognostischen Validität und ihrer Bedeutung als Kennzahl auch eine Bedeutung als Parameter für die patientenrelevante Ergebnisqualität haben. Die prospektive Validierung der in vorbereitenden Arbeiten identifizierten QI hinsichtlich ihrer Outcome-Relevanz ermöglicht die Adjustierung derselben und unterstützt so die Entwicklung eines externen Benchmarkings für Notaufnahmen.

- Es werden die QI der Notaufnahme in Bezug auf ihr patientenrelevantes Outcome evaluiert.
- Der Einfluss von diesen QI auf die Inanspruchnahme von Versorgungsstrukturen im weiteren Behandlungsverlauf wird untersucht.
- Die Stärken und Schwächen der QI sowie die Schärfung einzelner QI werden untersucht. Es wird eine Basis zur Entwicklung neuer QI in Anlehnung an relevante methodische Grundlagen geschaffen.

Durch die Identifikation von valide zu erfassenden und signifikant mit dem patientenrelevanten Outcome assoziierten QI können Empfehlungen für die Verbesserung der Versorgung von Patienten/innen in der Notaufnahme gegeben werden.

- Ein Set praktikabler QI mit Outcome-Relevanz als Steuerungselement zur Bestimmung und perspektivischen Verbesserung der Ergebnisqualität von Notaufnahmen lässt sich bestimmen.
- QI können durch die Fachgesellschaften als einheitliche Basis für ein externes Benchmarking konsentiert werden.
- Indikatoren lassen sich als Grundlage für den Gemeinsamen Bundesausschuss (G-BA) für planungsrelevante QI gemäß § 136c SGB V empfehlen.

1.3 Datenerhebung im Forschungsprojekt

1.3.1 Zeitlicher Verlauf

Im ENQuIRE Projekt sollen im Rahmen einer Kohorten-Studie Routinedaten auf Basis des Notaufnahmeprotokolls der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin e.V. (DIVI) mit Routinedaten der Techniker Krankenkasse (TK) verknüpft werden, die vor und nach der Inanspruchnahme von Leistungen aus einer der teilnehmenden Notaufnahmen stammen (vgl. Abbildung 1). Routinedaten von einzelnen Fällen der teilnehmenden Notaufnahmen von Patienten/in, die einwilligen, an der Studie teilzunehmen, werden im Jahr 2019 gesammelt. Diese Daten werden mit zusätzlichen Daten des/der jeweiligen Patienten/in verknüpft, die von der TK routinemäßig erhoben werden. Die Daten stammen aus einem Zeitraum von einem Jahr vor und nach dem Notaufnahmekontakt des/der jeweiligen Patienten/in. Ein Teil der Patienten/innen wird im Rahmen einer Patientenbefragung während und 6 bis 8 Wochen nach dem Notaufnahmekontakt kontaktiert. Zusätzlich werden Leistungsdaten der Krankenhäuser und der Datensatz Strukturparameter Notaufnahmen erhoben.

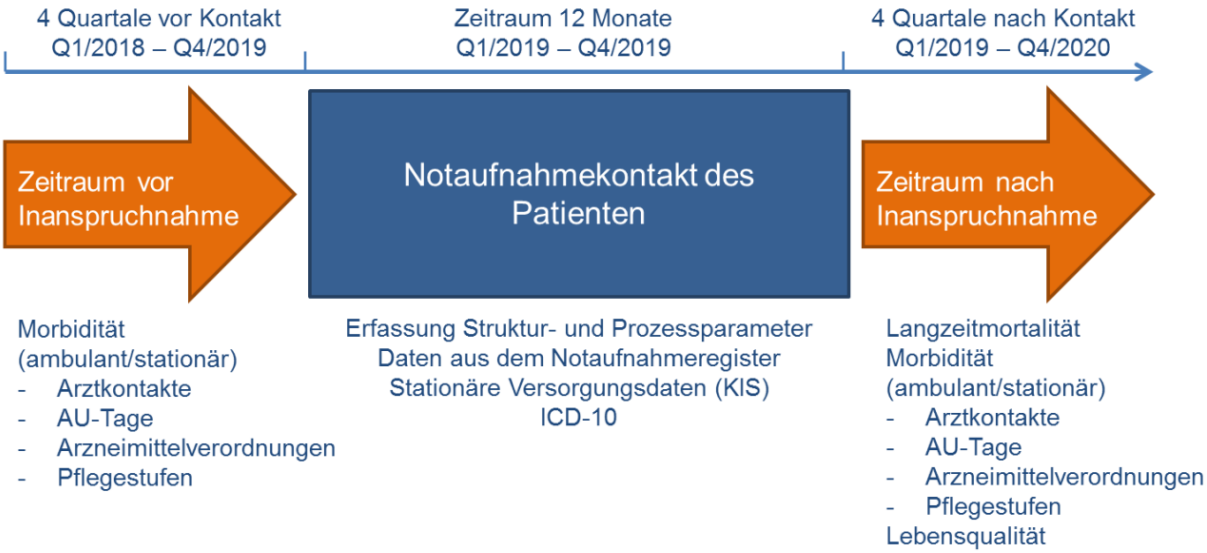

Abbildung 1: **Datenerhebungen im zeitlichen Verlauf**

1.3.1 Datenerhebung

Die Datenerhebung im Rahmen des ENQuIRE Projektes baut auf der Infrastruktur des deutschen Notaufnahmeregisters – entstanden im Rahmen des AKTIN-Projekts – auf (eine detaillierte Beschreibung der Datenflüsse findet sich in Abschnitt 4.1 Pseudonymisierung und Datenflüsse). Daten werden in Notaufnahmen erhoben, die einen einheitlichen Dokumentationsstandard in den Notaufnahmen etabliert haben (vgl. Abschnitt 2.1.4 AKTIN Infrastruktur). Die teilnehmenden Krankenhäuser speichern die ausgewählten Daten zu jedem/r Patienten/in der Notaufnahme in einem lokalen Data-Warehouse (DWH), welches Teil der Infrastruktur des AKTIN-Projektes ist. Grundlage für die elektronische Dokumentation ist der Datensatz Notaufnahme der DIVI (vgl. Anlage 1). Routinedaten von Patienten/innen, die einwilligen, an der Studie teilzunehmen, werden so mithilfe der Infrastruktur des deutschen Notaufnahme-Registers gesammelt. Anschließend werden die Daten

von einem Datentreuhänder, der sog. Vertrauensstelle, über die Infrastruktur des AKTIN-Projekts abgerufen. Diese Daten werden mittels einer Pseudonymisierungssoftware verschlüsselt und pseudonymisiert (vgl. Abschnitt 2.1.2 Software) an die sog. unabhängige Auswertestelle geliefert (vgl. Abschnitt Abschnitt 4.1.1 Sammlung und Weiterleitung der klinischen Primärdaten an die Auswertestelle)). Diese bereitet die Daten für weitere Analysen auf.

Um die Daten mit Routinedaten der TK verknüpfen zu können, werden die Patienten/innen im Rahmen der Studie von den Dateneignern (d.h. Kliniken und TK) und der Vertrauensstelle unter einem eindeutigen Pseudonym geführt, dem sog. Subject Identification Code, *SIC* (vgl. Abschnitt 4.1 Pseudonymisierung und Datenflüsse bzw. siehe Abbildung 3). Der SIC wird während der elektronischen Registrierung der Einwilligung eines/r Patienten/in im Krankenhaus generiert und in den DWH des AKTIN-Projektes gespeichert (vgl. Abschnitt 3.4 Erfassung der Einwilligungen). Für einen Datenauszug durch die TK werden zusätzlich die Krankenversicherungsnummern erhoben. Diese werden zusammen mit dem SIC auf der schriftlichen Einwilligungserklärung des/der Patienten/in notiert, an die Vertrauensstelle verschickt und dann an die TK in Form eines Scans sowie einer Patientenliste übermittelt (vgl. Abschnitt 4.1.3 Sammlung und Weiterleitung der Versicherungsdaten). Der SIC wird den jeweiligen Daten (sowohl in den einzelnen DWH des Notaufnahmeregisters als auch bei der TK) zugeordnet und kann anschließend genutzt werden, um im Zuge der Übermittlung der Daten an die Auswertestelle den SIC durch ein zweites eindeutiges Pseudonym, *PSN*, zu ersetzen (vgl. Abschnitt 2.1.2 Software). Die Auswertestelle kann über dieses Pseudonym PSN den Zusammenhang von Daten der Kliniken und TK herstellen.

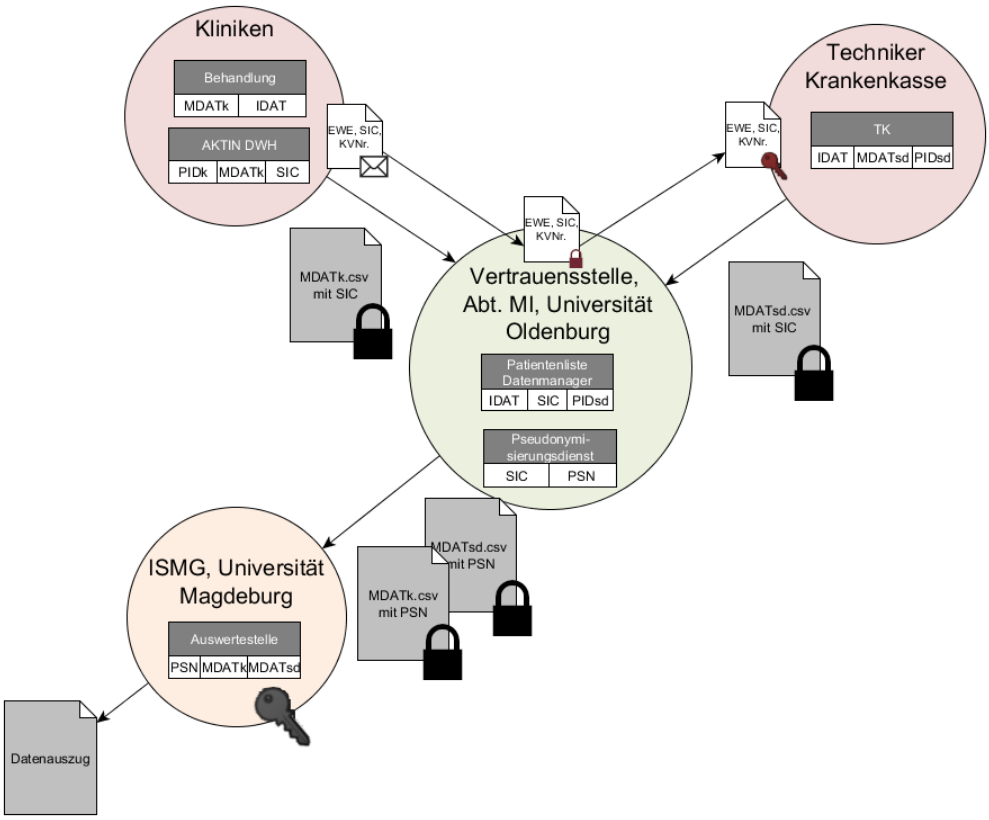

Abbildung 2: Schematischer Ablauf der Datenlieferungen von medizinischen Daten (MDAT) und Einwilligungserklärungen (EWE) im ENQuIRE Projekt.

