Datenmanagement im AKTIN-Notaufnahmeregister

Datenschutzkonzept

Stand: Version 2.1.4.2 vom 22.04.2021

Raphael W. Majeed, Dominik Brammen, Rainer Röhrig, Jonas Bienzeisler

Ansprechpartner

Jonas Bienzeisler
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

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)

AKTIN-Broker: Web Frontend Anwendung für die zentrale Verteilung von Anfragen an die lokalen *DWHs* und die Zusammenführung der Ergebnisse. Wird für das Daten- und Studienmanagement in der AKTIN-Zentrale benutzt und besteht aus *Query Broker* und Data *Aggregator* Komponente.

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 Aggregator: Komponente des AKTIN-Broker zum Sammeln von Abfrageergebnisse. Die zugehörigen Abfragen werden vom *Query Broker* an alle Standorte übermittelt.

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

Standort: Am AKTIN-Notaufnahmeregister teilnehmendes Klinikum.

Query Broker: Komponente des AKTIN-Broker zum Verteilen von Datenabfragen an alle Standorte. Die zugehörigen Ergebnisse werden vom Data *Aggregator* gesammelt.

Trusted Data Analyzing Center (TDAC): 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.

AKTIN IT Team: Arbeitsgruppe, die für den Betrieb und die Entwicklung der technischen Infrastruktur des Notaufnahmeregisters zuständig ist. Ist am Institut für medizinischen Informatik am Uniklinikum RWTH Aachen eingerichtet.

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

Das AKTIN-Notaufnahmeregister ist aus dem AKTIN-Projekt „Verbesserung der Versorgungsforschung in der Akutmedizin in Deutschland durch den Aufbau eines Nationalen Notaufnahmeregisters“ entstanden. Das Projekt wurde mit BMBF-Förderung in Trägerschaft des DLR zwischen 2013 und 2019 durchgeführt. Für die Verstetigung des Projekts und den zukünftigen Betrieb des AKTIN-Notaufnahmeregisters ist ein Verein – AKTIN e.V. - in Gründung. Mitglieder dieses Vereins sind die RWTH Aachen und die Medizinische Fakultät der Otto-von-Guericke-Universität Magdeburg. Das AKTIN-Notaufnahmeregister wird unter Beteiligung des Instituts für Medizinische Informatik am Universitätsklinikum RWTH Aachen und der Universitätsklinik für Unfallchirurgie der Medizinischen Fakultät der Otto-von-Guericke-Universität Magdeburg betrieben.

1.1. Hintergrund

Die Notfallversorgung in Deutschland befindet sich seit einigen Jahren im Umbruch. Außer stichprobenhaften Datenerhebungen im Rahmen von einzelnen Umfragen oder Studien sind keine regelmäßigen und einrichtungsübergreifenden Datensammlungen in der klinischen Notfallmedizin vorhanden. Eine valide und umfassende Datenerhebung zur Anzahl, den Vorstellungsgründen und der Versorgungssituation von Notfallpatient*innen ist zur Bewertung der Maßnahmen allerdings notwendig. Organisatorisch relevante Kennzahlen, die zur Beurteilung der Prozess- und Ergebnisqualität der Notaufnahmen herangezogen werden können, stehen im internationalen Vergleich in Deutschland abgesehen von Einzelfällen nur unzureichend zur Verfügung. Ebenfalls fehlt die Datengrundlage für systematische Analysen unterschiedlicher Versorgungsformen mittels organisatorischer und medizinischer Kennzahlen als Grundlage für den notwendigen Prozess der Organisationsentwicklung in der klinischen Notfallversorgung. Eine sinnvolle Versorgungsforschung im Akut- und Notaufnahmebereich ist ohne diese Datengrundlage kaum möglich.

Im AKTIN-Notaufnahmeregister wird auf einheitliche und standardisierte Weise die digitale Dokumentation aller Notfälle von teilnehmenden Kliniken (sog. *Standorte*) dezentral gesammelt. Die Erhebung der Daten in der Routineversorgung der Patienten*innen unter größtmöglicher Vermeidung von Redundanz ermöglicht die Verwendung von umfangreichen tagesaktuellen und flächendeckenden Datensätzen für Fragen des Qualitätsmanagements, der Versorgungsforschung (Secondary Use), Gesundheitsberichterstattung sowie Surveillance von infektiösen und nicht-infektiösen Krankheitsgeschehen. Die Basis für die Datenerhebung im AKTIN-Notaufnahmeregister ist der von der Sektion Notaufnahmeprotokoll der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin e.V. (DIVI) entwickelte Datensatz Notaufnahme für eine standardisierte, strukturierte Dokumentation in der Notaufnahme.