Ein von der Auswertestelle ausgewählter Teil der registrierten Patienten/innen wird zusätzlich im Rahmen einer Patientenbefragung während und nach dem Notaufnahmekontakt kontaktiert (vgl. Abschnitt 4.1.4 Patientenbefragung). Dazu werden im Rahmen der schriftlichen Einwilligung des/der Patienten/in ebenfalls Kontaktdaten erhoben, die zusammen mit dem SIC in Form der schriftlichen Einwilligungserklärung des/der Patienten/in an die Vertrauensstelle versendet und dort verwaltet

werden (vgl. Abschnitt 3.4 Erfassung der Einwilligungen). Über einen temporären Fragebogen ID (FID) können die versendeten Fragebögen von der Auswertestelle einem Pseudonym PSN zugeordnet werden (vgl. Abschnitt 4.1.4 Patientenbefragung).

1.3.1 Datenschutzkonzept der TMF

Dieses Datenschutzkonzept folgt dem Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – generische Lösungen der TMF 2.0 [1]. Die Datenerhebung in den Kliniken erfolgt gemäß des *klinischen Moduls* im Sinne des organisatorischen und technischen Konzepts für Forschungsverbünde der TMF. Die Auswertung durch die unabhängige Auswertestelle folgt dem Konzept eines *Forschungsmoduls* im Sinne der TMF. Das treuhänderische Führen des Identitätsmanagements durch die Vertrauensstelle erfolgt ebenfalls im Sinne des generischen Datenschutzkonzeptes der TMF. Da es kein generisches Datenschutzkonzept für die Sammlung von Sozialdaten nach SGB X gibt, wird bei der Sammlung von Sekundärdaten der TK vom Datenschutzkonzept abgewichen. Das ENQuIRE Projekt baut auf der Infrastruktur des deutschen Notaufnahmeregisters – entstanden im Rahmen des AKTIN-Projekts – auf, das ebenfalls von der TMF begutachtet wurde. Im Gegensatz zu diesem wird das ENQuIRE Projekt auf Basis einer Einwilligung der teilnehmenden Patienten/innen durchgeführt.

1.4. Organisationsstruktur und Verantwortlichkeiten

1.4.1. Projektkonsortium

Das Projekt ENQuIRE wird unter Leitung des Universitätsklinikums Magdeburg (Universitätsklinik für Unfallchirurgie) zusammen mit der Otto-von-Guericke-Universität Magdeburg (Institut für Sozialmedizin und Gesundheitsökonomie), der Universität Oldenburg (Abt. Medizinische Informatik), der Universität Witten/Herdecke (Institut für Forschung in der Operativen Medizin), der Hochschule Niederrhein (Fachbereich Gesundheitswesen), der Charité Universitätsmedizin Berlin (Notfallmedizin) und der Techniker Krankenkasse (Fachbereich Versorgungsmanagement) durchgeführt.

1.4.2. Auswertung/Datenempfänger

- Institut für Sozialmedizin und Gesundheitsökonomie (ISMG) der Otto-von-Guericke-Universität Magdeburg (Unabhängige Auswertestelle und Interpretation)
- Universitätsklinik für Unfallchirurgie des Universitätsklinikum Magdeburg (Interpretation)
- Institut für Forschung in der Operativen Medizin der Universität Witten/Herdecke (Interpretation)
- Fachbereich Gesundheitswesen der Hochschule Niederrhein (Interpretation)
- Notfallmedizin der Charité Universitätsmedizin Berlin (Interpretation)
- Techniker Krankenkasse (Interpretation)

1.4.3. Dateneigner

Dateneigner der Krankenversicherungsdaten ist die Techniker Krankenkasse (TK). Dateneigner der Primärdaten sind die teilnehmenden Notaufnahmen bzw. Krankenhäuser, die Daten auf Basis des Notaufnahmeprotokolls der DIVI e. V. erfassen und im Rahmen des Verbundforschungsprojektes Verbesserung der Versorgungsforschung in der Akutmedizin in Deutschland durch den Aufbau eines Nationalen Notaufnahmeregister (AKTIN) zur Verfügung stellen.

Die geplante Zusammensetzung kann sich im Laufe des Projekts verändern. Konkret beteiligte Krankenhäuser zum Projektstart sind:

- Klinikum Aschaffenburg-Alzenau
- Helios Klinikum Berlin-Buch
- Klinikum Chemnitz gGmbH
- Klinikum Fürth
- Universitätsmedizin Göttingen
- Paracelsus-Klinik Henstedt-Ulzburg

- Universitätsklinikum Jena
- Universitätsklinikum Magdeburg
- Pius-Hospital Oldenburg
- Klinikum Stuttgart – Katharinenhospital
- Klinikum Wolfsburg
- Krankenhaus der Barmherzigen Brüder Trier
- Klinikum Memmingen
- Gesundheit Nord / Klinikverbund Bremen

Zusätzlich werden Daten in Notaufnahmen gesammelt, die nicht am AKTIN Projekt teilnehmen, jedoch ebenfalls Daten auf Basis des Notaufnahmeprotokolls der DIVI e. V. erfassen:

- Charité Berlin, Standorte Virchow Klinikum und Campus Mitte

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 5).

1.4.4. Vertrauensstelle

Die Abteilung Medizinische Informatik der Universität Oldenburg richtet eine Vertrauensstelle ein, die Patienten- und Pseudonymisierungslisten unter Wahrung des Datenschutzes führt und verwaltet. Teil der Vertrauensstelle sind ein Pseudonymisierungsdienst und ein/e Datenmanager/in. Die Vertrauensstelle arbeitet mandantenspezifisch und wird nur für das ENQuIRE-Projekt eingerichtet.

Dateneignern wird Software für den verschlüsselten Versand und die Erzeugung von Pseudonymen erster Stufe (Subject Identification Code, SIC) für die Zuordnung der Datensätze von der Abteilung Medizinische Informatik der Universität Oldenburg zur Verfügung gestellt. Die klinischen Daten auf Individualebene werden über das AKTIN Projekt exportiert bzw. im Falle der Klinik, die nicht am AKTIN Projekt teilnimmt, direkt an die Auswertestelle übermittelt.

Die Universität Oldenburg stellt einen Pseudonymisierungsdienst bereit, der Pseudonyme der zweiten Stufe (PSN) verwaltet, die dazu dienen, die Pseudonyme zwischen den Dateneignern und der Auswertestelle zu vermitteln (siehe Abbildung 3). Weitere Erläuterungen finden sich in Abschnitt 4.1.

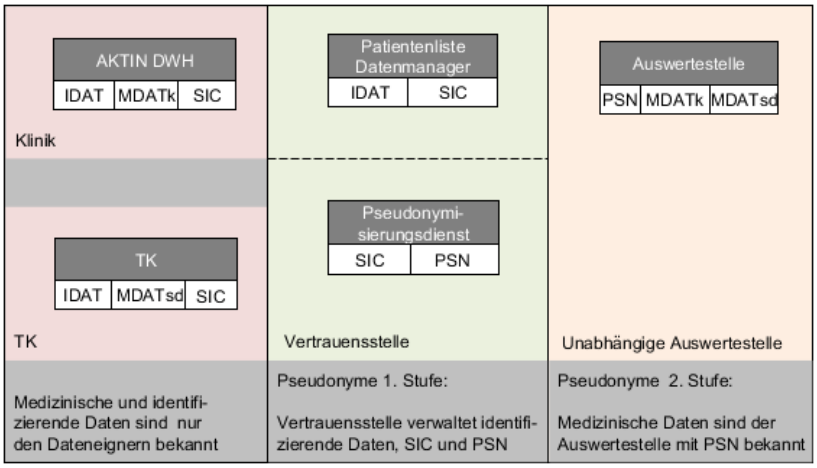

Abbildung 3: Pseudonyme 1. und 2. Stufe im ENQuIRE Projekt

1.4.5. Unabhängige Auswertestelle

Das Institut für Sozialmedizin und Gesundheitsökonomie der Otto-von-Guericke-Universität Magdeburg richtet eine unabhängige Auswertestelle ein, die die pseudonymisierten Daten verwaltet,

aufbereitet, ggfs. vergröbert und in Zusammenarbeit mit dem Data-Use-and-Access-Komitee an Konsortialpartner übermittelt.

1.4.6. Data-Use-and-Access-Komitee

Es wird ein Data-Use-and-Access-Komitee unter der Leitung der Konsortialführung (Universitätsklinik für Unfallchirurgie der Otto-von-Guericke-Universität Magdeburg) und der methodischen Projektleitung (Institut für Sozialmedizin und Gesundheitsökonomie der Otto-von-Guericke-Universität Magdeburg), unter Beteiligung der Vertrauensstelle (Carl von Ossietzky Universität), der Techniker Krankenkasse, der Notfallmedizin der Charité Universitätsmedizin Berlin, des Instituts für Forschung in der Operativen Medizin der Universität Witten/Herdecke, eines BVA-Mitglieds und eines Vertreters der Modellkliniken eingerichtet. Die Herausgabe eines 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 erstellt. Das genaue Vorgehen wird in einer Verfahrensordnung festgelegt.

1.4.7. Interpreten

Interpretierende Konsortialpartner können Datenauszüge auf der Grundlage einer formulierten Fragestellung und bezugnehmend auf ein *Data Dictionary* für alle Datenquellen des Projektes (wird noch erstellt) über das Data-Use-and-Access-Komitee beantragen. Darüber hinaus wird ein Basisvariablenset vom Data-Use-and-Access-Komitee erstellt, das interpretierenden Konsortialpartnern zur Verfügung gestellt wird.

1.4.7. Finanzierung

Das Projekt wird vom Innovationsfond finanziert, Förderkennzeichen FKZ01VSF17005.

1.5. Anfallende Daten

Im ENQuIRE Projekt werden Primärdaten in Notaufnahmen und durch Patientenbefragungen von Patienten/innen, die in diesen behandelt wurden, erhoben. Volljährige Patienten/innen, die die beteiligten Notaufnahmen im Jahr 2019 in Anspruch nehmen und Mitglied in der TK sind, werden vor Ort identifiziert und nach Aufklärung und schriftlicher Einwilligung in die Kohorten Studie einbezogen. Der Versichertenstatus der Patienten und Änderungen dessen werden erfasst. Grund und Datum eines Austritts werden erfasst und nur durchgängig in der TK versicherte Patienten berücksichtigt. Als Vergleichsgruppe werden die Daten aller Notaufnahmepatienten einer aggregierten Analyse zugeführt, um mögliche Verzerrungen durch Einschluss allein der TK-Versicherten zu überprüfen.

Bei ausgewählten Patientengruppen (ca. n=5000) erfolgt eine Fragebogen-gestützte Erhebung der gesundheitsbezogenen Lebensqualität nach der Notaufnahmebehandlung. Zur Evaluierung der Validität dieser retrospektiven Patientenbefragung erfolgt in einer Subgruppe von Patienten/innen an ausgewählten Studienzentren (Charité Berlin, Standorte Virchow Klinikum und Campus Mitte) eine zusätzliche Befragung (vgl. Abschnitt 4.1.4 Patientenbefragung).

Sekundärdaten werden sowohl von Krankenhäusern als auch von der Techniker Krankenkasse erhoben. Es werden nur jene Patienten/innen in die Studie einbezogen, die zum Behandlungszeitpunkt bei der Techniker Krankenkasse (TK) versichert sind (vgl. Abschnitt 4.1.3 Sammlung und Weiterleitung der Versicherungsdaten).

Durchschnittlich werden in den 15 angefragten Notaufnahmen jeweils 35.000 Patienten/innen pro Jahr versorgt, d.h. eine Gesamtzahl von 525.000 Patienten/innen ist zu erwarten. Davon sind ca. 85% in gesetzlichen Krankenversicherungen (GKV) versichert (der Rest verteilt sich auf Privatversicherte, Fälle der Berufsgenossenschaften und sonstige). Der Anteil der Versicherten der TK an der gesetzlich versicherten Bevölkerung beträgt 13,8% (Stand April 2017). Aus Erfahrungswerten der Konsortialpartner wird von einer Zustimmungsquote von 80% ausgegangen. Die Gesamtzahl der zu erwartenden Patienten/innen, die an der Studie teilnehmen, beläuft sich somit auf ca. 49.200.

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 von Qualitätsindikatoren gesammelt, die von einer Experten/innenrunde ausgewählt worden; Adressen werden für eine Kontaktierung des/der Patienten/in im Rahmen einer Patientenbefragung benötigt, Krankenversicherungsnummern werden von der TK zur Identifizierung von Datensätzen benötigt. Eine detaillierte Datensatzbeschreibung findet sich in Anlage 1 bis 4. 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.

Daten	Datenquelle
Klinische Primärdaten auf Individualebene	
Leitsymptom, Vorstellungsgrund	Datensatz Notaufnahme DIVI (Notaufnahmeregister), Klinikinformationssystem (KIS)
Prozessparameter	Datensatz Notaufnahme DIVI (Notaufnahmeregister), KIS
Notaufnahmediagnose (ICD-10-GM)	Datensatz Notaufnahme DIVI (Notaufnahmeregister)
Entlassdiagnose (ICD-10-GM)	KIS, Sekundärdaten der Techniker Krankenkasse
Klinische Sekundärdaten	
Leistungsdaten Krankenhaus	Entlassdaten der Krankenhäuser in einem Standardformat analog zum §21-Datensatz
Strukturparameter Notaufnahmen	Erhebung der Strukturdaten Notaufnahmen in Deutschland der DIVI und DGINA
Sekundärdaten auf Individualebene	
Anzahl der vertragsärztlichen Leistungsinanspruchnahmen	Sekundärdaten der Techniker Krankenkasse
Anzahl der Arbeitsunfähigkeitstage	
Anzahl und Art der Arzneimittelverordnungen	
Rehospitalisierungen	
Pflegegrad	
Patientenbefragung	
gesundheitsbezogene Lebensqualität, retrospektiv	patient-reported outcome, sozio-demografische Angaben SF 12 (SOEP-Version) Akutversion retrospektiv nach 6-8 Wochen
gesundheitsbezogene Lebensqualität, Klinik	patient-reported outcome, sozio-demografische Angaben SF 12 (SOEP-Version) Akutversion max. 3 Tage nach Notaufnahmebehandlung

Klinische Primärdaten

Datenquelle für die klinischen Daten aller teilnehmenden Patienten/innen ist der Datensatz Notaufnahme der DIVI, der im Notaufnahme-Informationssystem erfasst wird. Bei stationärer Aufnahme werden Daten aus dem weiteren stationären Behandlungsverlauf im Krankenhaus aus weiteren Klinikinformationssystemen (z. B. KAS) ebenfalls berücksichtigt (vgl. Abschnitt 4.1.1

Sammlung und Weiterleitung der klinischen Primärdaten). Mortalitätsdaten werden aus den Klinikdaten (Krankenhausmortalität) übernommen (detaillierte Datensatzbeschreibungen finden sich Anlage 1 bzw. Anlage 2).

Klinische Sekundärdaten
Teilnehmende Kliniken stellen Entlassdaten der Krankenhäuser in einem Standardformat analog zum §21-Datensatz zur Verfügung ebenso wie die Strukturparameter Notaufnahme (siehe Anlage 2 bzw. Anlage 4). Es werden Strukturdaten aus der *Erhebung der Strukturdaten Notaufnahmen in Deutschland der DIVI und DGINA* und den damit verbundenen Fragen zum Krankenhaus (Region, Bettenaufstellung und Fallzahlen, Fachabteilungen, Netzwerke, kassenärztlicher Bereitschaftsdienst, Weiterbildung und dezentrale Notaufnahmen) und zur Notaufnahme (Organisation, Kapazität, Informationstechnologie, apparative Ausstattung, Patientenkontakte nach Zuweisung, Weiterbehandlung und Fallart, Transportmittel, Versorgungsprozess, Personalaufwand, Person) ausgewertet (vgl. Abschnitt 4.1.2 Sammlung und Weiterleitung der klinischen Sekundärdaten).

Sekundärdaten der gesetzlichen Krankenversicherung
Die Techniker Krankenkasse übermittelt Routinedaten der Gesetzlichen Krankenversicherung (GKV) von teilnehmenden Patienten/innen. Für eine Bewertung der Ergebnisqualität nach der Entlassung aus der Notaufnahme bzw. stationären Behandlung werden Daten aus vier Quartalen nach der Inanspruchnahme der Notaufnahmen herangezogen. Zur Risikoadjustierung werden patientenbezogene Daten aus vier Quartalen vor Inanspruchnahme sowie Strukturdaten der jeweiligen Notaufnahmen berücksichtigt. Mortalitätsdaten werden aus den Sekundärdaten (Langzeitmortalität) übernommen. Außerdem werden Morbiditätsmerkmale erfasst, soweit sie sich in den Sekundärdaten abbilden. Dazu zählen u.a. vertragsärztliche Leistungsinanspruchnahme, Rehospitalisierungen, Arzneimittelverordnungen, Arbeitsunfähigkeit (AU-Fälle und –tage) und Pflegegrade (siehe Anlage 3, vgl. Abschnitt 4.1.3 Sammlung und Weiterleitung der Versicherungsdaten).

1.5.4 Patientenbefragung
Die gesundheitsbezogene Lebensqualität und Zufriedenheit als weitere patientenrelevante Endpunkte werden als *patient-reported outcome* erhoben. Die Patientenbefragung erfolgt für von der Auswertestelle definierte Subgruppen entweder ca. 2 bzw. ca. 6-8 Wochen nach Inanspruchnahme der Notaufnahme (siehe Anlage 14 bzw. Anlage 15).

1.5.5 Schutzbedarf und Risikoklassifiziernug
Bei den im Projekt erhobenen Gesundheitsdaten handelt es sich im Sinne der DSGVO um personenbezogene Daten der besonderen Kategorie. Für diese Daten gilt ein entweder ein hoher Schutzbedarf bzw. sehr hoher Schutzbedarf. Insbesondere Daten mit sehr hohem Schutzbedarf werden von der Vertrauensstelle 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 4.

Tabelle 2: Schutzbedarf und Risikoklassifizierung nach DIN 66399

Datenquelle	Schutzbedarf	Risikoklasse
Klinische Primärdaten auf Individualebene (verschlüsselt durchgeleitet)		
Leitsymptom, Vorstellungsgrund	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Prozessparameter	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Notaufnahmediagnose (ICD-10-GM)	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2

Entlassdiagnose (ICD-10-GM)	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Klinische Sekundärdaten (verschlüsselt durchgeleitet)		
Leistungsdaten Krankenhaus	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Strukturparameter Notaufnahmen	Normaler Schutzbedarf, Schwere eines möglichen Schadens ist überschaubar	1
Sekundärdaten auf Individualebene (verschlüsselt durchgeleitet)		
Anzahl der vertragsärztlichen Leistungsinanspruchnahmen	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Anzahl der Arbeitsunfähigkeitstage	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Anzahl und Art der Arzneimittelverordnungen	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Rehospitalisierungen	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Pflegegrad	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Patientenbefragung		
gesundheitsbezogene Lebensqualität, retrospektiv	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
gesundheitsbezogene Lebensqualität, Klinik	Hoher Schutzbedarf, Schwere eines möglichen Schadens ist substantiell	2
Organisatorische Daten (Vertrauensstelle)		
Krankenversicherungsnummer	Sehr hoher Schutzbedarf, Schwere eines möglichen Schadens ist groß	3
Kontaktdaten	Sehr hoher Schutzbedarf, Schwere eines möglichen Schadens ist groß	3
Patienten-Listen	Sehr hoher Schutzbedarf, Schwere eines möglichen Schadens ist groß	3
Pseudonymisierungs-Listen	Sehr hoher Schutzbedarf, Schwere eines möglichen Schadens ist groß	3

1.6. Re-Identifizierungsmöglichkeiten

Die Daten liegen für die Auswertung in pseudonymisierter Form i. S. d. Artikel 4 Nr. 5 DSGVO vor. Die Pseudonyme (PSN) des Auswerte-Datensatzes können nur durch das Zusammenwirken der Vertrauensstelle und eines Dateneigners/in 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 bzw. Versicherte zu ermöglichen.