Um für die verschiedenen Fragestellungen die relevanten Daten zusammenzuführen, wurde für das AKTIN-Notaufnahmeregister eine DSGVO-konforme dezentrale Registerinfrastruktur implementiert. In der klinischen Routine erhobene Daten werden automatisiert in *dezentralen* Data-Warehouses (DWH) der teilnehmenden Standorte gespeichert. Die Daten werden pseudonymisiert und innerhalb des Behandlungskontextes dezentral vorgehalten. Dies geschieht gemäß den Vorschriften des jeweiligen Landes. Zu Zwecken der Qualitätssicherung und Versorgungsforschung sind diese Daten für die Kliniken über eine Benutzeroberfläche verfügbar. Für wissenschaftliche Fragestellung können die gesammelten Daten über einen *zentralen* AKTIN Broker verfügbar gemacht werden – allerdings erst nachdem ein *wissenschaftliches Kontrollgremium* – das *Data Use and Access Committee (DUAC)* – eine entsprechende Anfrage geprüft und genehmigt hat. Die Datenanalyse erfolgt dann im *Trusted Data Analyzing Center* (TDAC) Magdeburg.

1.2. Zweck der Datenverarbeitung

Daten des AKTIN-Notaufnahmeregister werden zu folgenden Zwecken erhoben:

1. Einrichtungsinternes Qualitätsmanagement
2. Einrichtungsübergreifendes Qualitätsmanagement und Benchmarking
3. Einrichtungsübergreifende Versorgungsforschung in der Akutmedizin
4. Gesundheits- und Infektionssurveillance durch Robert Koch-Institut (RKI) und Landesgesundheitsämter
5. Erstellung von Gesundheitsberichten
6. Datensammlung und –export an spezialisierte Register im Rahmen bereits zu erstellender Verträge

Ziel ist die Erreichung einer möglichst hochwertigen Qualität des Qualitätsmanagements, der Forschung sowie der Gesundheits- und Infektionssurveillance in der Akutmedizin und eine Verarbeitung dieser Daten in voller Übereinstimmung mit den in Deutschland bzw. der EU gültigen Rechtsnormen und Empfehlungen.

1.3. Umfang der Datenverarbeitung

Im Rahmen des AKTIN-Notaufnahmeregisters werden Daten kontinuierlich prospektiv gesammelt. Dies erfolgt in den teilnehmenden Standorten mit Beginn der Teilnahme am Register, in Einzelfällen können Daten auch rückwirkend in die lokalen DWH-Systeme übermittelt werden. Die Daten werden in Notaufnahmen erhoben, die einen einheitlichen Dokumentationsstandard etabliert haben. Die teilnehmenden Krankenhäuser speichern die ausgewählten Daten zu jedem/r Patienten*in der Notaufnahme in einem lokalen DWH. Dieses ist Teil der Infrastruktur des AKTIN-Notaufnahmeregisters, wird aber von den Standorten selbst administriert. Die Daten und der Server, auf dem diese sich befinden, sind im Besitz bzw. Verantwortungsbereich der Standorte. Die Daten werden vom jeweiligen Standort eigenständig erhoben. Für wissenschaftliche Fragestellungen können die Daten über den AKTIN Broker zentral abgefragt werden (siehe Anlage 1 – Studienzentren).