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:

- Versicherte bzw. Patienten/innen
- Krankenhausmitarbeiter/innen
- Krankenhäuser

1.7. Rechtsgrundlagen der Datenverarbeitung

Die gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung treffen die unabhängige Auswertestelle (Institut für Sozialmedizin und Gesundheitsökonomie der Otto-von-Guericke-Universität Magdeburg) und die Vertrauensstelle (Abteilung Medizinische Informatik der Universität Oldenburg). 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. Die Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten ist die freiwillige schriftliche Einwilligung gemäß DSGVO. Für die Verarbeitung und Archivierung der Daten gilt Art. 89 DSGVO und § 27 BDSG (neue Fassung, 2018).

1.7.1 Ebene 1: Klinische Daten

Die Versicherten werden durch die Teilnehmerinformation aufgeklärt und geben ihre Einwilligung für die Einholung, Übermittlung, Verarbeitung und Speicherung ihrer Daten (vgl. Art. 6 Abs. 1 lit. a DSGVO), ebenso wie eine Entbindung von der ärztlichen Schweigepflicht (gem. § 203 StGB).

1.7.2 Ebene 2: Daten der gesetzlichen Krankenversicherung

Für die Verarbeitung der Krankenversichertendaten gilt das SGB X. Die Nutzung von Versichertendaten wird beim Bundesversicherungsamt beantragt. Die Versicherten werden durch die Teilnehmerinformation aufgeklärt und geben ihre Einwilligung für die Einholung, Übermittlung, Verarbeitung und Speicherung ihrer Krankenversicherungsdaten (vgl. Art. 6 Abs. 1 lit. a DSGVO).

1.7.3 Ebene 3: Patientenbefragung

Die Versicherten werden durch die Teilnehmerinformation aufgeklärt und geben ihre Einwilligung für die Einholung, Übermittlung, Verarbeitung und Speicherung ihrer Daten sowie für die Kontaktierung bzw. Re-Kontaktierung zum Zwecke der Patientenbefragung (vgl. Art. 6 Abs. 1 lit. a DSGVO).

1.8. 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. Die Projektleitung von ENQuIRE hat zum Vorgehen im Projekt und zum Datenschutzkonzept zudem ein Votum des Datenschutzbeauftragten des Landes Sachsen-Anhalt eingeholt (siehe Anlage 16).

Es werden bzgl. der wissenschaftlichen Qualität die Vorgaben für Gute Praxis Sekundärdatenanalyse (GPS [2]), die Richtlinien zur Sicherung der guten wissenschaftlichen Praxis der Deutschen Forschungsgemeinschaft, sowie der Guten Epidemiologischen Praxis (GEP [3]) eingehalten.

Über die Ethikkommission der Otto-von-Guericke-Universität Magdeburg wird ein koordiniertes Verfahren beantragt, um ein gemeinsames Ethik-Votum für alle relevanten Kommissionen zu erhalten

(siehe Anlage 10). Die im Projekt genutzte Infrastruktur des AKTIN Registers wurde bereits von den Ethikkommissionen der Universitäten Magdeburg und Oldenburg begutachtet.

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 Vertrauensstelle 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 (http://www.enquire-projekt.de).

2. IT-Infrastruktur

2.1. IT-Komponenten

2.1.1. Hardware

Für den Pseudonymisierungsdienst (betrieben von der Universität Oldenburg) wird ein virtueller Server im Rechenzentrum der Universität eingesetzt.

Die technische Infrastruktur des ISMG ist in Anlage 11 beschrieben. Da die Klinik für Unfallchirurgie Magdeburg für die Datenverarbeitung auf den gleichen Server zugreift, gelten die in der Anlage beschriebenen Vorkehrungen gleichermaßen für beide Auswertestellen.

2.1.2. Software

Für die erste Pseudonymisierungsstufe der klinischen Daten in AKTIN Kliniken (lokal beim Dateneigner) wird der während der Laufzeit des AKTIN-Projektes entwickelte und in den AKTIN Data-Warehouse-Manager integrierte, *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.

Für die erste Pseudonymisierungsstufe der klinischen Daten in Kliniken, die nicht am AKTIN Projekt teilnehmen, wird eine eigens dafür entwickelte Java-Anwendung eingesetzt. Die Software generiert lokal *Subject Identification Codes* (SIC), mit denen die klinischen Daten des/der Patienten/innen später den Sekundärdaten der Techniker Krankenkasse zugeordnet werden können.

Die Zuordnung der Pseudonyme der zweiten Pseudonymisierungsstufe (PSN) zur Zusammenführung der Daten geschieht lokal bei der Auswertestelle mit einer separaten, eigens dafür entwickelten Java-Anwendung. Zentraler Baustein der Pseudonymisierungssoftware ist ein Webservice, der eindeutig Pseudonyme der ersten Pseudonymisierungsstufe in Pseudonyme der zweiten Pseudonymisierungsstufe tauscht und versendet (vgl. Abbildung 4). Diese Software wird unabhängig von AKTIN betrieben und auf den Servern der Universität Oldenburg gehostet. Das Gesamtsystem besteht aus zwei Elementen, einer Client-Software und einem serverbasierten Dienst. Die lokale Client-Software wird sowohl von Dateneignern als auch von Datenempfängern verwendet. Beide Benutzergruppen verwenden unterschiedliche Funktionalitäten der Software. Die Dateneigner nutzen Patienten-Identifikatoren (im Falle des ENQuIRE Projekts handelt es sich dabei um den SIC), die durch eine Anfrage für eine temporäre ID an den Pseudonymisierungsdienst übermittelt werden. Diese temporären IDs werden anschließend als Ersatz für identifizierende Personendaten eingesetzt. Für die Datenempfänger erfolgt ein analoger Prozess, allerdings mit dem Austausch temporärer IDs zu permanenten Pseudonymen (PSN). Die Funktionalitäten der Datenverarbeitung stellen Basisfunktionen dar und werden von beiden Benutzergruppen geteilt. Der Pseudonymisierungsdienst stellt die Verwaltungslogik und die Verwaltung von Patienten-Identifikatoren, temporären IDs sowie PSNs. Der Pseudonymisierungsdienst ist ein passiver Teilnehmer und reagiert nur auf Anfragen der

jeweiligen Nutzer bzw. deren Software. Die Verbindungen müssen stets von Seiten des Clients (Dateieigner/Datenempfänger) initiiert werden. Es müssen keine eingehenden Verbindungen in den dortigen Firewalls konfiguriert werden. Details zur Implementierung sind der Anlage 9 zu entnehmen.

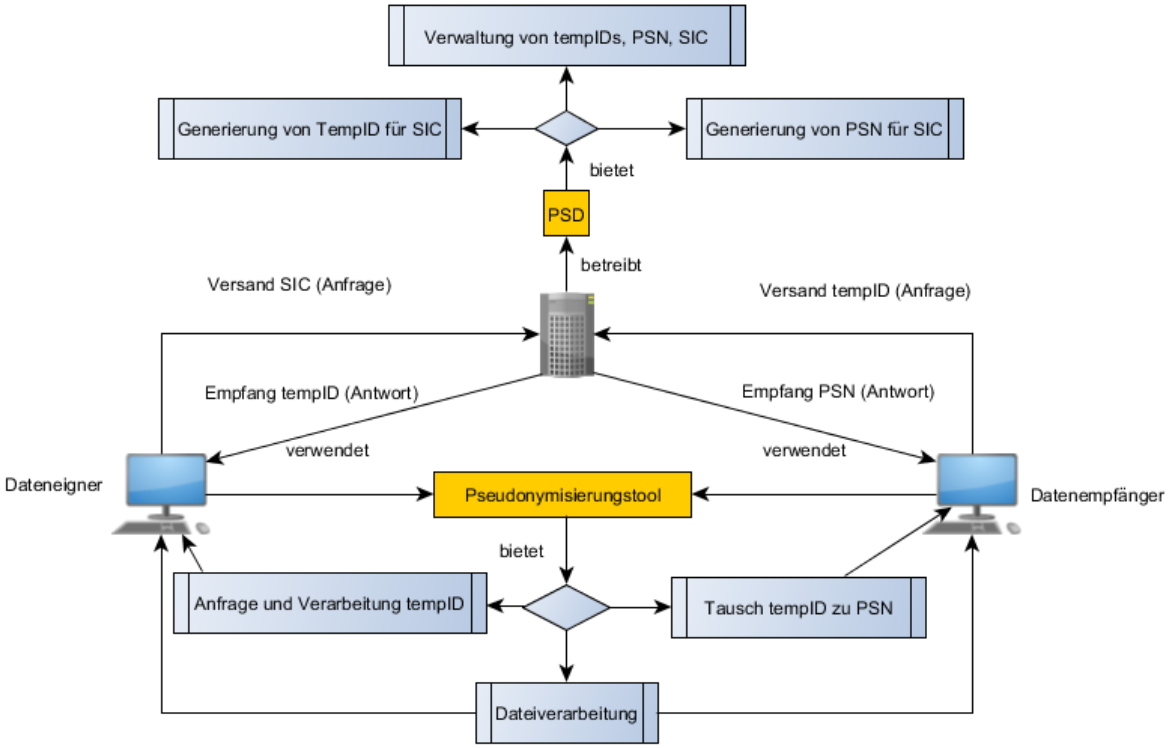

Abbildung 4: Technische Übersicht der Pseudonymisierungssoftware für SIC und Pseudonyme (PSN)

2.1.3. Datenübertragung

Die Daten werden mit Pseudonym (SIC) versehen derart verschlüsselt vom Pseudonymisierungsdienst durchgeleitet, dass eine Kenntnisnahme seitens des Pseudonymisierungsdienstes oder anderer Dritter ausgeschlossen ist (vgl. Abschnitt 4.2.2 Übermittlung der Daten zwischen Dateneignern und Auswertestelle). Klinische Daten und Sekundärdaten der Krankenkassen werden anhand der Pseudonyme zusammengeführt und verschlüsselt mit neuen, dauerhaften Pseudonym PSN versehen an die Auswertestelle gesendet.

2.1.4. AKTIN Infrastruktur

Die teilnehmenden Krankenhäuser speichern ausgewählte Daten zu jedem Patienten in der Notaufnahme in einem lokalen Data Warehouse (DWH) in einem standardisierten Format. Mittels einer Exportschnittstelle werden Notaufnahmeprotokolle aus dem Informationssystem der Notaufnahme digital exportiert und als standardisierte HL7-CDA-Dokumente abgelegt. Diese CDA-Dokumente werden anschließend auf den DWH-Server übertragen. Über eine weitere Schnittstelle können außerdem zusätzliche Daten im CSV-Format übertragen werden. Der Server und die im DWH gespeicherten Daten sind Eigentum des jeweiligen Krankenhauses.