Ein Export der Daten erfolgt grundsätzlich anonymisiert. Es werden bei den Abfragen an die Standorte die Prinzipien der Datensparsamkeit angewendet. Die Datenanalyse erfolgt im TDAC. Dort wird durch technische und organisatorische Maßnahmen sichergestellt, dass die Daten nicht mit anderen Datenquellen verknüpft werden können. An Dritte, nicht an dem Projekt beteiligte Partner, erfolgt ausschließlich einen Übermittlung von aggregierten Daten. Ausnahmen, z.B. im Rahmen der Gesundheitsberichterstattung oder auf Basis von Verträgen sind nach Prüfung durch das DUAC möglich. Jede Datenabfrage bedarf eines Studienprotokolls, welches vom DUAC auf die Einhaltung von Wissenschaftlichkeit, ethischen Prinzipien und des Datenschutzkonzeptes einschließlich der Datensparsamkeit geprüft wird. Für den technischen Betrieb, zum Zwecke der Qualitätssicherung und für den technischen Support werden außerdem Daten vom *AKTIN IT Team* am Institut für Medizinische Informatik am Universitätsklinikum RWTH Aachen verarbeitet. Art und Umfang der Datenerhebung hängen vom Umfang des technischen Supports ab. Es werden – soweit möglich - anonymisierte Daten verarbeitet, die nach Abschluss des technischen Supports gelöscht werden. Sollte im Rahmen des technischen Supports der Zugriff auf personenbezogene Daten erforderlich werden, so ist eine gesonderte Vereinbarung über eine Auftragsverarbeitung zwischen der Uniklinik RWTH Aachen und dem jeweiligen Standort zu schließen.

Jede darüber (und über dieses Datenschutzkonzept) hinausgehende Datenverarbeitung bedarf einer eigenständigen Rechtsgrundlage und eines adäquaten Datenschutzkonzepts sowie der Zustimmung des DUAC.

1.3.1. Datenerhebung gemäß Leitfaden zum Datenschutz der TMF

Die Datenerhebung bzw. die organisatorische Trennung von identifizierenden und medizinischen Daten folgt den Empfehlungen der Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF). Es erfolgt eine Datenerhebung im Sinne des Basismodells (mit dezentralen Patientenlisten) des Leitfadens zum Datenschutz in medizinischen Forschungsprojekten – generische Lösungen der TMF 2.0 [1]. Die Daten werden jeweils vor Ort pseudonymisiert in ein lokales Data-Warehouse überführt, welches in der Datenhoheit der behandelnden Einrichtung, der Notaufnahme des jeweiligen Krankenhauses, steht. Für Auswertungen werden die Daten über den AKTIN Broker in grundsätzlich anonymisierter Form verfügbar gemacht.

Eine Abweichung vom TMF-Datenschutzleitfaden liegt im Verzicht auf eine explizite Einwilligung der Betroffenen, die oft gar nicht einwilligungsfähig sind. Der vollständige Einschluss aller behandelten Patienten*innen ist aber insbesondere wegen der Teilnahme an der Infektionssurveillance erforderlich.

1.4. Organisationsstruktur und Verantwortlichkeiten

Das AKTIN-Notaufnahmeregister wird vom AKTIN e.V. in Zusammenarbeit mit dem Institut für Medizinische Informatik am Universitätsklinikum RWTH Aachen (IMI) und der Universitätsklinik für Unfallchirurgie der Otto-von-Guericke-Universität Magdeburg (KCHU) betrieben (siehe Anlage 2 – Ansprechpartner Datenschutz).

1.4.1. AKTIN Geschäftsstelle

Die AKTIN Geschäftsstelle wird von der KCHU betrieben. Die AKTIN Geschäftsstelle betreut die (nicht-technischen) organisatorischen Vorgänge im AKTIN-Notaufnahmeregister, wie z.B. der Freigabeprozess für Forschungsanfragen.

1.4.2. Studienzentren

An der Datenerfassung im Rahmen des AKTIN-Notaufnahmeregisters beteiligen sich die Notaufnahmen von Kliniken, die ein AKTIN DWH betreiben – sog. teilnehmende *Standorte*. Ein Standort mit mehreren Notaufnahmen kann mehrere DWH einschließen. Vor der Zusammenarbeit mit Standorten werden Verträge geschlossen. Das lokale Datenmanagement wird von Standortkoordinatoren verantwortet. Sie sind für die Umsetzung und Einhaltung aller ethischen, rechtlichen, vertraglichen und organisatorischen Vorgaben zum Datenmanagement verantwortlich (siehe Anlage 1 - Studienzentren).

1.4.3. AKTIN IT Team

Für den Betrieb der technischen Infrastruktur des AKTIN-Notaufnahmeregisters, die technische Realisierung von Datenabfragen über den AKTIN Broker (gemäß den Vorgaben und Weisungen des DUAC) und den IT-Support der Standorte ist die AKTIN IT Team am IMI verantwortlich.