Die regulär im Rahmen des AKTIN-Projekts gespeicherten Daten sind pseudonymisiert und beinhalten keine identifizierenden Daten. Zur Vermeidung von Duplikaten wird ein Einweg-Hashverfahren verwendet und der berechnete Einweg-Hash patientenbezogen im DWH gespeichert. Alle Daten verbleiben innerhalb der patientenführenden Abteilung (i.d.R. Zentrale Notaufnahme) – Zugriff auf die

Daten haben nur berechtigte Mitarbeiter/innen dieser Abteilung über die Benutzeroberfläche des DWH. An der ENQuIRE Studie teilnehmenden Patienten kann allerdings über eine zusätzliche im DWH hinterlegte Tabelle ein SIC zugeordnet werden. In dieser Tabelle wird mithilfe der AKTIN Consent Manager Oberfläche der Einschluss von Patienten/innen für die Studie registriert (vgl. 3.4 Erfassung der Einwilligungen); SIC und eine klinikinterne Patientennummer werden gespeichert. Die gespeicherten Daten von an der ENQuIRE Studie teilnehmenden Patienten/innen sind dementsprechend zwar pseudonymisiert, beinhalten allerdings identifizierenden Daten, die die Verknüpfung von mehreren Datenquellen erlauben.

Alle Anfragen für Datenauszüge für Forschungsvorhaben und Fragestellungen (z.B. für Forschung, Qualitätssicherung) werden durch ein Review-Verfahren geprüft und anschließend an die teilnehmenden Kliniken weitergeleitet. In jeder Klinik muss der Fragestellung explizit zugestimmt werden, bevor eine Abfrage durchgeführt und Daten exportiert werden. Die Exporte der Kliniken werden an einer zentralen, unabhängigen Stelle (AKTIN Broker) gesammelt und nach Prüfung an die Forscher übermittelt.

2.2. Rollen und Rechte

2.2.1. Vertrauensstelle

Für die Verarbeitung und die Verwaltung der Zuordnungslisten zweiter Stufe von SIC und PSN, nicht jedoch die Identitätsdatendaten, werden ausgewählte Mitarbeiter/innen der Universität Oldenburg benannt. Diese Mitarbeiter/innen sind für den *Pseudonymisierungsdienst* zuständig (siehe Anlage 7).

Für den Empfang und die Verarbeitung der Einwilligungserklärungen, das Führen von Kontaktdaten und Zuordnungslisten erster Stufe (IDAT zu SIC) sowie der Anforderung von Daten bei der Krankenkasse und die Kontaktierung bzw. den Versand der Patientenbefragungen wird ein/e ausgewählter Mitarbeiter/in der Universität Oldenburg als *Datenmanger/in* benannt (siehe Anlage 7). Diese/r Mitarbeiter/in ist nicht für den Pseudonymisierungsdienst zuständig. Für die Einrichtung und den Betrieb der technischen Infrastruktur für den Pseudonymisierungsdienst, den AKTIN-Export und das Record Linkage werden ausgewählte Mitarbeiter/innen der Universität Oldenburg benannt (siehe Anlage 7).

2.2.2. Auswerter

Der Gesamtdatensatz wird von der Vertrauensstelle allein an die unabhängige Auswertestelle (ISMG, Otto-von-Guericke-Universität Magdeburg) übermittelt. Die Verarbeitung der pseudonymisierten klinischen Daten sowie Krankenkassen- und Befragungsdaten ist nur Mitarbeitern des ISMG der Otto-von-Guericke-Universität Magdeburg gestattet. Beim Konsortialführer wird eine Liste derjenigen Personen geführt, die zum Umgang mit den Daten berechtigt sind sowie eines internen Ansprechpartners in datenschutzrechtlichen Angelegenheiten (siehe Anlage 6 bzw. Anlage 7). Die Namensliste wird fortlaufend aktualisiert. Nicht in der Anlage gelistete Personen wird der Zugang durch Zugangsbeschränkungen technisch verschlossen. Alle Personen, die Datenzugang erhalten, unterschreiben eine Schweigepflichterklärung. Sie unterliegen auch nach dem Ende des Projekts der Geheimhaltungspflicht.

2.2.3 Data-Use-and-Access-Komitee

Die weiteren Projektteilnehmer können Datensätze für die Beantwortung ihrer Fragestellungen anfordern. Die Herausgabe eines Datensatzes wird beim *Data-Use-and-Access-Komitee* des ENQuIRE-Projektes beantragt. Das Komitee prüft den Antrag und sendet - bei positiver Bewertung - den informationen über den jeweiligen Datenauszug an die Auswertestelle, die die Daten dann an den jeweiligen Projektteilnehmer versendet. Die Auswahl der Fälle, Variablen und Ausprägungen erfolgt

anhand der konkreten Fragestellung, so dass jeweils nur ein reduzierter Datensatz an die auswertenden Stellen übermittelt wird[1].

2.2.4. Weitere Beteiligte des Projektkonsortiums

Mitarbeiter/innen der Universität Oldenburg werden keinen Zugriff auf die klinischen Daten sowie Krankenkassen- und Befragungsdaten erhalten, die bei der Auswertestelle vorliegen. Mitarbeiter der Universität Witten/Herdecke, Hochschule Niederrhein, Charité Universitätsmedizin Berlin sowie der Techniker Krankenkasse haben ebenfalls keinen direkten Zugriff auf die klinischen Daten, sondern wirken nur bei der Interpretation mit.

2.2.5. Rollenkonflikte

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

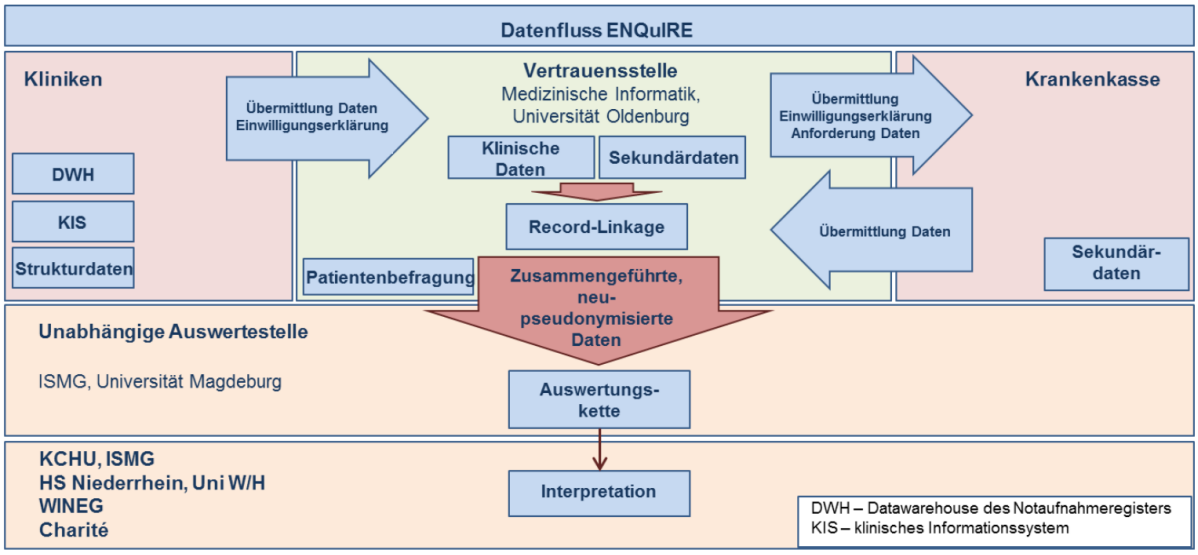

Abbildung 5: Datenflüsse und Zuständigkeitsbereiche

3. IT-gestützte Prozesse

3.1. Datenerhebung und –speicherung

Die Datenerhebung erfolgt in der Ebene 1 (vgl. 1.6.1) in Notaufnahmen von Kliniken, die am AKTIN-Projekt teilnehmen. Die Daten werden mit der Infrastruktur des AKTIN-Projekt erhoben (vgl. 2.1.4) und für das ENQuIRE Projekt verwendet. In Ebene 2 (vgl. 1.6.2) erfolgt die Datenerhebung durch Aufbereitung bereits erhobener Daten (Sekundärdaten). In Ebene 3 (Befragung, vgl. 1.6.3) werden die Daten Papier-basiert erhoben und anschließend von der Auswertestelle digitalisiert; nach der Erfassung werden die originalen Fragebögen vernichtet.

3.2. Datenverarbeitung

Die klinischen Daten und die Sekundärdaten der Krankenkasse (vgl. 1.4.1 und 1.4.3) werden über den in Abschnitt 4.2 beschriebenen Pseudonymisierungsprozess ohne inhaltliche Manipulation an die Auswertestelle übermittelt.

Die Fragebögen der Patientenbefragung (vgl. 1.4.4) werden vom Datenmanager/in Vertrauensstelle an Patienten/innen verschickt, die von der Auswertestelle bestimmt wurden. Die Daten der Patientenbefragung erreichen die Auswertestelle direkt von dem/der Befragten in Papier-basierter

[1] 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.

Form ohne Absender, versehen mit einer temporären Fragebogen ID, die einem Pseudonym PSN zugeordnet werden kann (vgl. Abschnitt 4.1.4 Patienten/innenbefragung), und werden in der Auswertestelle elektronischerfasst. Sind zu einer Person mehrere Datenarten verfügbar, werden diese anhand des Pseudonyms miteinander verknüpft (vgl. Abschnitt 1.6.2).

Die Daten werden von der Auswertestelle gemäß der formulierten Ziele und wissenschaftlicher Standards ausgewertet. Eine darüberhinausgehende Datenverarbeitung findet nicht statt.

3.3. Datenlöschung

Die Datenübermittlungen bzw. -erhebungen sind für die Jahre 2018 bis 2020 vorgesehen (vgl. Abbildung 1).

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 01.05.2022 durch den Pseudonymisierungsdienst vorgehalten und zu diesem Datum gelöscht.

Es ist den Daten-auswertenden Stellen erlaubt, die Daten bis zu 10 Jahre nach Ende der Projektförderung durch den Innovationsfonds auszuwerten. 10 Jahre nach Projektende (am 01.05.2032) werden die Daten nicht mehr benötigt und mit der unten genannten Ausnahme und Einschränkung vollständig von allen Speichermedien gelöscht bzw. vernichtet.

Die Krankenversicherungs-, klinischen- und Befragungsdaten, die der Universität Magdeburg und dem Universitätsklinikum Magdeburg 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 01.05.2032. Zu diesem Zweck wird eine digitale Kopie des Datenbestandes im ISMG der Otto-von-Guericke-Universität Magdeburg auf einem geeigneten Datenträger (passwortgeschützt) gespeichert und im Tresor des Direktors des ISMG für zehn Jahre, d. h. bis zum 01.05.2032, aufbewahrt.

Die bei der Übermittlung anfallenden temporären IDs (von der Pseudonymisierungssoftware generierte tempIDs sowie FIDs und Auftragsnummern) werden unverzüglich gelöscht, wenn die Zusammenführung erfolgt ist. Ausgefüllte Fragebögen werden nach der elektronischen Erfassung in der Auswertestelle vernichtet.

3.4 Erfassung der Einwilligungen

Patienten/innen der Techniker Krankenkasse werden in den Notaufnahmen gemäß der Deklaration von Helsinki nur nach erfolgter Aufklärung und dokumentierter Einwilligungserklärung in die Studie einbezogen (Anlage 5). Die Identifikation der Patienten/innen und Einholung der Einwilligungserklärung erfolgt über eine/n Studienassistenten/in. Die von den Krankenhäusern angestellten Studienassistenten/innen haben Einsicht in den Versichertenstatus des/der Patienten/in, sprechen den/die jeweilige/n Patienten/in an und führen ein Aufklärungsgespräch. Sollten Patienten/innen aufgrund ihres akuten Zustandes nicht einwilligungsfähig sein, kann die Einwilligung bei stationär aufgenommenen Patienten/innen noch während der Krankenhausbehandlung nach einem Aufklärungsgespräch eingeholt werden. Nach dem Aufklärungsgespräch erhält der/die teilnehmende/r Patient/in eine Einwilligungserklärung, zwei weitere unterschriebene Erklärungen werden von dem/der Studienassistenten/in gesammelt und anschließend im AKTIN Consent Manager elektronisch dokumentiert. Die klinikinterne Patientennummer dient nur dem Zwecke der Zusammenführung der Daten und wird nie übermittelt. Der SIC wird auf der jeweiligen Einwilligung notiert. Die gesammelten Einwilligungserklärungen und personenbezogenen Daten zum Zwecke der Kontaktierung und der Zusammenführung der Daten werden zweiwöchentlich postalisch an die Vertrauensstelle z. Hdn. des/der Datenmanagers/in verschickt. Kontaktdaten und Krankenversicherungsnummern werden vom Datenmanager/in digitalisiert und unter Wahrung der Vertraulichkeit in einer Datenbank auf einem Server, der im Rechenzentrum der Universität Oldenburg betrieben wird, gespeichert.

Die Patienten/innen können abgestuft einer Teilnahme am Projekt und einer Kontaktierung zum Zwecke der Patientenbefragung zustimmen. Sie stimmen einer Übermittlung von Gesundheitsdaten zu und willigen ggf. ein, nach der Inanspruchnahme der Notaufnahme (6 bis 8 Wochen nach Index-Kontakt mit der Notaufnahme) für eine Befragung kontaktiert werden zu dürfen (Anlage 5). Die Patienten/innen teilen Kontaktdaten und Krankenversichertennummer mit und erklären sich damit einverstanden, dass personenbezogene Daten im Rahmen der Studie erhoben und zum Zwecke der Kontaktaufnahme sowie der Zusammenführung von Datensätzen an die Vertrauensstelle übermittelt werden. Die Patienten erklären sich außerdem damit einverstanden, telefonisch kontaktiert zu werden.

Im Falle von in der Notaufnahme verstorbenen Patienten/innen wird eine Ausnahmeregelung nach Paragraph § 75 SGB X angestrebt, so dass diese Patienten/innen zur Minimierung eines *Selection Bias* ebenfalls in die Auswertungen einbezogen werden können. Die konkrete Ausgestaltung dieses Vorgehens wird im Rahmen des Projekts mit den Datenschutzbeauftragten der beteiligten Kliniken und der Techniker Krankenkasse abgestimmt.

4. Technische und organisatorische Maßnahmen

Die technisch-organisatorischen Maßnahmen bei den Dateneignern sind nicht Bestandteil der Datenschutzvereinbarung, da der Schutzbedarf dort unabhängig vom Projekt besteht und entsprechend bereits umgesetzt ist. Insbesondere handelt es sich dabei um Datenverarbeitungen mit anderen Zwecken und Rechtsgrundlagen außerhalb der Regelungskompetenz des Projektkonsortiums.

Auf die Maßnahmen bei der Auswertestelle wird nicht im Detail eingegangen, da diese bereits in einem eigenen Datenschutzkonzept (Anlage 11) beschrieben sind. Die Maßnahmen der Datensammlung in den Notaufnahmen, die mithilfe der Infrastruktur des AKTIN Projektes stattfinden, sind in einem eigenen Datenschutzkonzept beschrieben (Anlage 12), gleiches gilt für die Datensammlung bei der Techniker Krankenkasse (Anlage 16)

Die technisch-organisatorischen Maßnahmen der Universität Oldenburg bzw. des Pseudonymisierungsdienstes werden so weit dargestellt, wie es für den Gesamtprozess Relevanz hat. Für die hier verarbeiteten Daten gilt ein entweder ein hoher Schutzbedarf bzw. sehr hoher Schutzbedarf. Insbesondere Daten mit sehr hohem Schutzbedarf werden von der Vertrauensstelle verwaltet. Für alle weiteren Daten, die gesammelt erhoben werden, gelten Maßnahmen entsprechend eines hohen Schutzbedarfs. Mit Hilfe der technischen und organisatorischen Maßnahmen werden insbesondere die durch Art. 32 DSGVO (Sicherheit der Verarbeitung) vorgegebenen Grundsätze eingehalten.

4.1. Pseudonymisierung und Datenflüsse

Die Pseudonymisierung erfolgt zweistufig (siehe auch Abb. 3). Auf Seiten der Dateneigner wird ein Pseudonym (SIC) erzeugt, das eine personenbezogene Zusammenführung von Daten unterschiedlicher Dateneigner über Einrichtungsgrenzen ermöglicht. Der SIC besteht aus einer klinikinternen laufenden Nummer und enthält einen Klinik-spezifischen Anteil in Form einer Klinik ID, um Dopplungen zu vermeiden. Anhand der SIC werden dann zufällige, 64-stellige, alphanumerische Pseudonyme zweiter Stufe (PSN) über einen zentralen Pseudonymisierungsdienst in der Vertrauensstelle vermittelt. Dieser erhält außer dem SIC keine weiteren Daten, sondern stellt nur die Verbindung zwischen der ersten und der zweiten Pseudonymisierungsstufe her. Dafür wird die Pseudonymisierungssoftware des Pseudonymisierungsdienstes verwendet (vgl. 2.1.2. Software).

Eine Zuordnungstabelle von Pseudonymen erster Stufe und personenbezogenen Daten wird in der Vertrauensstelle von einem/r Datenmanager/in ohne Zugriff auf den Pseudonymisierungsdienst verwaltet. Mit dem zweiten (Forschungs-)Pseudonym werden die Daten bei den Auswertern geführt, so dass die Re-Identifizierung nur durch die Zusammenarbeit von Dateneigner, Datenmanager/in und Pseudonymisierungsdienst erfolgen könnte. Insbesondere kann durch die Löschung der

Zuordnungstabelle beim Pseudonymisierungsdienst eine spätere Re-Identifizierung wirksam ausgeschlossen werden.

Für den Versand und die Verknüpfung von Fragebögen und medizinischen Daten werden alle Fragebögen mit einer temporären Fragebogen ID (FID) als Barcode versehen. Die FID ist ein sechsstelliges Buchstabenkürzel, das zufällig erzeugt wird. Eine Zuordnungstabelle von FID und SIC wird in der Vertrauensstelle vom/von Datenmanager/in ohne Zugriff auf den Pseudonymisierungsdienst verwaltet.

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

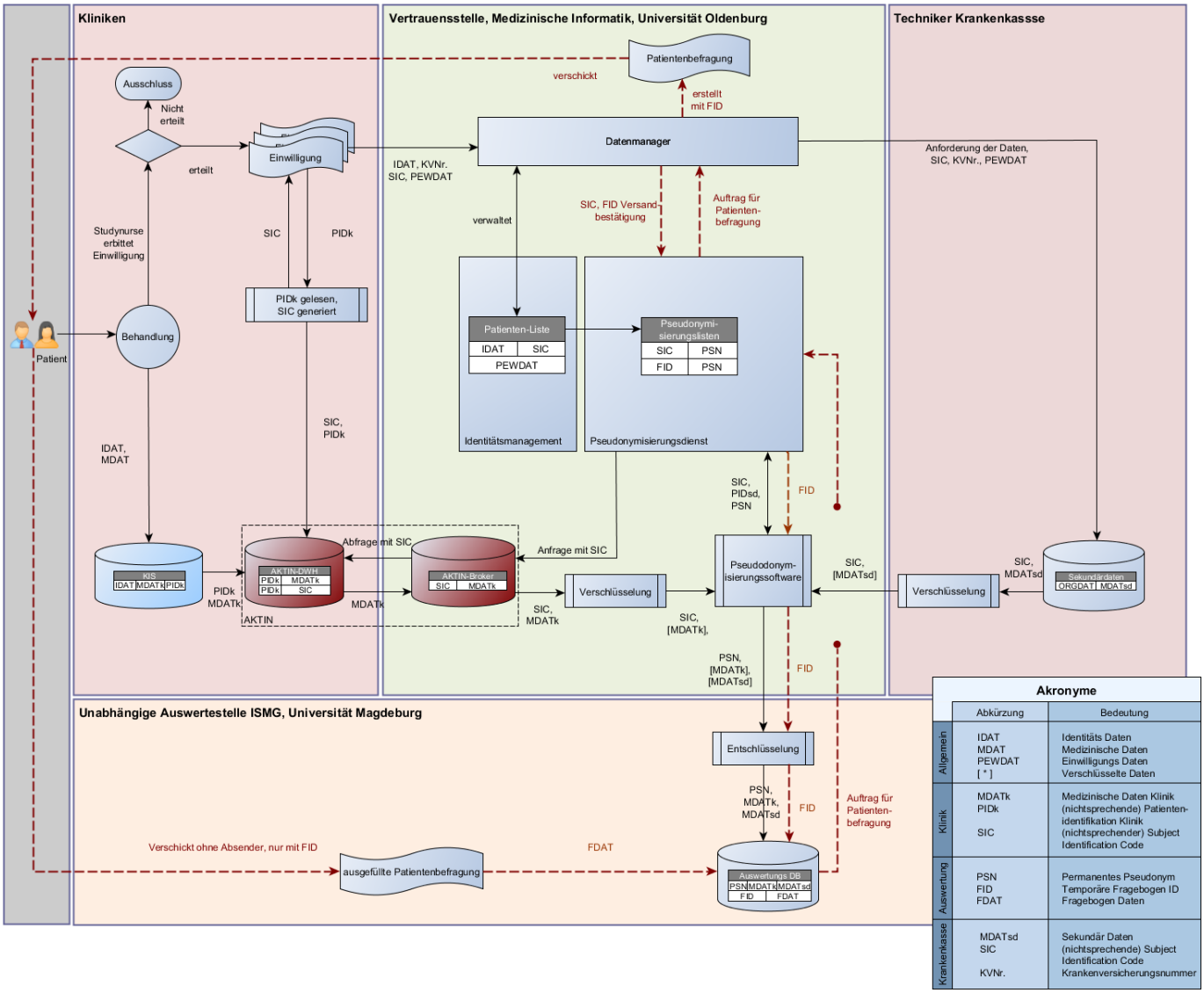

Abbildung 6: Datenfluss auf Basis von AKTIN. Datenfluss von Dateneignern/innen zur Auswertestelle in schwarz, Datenfluss der Patientenbefragung in rot