1.4.4. Trusted Data Analyzing Center

Die KCHU betreibt das *Trusted Data Analyzing* Center (TDAC). Es werden die von den datenbereitstellenden Projektpartnern zur Verfügung gestellten Daten verarbeitet (gemäß Zweck der Datenverarbeitung) und ggf. weitergeleitet. Das TDAC führt die Analysen durch und stellt durch technische und organisatorische Maßnahmen sicher, dass die Daten nicht mit anderen Datenquellen verknüpft werden können. An Dritte, nicht an dem Projekt beteiligte Partner, können aggregierten Daten in Rahmen von Forschungsanfragen übermittelt werden. Ausnahmen, z.B. im Rahmen der Gesundheitsberichterstattung oder auf Basis von Verträgen sind nach Prüfung durch das DUAC möglich.

1.4.5. Data Use and Access Committee

Die Bereitstellung eines Datensatzes kann bei einem unabhängigen wissenschaftlichen Kontrollgremium – dem *Data Use and Access Committee (*DUAC) – von Wissenschaftlern beantragt werden. Eine solche Anfrage erfolgt für eine konkrete wissenschaftliche Fragestellung. Das Gremium prüft den Antrag in Hinblick ethischer und datenschutzrechtlicher Gesichtspunkte. Bei einer positiven Bewertung wird dann der jeweilige Datenauszug entsprechend der Vorgaben des Review Boards erstellt und zum Zwecke der Auswertung im Hinblick der Fragestellung weitergeleitet. Das genaue Vorgehen ist in einer Geschäftsordnung festgelegt. Es werden unter Wahrung des Datenschutzes nur die erforderlichen Daten abgefragt und ausgewertet.

1.4.6. Externe Kooperationen

Externe Kooperationen sind vorgesehen. Von externen Partnern kann eine *Auswertestelle* eingerichtet werden. Eine solche Kooperation muss jeweils vertraglich geregelt und vom DUAC genehmigt werden. Eine Datenweitergabe an Kooperationspartner erfolgt analog zu der Datenweitergabe an Wissenschaftler wie in Abschnitt 2.2.6. angegeben.

1.5. Anfallende Daten und verbundene Risiken

Datenstandard ist der Datensatz Notaufnahme in der jeweils gültigen Version, aktuell V2015.1 (Stand 06/2020). Die zu erfassenden Daten wurden von der Sektion Notaufnahmeprotokoll der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin e.V. (DIVI) erarbeitet [2]. Die DIVI ist eine Dachorganisation der in Deutschland an der Intensiv- und Notfallmedizin beteiligten 18 Fachgesellschaften mit individueller Personenmitgliedschaft.

Darüber hinaus können anlass- oder projektbezogen stationäre Behandlungsdaten (einzelne Items aus dem Datensatz gem. § 21 KHEntgG, siehe Anlage 8 – Datensatz Abrechnungsdaten) *optional* zur Verfügung gestellt werden. Ein geeigneter Anlass kann durch das DUAC festgestellt werden. Jeder Standort entscheidet dann eigenständig über den Inhalt und Umfang der verarbeiteten stationären Behandlungsdaten. Insbesondere können von den Standorten (ohne Begründung) auch nur bestimmte Items zur Verfügung gestellt werden, es gelten allerdings Vorgaben für Struktur und einen minimalen Datensatz (vgl. Anlage 8 – Datensatz Abrechnungsdaten). Die Daten können über eine Benutzerschnittstelle im AKTIN-DWH-Manager in das lokale AKTIN DWH importiert werden (vgl. Kapitel 2.2). Die Daten werden dann in gleicher Weise wie die anfallenden Daten des Datensatz Notaufnahme verarbeitet.