4.1.1 Sammlung und Weiterleitung der klinischen Primärdaten an die Auswertestelle

Klinische Primärdaten werden in Notaufnahmen erhoben, die als Modellkliniken im AKTIN-Projekt zum Aufbau eines elektronischen Notaufnahmeregisters einen einheitlichen Dokumentationsstandard in den Notaufnahmen etabliert haben. Hinzu kommen weitere Notaufnahmen, die ebenfalls elektronisch dokumentieren. Grundlage für die elektronische Dokumentation ist der Datensatz Notaufnahme der DIVI.

Die klinischen Primärdaten werden in den einzelnen Kliniken gesammelt und mit einem (nichtsprechenden) Subject Identification Code (SIC) versehen, der von einem/er Studienassistenten/in bei der Registrierung der persönlichen Daten bzw. Einwilligungserklärung mit einer Software generiert wird. Über den SIC können so einrichtungsübergreifend Patientendaten zusammengeführt werden, ohne dass der SIC (ohne entsprechendes Zusatzwissen) einer Person zugeordnet werden kann.

In einem zweiten Schritt wird mit Hilfe der Pseudonymisierungssoftware des Pseudonymisierungsdienstes der SIC durch zufällig generierte Pseudonyme zweiter Stufe (PSN) ersetzt (siehe Abb. 5). SICs und identifizierende Daten werden vom Datenmanager/in verwaltet, zuordnende Daten von SIC und PSN werden vom Pseudonymisierungsdienst verwaltet.

Um die klinischen Daten aus dem AKTIN DWH zu extrahieren, wird über den AKTIN Broker eine Anfrage mit SICs gestellt. Vor Anfragen prüft der/die für den Pseudonymisierungsdienst zuständige Mitarbeiter/in etwaige Widersprüche bzw. Löschanfragen durch Betroffene, die sich im Verfahren befinden. Nach einer Anfrage an den AKTIN Broker werden passenden Daten zusammengeführt und über den AKTIN Broker zur Verfügung gestellt. Es werden nur Daten von Patienten/innen geliefert, für die im DWH eine Einwilligung registriert ist (im Falle eines zwischenzeitlichen Widerrufs wird die Einwilligung im DWH gelöscht). Die medizinischen Daten, die nicht für das Record Linkage benötigt werden (d.h. sämtliche Daten außer dem SIC), werden hybrid verschlüsselt (AES und RSA), so dass sie von der Vertrauensstelle 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.

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 Vertrauensstelle über das Ergebnis dieser Eingangsprüfung. Sind die Daten in einem Umfang fehlerhaft, dass eine Nutzung für die Zwecke der Evaluation nicht möglich ist, erfolgt eine Neulieferung der fehlerhaften Tabellen innerhalb von weiteren drei Wochen nach Mitteilung über das Prüfergebnis, 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. Der Gesamtdatensatz liegt allein der Auswertestelle vor.

Nach dem Projektende kann die Zuordnung SIC zu PSN beim Pseudonymisierungsdienst gelöscht werden. Es gibt danach keine (kryptografische) Möglichkeit mehr, das Pseudonym PSN noch einer Person zuzuordnen, da es sich um zufällig generierte IDs handelt, für die auch die Dateneigner keine Zuordnungsvorschrift besitzen. In diesem Sinne sind die PSNs auch nach der Löschung beim Pseudonymisierungsdienst keine Pseudonyme mehr, sondern lediglich zufällige IDs.

Einen Sonderfall stellt die Datensammlung in den Notaufnahmen der Charité Berlin, Standorte Virchow Klinikum und Campus Mitte sowie die Notaufnahme der Gesundheit Nord / Klinikverbund Bremen dar. Alle anderen klinischen Primärdaten werden in Notaufnahmen von Kliniken, die am AKTIN-Projekt teilnehmen, erhoben, d. h. mithilfe der Infrastruktur des AKTIN-Projektes. In den anderen Notaufnahmen werden Daten nicht mit der Infrastruktur des AKTIN-Projekts erhoben, sondern direkt vom Dateneigner an die unabhängige Auswertestelle mittels der Pseudonymisierungssoftware geliefert (vgl. 2.1.2. Software). Das sonstige Vorgehen entspricht dem Vorgehen in den anderen Kliniken.

4.1.2 Sammlung und Weiterleitung der klinischen Sekundärdaten

Entlassdaten der Krankenhäuser in einem Standardformat analog zum §21-Datensatz werden über eine Schnittstelle im AKTIN System zur Verfügung gestellt. Die Daten werden mittels des in Abschnitt 4.1 beschriebenen Pseudonymisierungsprozess verschlüsselt und ohne inhaltliche Manipulation an die Vertrauensstelle geliefert und an die Auswertestelle durchgeleitet. Die verschlüsselten Daten können von der Auswertestelle mit einem nur ihr zugänglichen RSA Schlüssel und einem AES Schlüssel entschlüsselt werden und werden von der Vertrauensstelle nur durchgeleitet. Es erfolgt eine Prüfung und ggf. Bestätigung über die Entgegennahme der Datenlieferung von der Auswertestelle an die Vertrauensstelle (vgl. 4.1.1 Sammlung und Weiterleitung der klinischen Primärdaten an die Auswertestelle).

4.1.3 Sammlung und Weiterleitung der Versicherungsdaten

Der/die Datenmanager/in stellt eine Anfrage für Krankenversichertendaten von Studienteilnehmern/innen (vgl. 1.4.3) an die Techniker Krankenkassen (TK). Dazu werden Krankenversicherungsnummern und Namen sowie Geschlecht zum Zwecke einer Plausibilitätsprüfung), Einwilligungserklärungen und SICs an einen zu diesem Zweck benannte/n Mitarbeiter/in der TK weitergeleitet. Der/die Datenmanager/in prüft dazu zuerst die zu übermittelnden SICs auf etwaige sich im Verfahren befindende Widersprüche bzw. Löschanfragen durch Betroffene und versendet mit der Pseudonymisierungssoftware eine verschlüsselte, jedoch nicht pseudonymisierte Liste mit SIC und Krankenversicherungsnummern sowie Scans der Einwilligungen an die TK.

Die angefragten Sekundärdaten der einzelnen Patienten werden von der TK mittels des in Abschnitt 4.1 beschriebenen Pseudonymisierungsprozess verschlüsselt, mit SIC versehen und dann ohne inhaltliche Manipulation an die Vertrauensstelle gesendet. Von dort werden diese, versehen mit dem permanenten Pseudonym PS, das den SIC ersetzt, an die Auswertestelle durchgeleitet. Die verschlüsselten Daten können von der Auswertestelle mit einem nur ihr zugänglichen RSA Schlüssel und einem AES Schlüssel entschlüsselt werden und von der Vertrauensstelle nur durchgeleitet. Es erfolgt eine Bestätigung, Prüfung und ggf. Beanstandung oder Bestätigung über die Entgegennahme der Datenlieferung von der Auswertestelle an die Vertrauensstelle (vgl. 4.1.1 Sammlung und Weiterleitung der klinischen Primärdaten an die Auswertestelle).

SICs und identifizierende bzw. organisatorische Daten werden vom Datenmanager/in verwaltet, zuordnende Daten von SIC und PSN werden vom Pseudonymisierungsdienst verwaltet. Die TK stellt sicher, dass in den übermittelten Daten keine identifizierenden Daten enthalten sind. Die genaue Ausgestaltung des Vorgehens ist Gegenstand einer noch zu schließenden Kooperationsvereinbarung.

4.1.4 Patientenbefragung

Die Auswertestelle selektiert eine Subpopulation von Patienten/innen für eine Patientenbefragung. Die Auswertestelle erteilt einen Auftrag für die Befragung aller Patienten eines Zeitraumes an eine/n für den Pseudonymisierungsdienst zuständigen Mitarbeiter/in der Vertrauensstelle. Hierfür werden die Pseudonyme PSN der ausgewählten Patienten, die innerhalb des Zeitraumes behandelt wurden, übermittelt. Der zu den einzelnen Pseudonymen gehörige SIC und ein temporärer Fragebogen-Identifikator (FID) werden vom Mitarbeiter/in an den/die Datenmanager/in weitergeleitet. Der/die Datenmanager/in verschickt die Patientenbefragung an den/die Patienten/in und bestätigt dem Pseudonymisierungsdienst den Versand durch Übermittlung des FIDs. Auf diese Weise ist zusätzlich eine Trennung von Pseudonymen und identifizierenden Daten innerhalb der Vertrauensstelle gewährleistet.

Der FID wird zusammen mit dem zugehörigen PSN nach dem Versand des Fragebogens vom Pseudonymisierungsdienst an die Auswertestelle übermittelt (vgl. 4.1.1 Sammlung und Weiterleitung der klinischen Primärdaten an die Auswertestelle).

Die Daten der Patientenbefragung erreichen die Auswertestelle direkt vom Befragten in Papier-basierter Form ohne Absender und re-identifizierende Merkmale, versehen mit einer FID, und werden in der Auswertstelle elektronisch erfasst. Sind zu einer Person mehrere Datenarten verfügbar, werden diese anhand des Pseudonyms miteinander verknüpft (vgl. 1.6.2). Es erfolgt eine Bestätigung über die Entgegennahme des Fragebogens, wenn dieser in der Auswertestelle eintrifft.

Falls ein kontaktierter Patient/in nicht nach 3 Wochen antwortet, kann dieser telefonisch vom Datenmanager/in erneut kontaktiert werden. Dazu wird ein Auftrag von der Auswertestelle an eine/n für den Pseudonymisierungsdienst zuständigen Mitarbeiter/in der Vertrauensstelle gestellt, der diesen bestätigt und an den/die Datenmanager/in weiterleitet.

Eine zusätzliche Patientenbefragung aller einwilligenden Patienten/innen wird vor Ort in ausgewählten Notaufnahmen (u.a. Charité Berlin, Standorte Virchow Klinikum und Campus Mitte) durchgeführt. Die Fragebögen werden zum Zeitpunkt des Aufenthaltes in der Notaufnahme, bei stationär aufgenommenen Patienten innerhalb von 2 bis 3 Tagen nach der Aufnahme verteilt. Die ausgefüllten Fragebögen werden mit einem temporären Fragebogen-Identifikator Klinik (FID_K) versehen, gesammelt und ohne re-identifizierende Merkmale an die unabhängige Auswertestelle verschickt. Es wird eine Zuordnungsliste von SIC und FID_K geführt, die mittels der Pseudonymisierungssoftware pseudonymisiert und verschlüsselt verschickt werden kann.

4.2. 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.

4.2.1 Kommunikation/Vermittlung der IDs mit dem zentralen Pseudonymisierungsdienst

Die seitens der Dateneigner und der Auswertestelle lokal ausführbare Pseudonymisierungssoftware baut eine zertifikatsbasierte verschlüsselte HTTPS-Verbindung (mindestens TLS 1.2) zum Pseudonymisierungsserver der Universität Oldenburg auf. Der gesamte Datenverkehr ist verschlüsselt und eine Kenntnisnahme durch Dritte nach dem Stand der Technik ausgeschlossen.

4.2.2 Übermittlung der Daten zwischen Dateneignern und Auswertestelle

Zusätzlich zur Transportverschlüsselung werden die Daten durch ein asymmetrisches Verfahren derart verschlüsselt (AES und RSA), dass sie nur von der Auswertestelle entschlüsselt werden können. Die technische Infrastruktur dafür stellt die Universität Oldenburg bereit. 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. Diese asymmetrisch verschlüsselten Datenpakete können vom Pseudonymisierungsdienst nicht entschlüsselt werden. Deshalb könnten die Daten über diesen zentralen Webservice geleitet werden, ohne dass die Vertraulichkeit beschädigt wird.

Bei der Entwicklung des Pseudonymisierungsverfahrens werden etablierte und erprobte Verfahren (HMAC, SHA2, Salt/Pepper etc.) eingesetzt. Details zur Implementierung sind der Anlage 9 zu entnehmen.

4.3. 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. Die entsprechenden Maßnahmen für die Auswertestelle können der Anlage 11 entnommen werden.

4.4. Gewährleistung der Integrität

Bei der Erstellung der SICs werden neben der fertig pseudonymisierten Datei auch die originale Datei und eine Zuordnungsliste von Identitätsdaten zur SIC von den Dateneignern lokal aufgehoben, um die korrekte Durchführung zu protokollieren und überprüfbar zu machen.

Bei der Übertragung der Krankenversichertendaten und klinischen 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 Vertrauensstelle 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 Vertrauensstelle 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.

4.5. Gewährleistung der Verfügbarkeit

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

Eine hohe Verfügbarkeit ist darüber hinaus im Projekt ENQuIRE nicht erforderlich. Ein Ausfall des Pseudonymisierungsdienstes für wenige Tage wäre für Datenlieferungen oder Auskunftsverfahren unschädlich.

4.6. Gewährleistung der Belastbarkeit der Systeme

Die Belastbarkeit der Hardware bzw. des Rechenzentrums des Pseudonymisierungsdienstes in Oldenburg 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.

4.7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener 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 1einen 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.

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

Eine jährliche Überprüfung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen ist Bestandteil des Betriebskonzepts. Dabei werden die folgenden Aspekte geprüft und ggf. Maßnahmen beachtet:

- 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

4.9. Schriftliche Dokumentation von sonstigen Maßnahmen

Für die unabhängige Auswertestelle im ISMG der Otto-von-Guericke-Universität Magdeburg gibt es ein eigenes Datensicherheits- und Datenschutzkonzept (Anlage 11). Es beschreibt neben den o.g. speziellen Maßnahmen auch grundsätzliche organisatorische Aspekte.

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

5. Betroffenenrechte

Im Folgenden wird konkretisiert, wie Personen ihre Betroffenenrechte gegenüber dem Projektkonsortium im Rahmen des Projektes geltend machen können.

5.1 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 personenbezogene Daten bei Dritten im Rahmen der Nutzung von Behandlungs- und Sekundärdaten der Kliniken und der TK 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 4).

Darüber hinaus werden die Informationen nach Artikel 14 Abs. 1 und 2 DSGVO für die Öffentlichkeit auf der Webseite des Projekts (http://enquire-projekt.de) zur Einsicht gestellt.

5.2 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 muss über die Vertrauensstelle 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) und werden gebeten, die Anfrage ggf. erneut gegenüber der Vertrauensstelle zu stellen. Da der Auswertestelle keine direkt personenidentifizierbaren Merkmale vorliegen, kann eine Anfrage dort nicht direkt bearbeitet werden und wird deshalb an die Vertrauensstelle 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 Vertrauensstelle gilt folgendes Verfahren:

a) **Anfrage bei der Vertrauensstelle** (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 Vertrauensstelle verschickt.
d) **Beantwortung der Anfrage durch die Vertrauensstelle** (schriftlich)

Logisch wird dabei (insbesondere im Schritt b) bei der Weiterleitung an die Auswertestelle) exakt das in Abschnitt 4.1 beschriebene Verfahren (Vergabe einer TempID bzw. einer Ticket-Nummer für die Kommunikation zwischen Dateneigner und Auswertestelle) eingehalten.

5.3 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 muss über die Vertrauensstelle 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 Vertrauensstelle zu stellen.

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

a) **Anfrage bei der Vertrauensstelle** (schriftlich oder elektronisch)
b) **Datenlieferungen werden gestoppt**

Datenmanager/in und Pseudonymisierungsdienst werden informiert. Datenlieferungen von Daten mit dem jeweiligen SIC 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 (Krankenhäuser) wird der SIC übermittelt.

d) **Löschung und anschließende Bestätigung von der Auswertestelle und den Dateneignern an die Vertrauensstelle**
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 Vertrauensstelle** (schriftlich oder elektronisch)

Logisch wird dabei (insbesondere im Schritt b bei der Weiterleitung an die Auswertestelle) exakt das in Abschnitt 4.1 beschriebene Verfahren (Vergabe einer TempID bzw. einer Ticket-Nummer für die Kommunikation zwischen Dateneigner und Auswertestelle) eingehalten.

5.3.1 Widerrufsfolgen bzw. Folgen von Löschanfragen

Vom Datenmanager wird in der Vertrauensstelle eine Liste von SICs geführt, die einen Widerruf bzw. eine Löschanfrage gestellt haben, bis dieser komplett umgesetzt wurde. Ein Widerruf führt zu einer Löschung des Eintrages des/der Patienten/in in der Patientenliste, des Eintrages des Patienten in den Pseudnoymisierungslisten, der in den AKTIN DWH gespeicherten medizinischen Daten inklusive der mit dem Consent Manager registrierten Einwilligungen und der von der Auswertestelle gesammelten medizinischen Daten. Digitalisierte Kontaktdaten und Krankenversicherungsnummern werden gelöscht. Daten der TK werden nicht gelöscht.

5.4 Verantwortung für die Umsetzung der Betroffenenrechte

Für die Erfüllung der Betroffenenrechte übernehmen die unabhängige Auswertestelle (Institut für Sozialmedizin und Gesundheitsökonomie der Otto-von-Guericke-Universität Magdeburg) und die Vertrauensstelle (Abteilung Medizinische Informatik der Universität Oldenburg) die Verantwortung im Sinne von Art. 26 DSGVO. Die Abteilung Medizinische Informatik der Universität Oldenburg und das ISMG der Otto-von-Guericke-Universität Magdeburg werden vertraglich verpflichtet, entsprechend des hier definierten Prozesses an der Erteilung der Auskunft mitzuwirken. Die Dateneigner verpflichten sich ebenfalls zur Mitwirkung.

6. 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.

7. Anlagen

Anlage 1 Datensatzbeschreibung Datensatz Notfallregister

Anlage 2	Datensatzbeschreibung Entlassdaten
Anlage 3	Datensatzbeschreibung GKV-Routinedaten
Anlage 4	Datensatzbeschreibung Strukturdaten
Anlage 5	Patienteninformation und Einwilligungserklärung
Anlage 6	Ansprechpartner Datenschutz
Anlage 7	Personen mit Umgang mit Daten
Anlage 8	Mitglieder des Data-Use-and-Acess Komitee
Anlage 9	Anforderungsbeschreibung der Pseudonymisierungssoftware
Anlage 10	EK-Stellungnahme Magdeburg
Anlage 11	Datenschutzkonzept des ISMG, Universität Magdeburg (Version 2.0 vom 30.06.2017)
Anlage 12	AKTIN Datenschutzkonzept
Anlage 13	Übersicht der Studienzentren
Anlage 14	Fragebogen Klinik
Anlage 15	Fragebogen retrospektiv
Anlage 16	Votum des Datenschutzbeauftragten des Landes Sachsen-Anhalt
Anlage 17	EK-Stellungnahme Universität Oldenburg

8. Literatur

1 SWART, E., et al. Gute Praxis Sekundärdatenanalyse (GPS): Leitlinien und Empfehlungen. *Das Gesundheitswesen*, 2015, 77. Jg., Nr. 02, S. 120-126.

2 BELLACH, B.-M. Leitlinien und Empfehlungen zur Sicherung von guter Epidemiologischer Praxis (GEP) Eine Mitteilung der Arbeitsgruppe epidemiologische Methoden der deutschen Arbeitsgemeinschaft Epidemiologie (DAE). *Bundesgesundheitsblatt-Gesundheitsforschung-Gesundheitsschutz*, 2000, 43. Jg., Nr. 6, S. 468-475.

3 HELBING, Krister, et al. *Leitfaden zum Datenschutz in medizinischen Forschungsprojekten: Generische Lösungen der TMF 2.0*. MWV, 2017.