1.5.1. Datenkategorien

Bei den Daten 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 Datensparsamkeit und für die Zwecke zur Datenverarbeitung (Zweck der Datenverarbeitung) nötig. Die Nutzung der Daten ist ausschließlich gemäß dieser Zwecke vorgesehen. Eine andere Nutzung dieser Daten als zu den beschriebenen Zwecken findet nicht statt. Es ist gewährleistet, dass die Bestimmungen des Datenschutzes eingehalten und ausschließlich die Daten ausgewertet werden, die für den jeweiligen Zweck 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. Insbesondere für Daten aus Notaufnahmen gilt ein sehr hoher Schutzbedarf. Für alle Daten die erhoben werden gelten Maßnahmen entsprechend des höchsten Schutzbedarfs. Es wird technisch und organisatorisch (mittels des DUAC) sichergestellt, dass identifizierende, medizinische Daten nicht außerhalb der Notaufnahme, in dem der/die Patient*in persönlich bekannt ist, zusammengeführt werden können.

Die genauen technischen und organisatorische Maßnahmen – passend zum Schutzbedarf bzw. der Schutzklassen – finden sich in Kapitel Technische und organisatorische Maßnahmen. Re-Identifizierungsmöglichkeiten

Die Daten liegen für die Auswertung in anonymisierter Form i. S. d. Artikel 4 Nr. 5 DSGVO vor.

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

- Patienten*innen
- Klinikmitarbeiter*innen

1.5.3. Restrisiko

Auch wenn durch technische und organisatorische Maßnahmen (Kapitel 2) sichergestellt wird, dass identifizierende und medizinische Daten nicht zusammengeführt werden können, so kann dies nicht vollständig ausgeschlossen werden. Dem TDAC könnte durch unzulängliche Anonymisierung personenbeziehbare Daten zugespielt werden. Dem IT-Team könnte es im Rahmen des IT-Support möglich sein Einwegpseudonyme aus verschiedenen Einrichtungen einzusehen und anschließend durch Brute Force Verfahren wie Probeverschlüsselung die Pseudonyme aufzulösen. Der IT-Support hätte dann Zugriff auf potenziell personenbeziehbare Fall- oder Patientennummern. Eine Zusammenführung über mehrere Standorte ist nicht möglich. Den Mitarbeitern und Mitarbeiterinnen des TDAC bzw. IT-Team wird aufgrund dieses Restrisikos in Form von Dienstanweisungen oder Verschwiegenheitserklärungen verboten, die erhobenen Daten einer betroffenen Person zuzuordnen.

1.6. Ethische und regulatorische Anforderungen

Die Forschung am Menschen und die Verarbeitung von zugehörigen Daten ist notwendig für die Entwicklung und Sicherheit der Medizin und ist damit von einem hohen gesellschaftlichen Interesse. Dabei sind die Interessen der Patienten*innen jederzeit zu wahren.

Zu jedem Zeitpunkt werden die Datenschutzbestimmungen der Europäischen Union (EU), des Bundes und des jeweiligen 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 AKTIN-Notaufnahmeregister 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. Bei schwerwiegenden Störungen des Verarbeitungslaufs, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten werden betroffene Personen, die Dateneigner sowie die Aufsichtsbehörde unverzüglich vom AKTIN-Notaufnahmeregister durch die AKTIN Geschäftsstelle informiert. Betroffene Personen, die nicht kontaktiert werden können, werden über eine Website informiert (http://www.aktin.org).

Es werden bzgl. der wissenschaftlichen Qualität die Richtlinien zur Sicherung der guten wissenschaftlichen Praxis der Deutschen Forschungsgemeinschaft eingehalten [3]. Es gelten die WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects [4].

Die Infrastruktur des AKTIN-Notaufnahmeregisters wurde von der Ethikkommission der Medizinischen Fakultät der Universität Magdeburg positiv begutachtet (siehe Anlage 5 - Ethikvotum, Votum 160/15). Das Register ist im Deutschen Register Klinischer Studien registriert (Studien-ID: DRKS00009805).

1.7. Rechtsgrundlagen der Datenverarbeitung

1.7.1. Präambel zur rechtlichen Einschätzung der AKTIN-Infrastruktur

Die AKTIN-Infrastruktur stellt einen Sonderfall in der Registerlandschaft dar. Die Daten werden pseudonymisiert innerhalb der Kliniken im Behandlungskontext gemäß den Vorschriften des Landes dezentral verarbeitet und vorgehalten. Alle Daten verbleiben innerhalb der patientenführenden Abteilung (i. d. R. Notaufnahme). Die Verantwortung für die Durchführung der Datenabfragen in den DWH-Systemen liegt bei den Standorten. Diese erhalten durch die Technik Einsicht in die Abfragen sowie in die zu übermittelnden Daten und können prüfen, ob Abfragen und zu übermittelnde Daten den für den Standort gültigen Gesetzen, sowie internen und externen Regelungen genügen. Erst nach der Freigabe durch die Klinik werden die Daten zentral zusammengeführt.

Die Datenübermittlung an Dritte, in diesem Fall die zentrale Infrastruktur des AKTIN-Notaufnahmeregisters erfolgt mit anonymisierten Teildatensätzen, wobei die k-Anonymität der Daten in der mehrstufigen Verarbeitungskette steigt. Damit wird sichergestellt, dass bei jedem Schritt in der Verarbeitungskette eine Re-Identifizierung der betroffenen Personen ausgeschlossen wird. Spätestens ab dem Punkt der vollständigen Anonymisierung der Daten fällt die Verarbeitung nicht mehr unter die Datenschutzgesetzgebung. Es wird bei Datenabfragen im Rahmen von wissenschaftlichen Fragestellungen angestrebt, diesen Zustand möglichst früh in der Verarbeitungskette zu erreichen. Damit fällt die zentrale Datenverarbeitung bei vielen Forschungsvorhaben nicht unter die Datenschutzgesetzgebung. Wenn noch nicht vollständig anonymisierte Datensätze an die zentrale AKTIN-Infrastruktur übermittelt werden, gilt die im folgenden Absatz beschriebene Rechtsgrundlage für die Datenverarbeitung.

1.7.2. Rechtgrundlage für die Datenverarbeitung ohne Einwilligung.

Die Entscheidung über die Zwecke und Mittel der Verarbeitung trifft AKTIN e. V. . Die medizinischen Daten werden von den datenbereitstellenden Projektpartnern erhoben (siehe Studienzentren). Datenanfragen werden nach einer Begutachtung durch das DUAC an die Standorte übermittelt, die eigenständig über die Teilnahme und Datenbereitstellung entscheiden. Die teilnehmenden Standorte bestimmen selbst, welche Mitarbeiter*innen – sog. *Standortkoordinatoren*innen* - die entsprechenden Befugnisse haben. Damit liegt die Verantwortung für die Entscheidung der Datennutzung bei den Standorten als Dateneignern (vgl. DSGVO Art. 6 (4)), hingegen die Verantwortung für die technische Durchführung, Datenzusammenführung und Datenanalyse bei dem AKTIN-Notaufnahmeregister.

Rechtsgrundlagen für die Verarbeitung der Daten sind:

- EU-DSGVO (EU-V 2017/679)
- Bundesdatenschutzgesetz
- Strafgesetzbuch (StGB)
- Für die Verarbeitung in den Krankenhäusern ist zusätzlich die jeweilige Landesgesetzgebung zu berücksichtigen.

Grundsätzlich fällt die Datenverarbeitung von Gesundheitsdaten unter DSGVO Art. 9 (Verarbeitung besonderer Kategorien personenbezogener Daten) bzw. §22 BDSG. Die Rechtmäßigkeit der Datenverarbeitung von Daten, die nicht zur besonderen Kategorie personenbezogener Daten gehören, ist über DSGVO Art. 6 (1) lit.e. begründet.

> „Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“ (DSGVO Art. 6 (1) lit.e).

Die Bereitstellung solcher Daten für die einrichtungsübergreifende Qualitätssicherung in der Notfallversorgung (Benchmarking) und zur Beantwortung wissenschaftlicher

Forschungsfragestellungen zur Notfallversorgung oder im Rahmen der Gesundheitsberichterstattung ist im öffentlichen Interesse.

Darüber hinaus können Daten nach DSGVO Art. 6 (1) lit. f. bereitgestellt werden;

> *„die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt“* (DSGVO Art. 6 (1) lit. f).

Die Verarbeitung ist rechtmäßig, da die Datenbereitstellung aufgrund eines berechtigten (wissenschaftlichen) Interesses der beteiligten Kooperationspartner oder eines Dritten erfolgt. Ein wirksamer Schutz der Identität und der Interessen der betroffenen Personen / Patient*innen wird zu jeder Zeit gewährleistet und durch das DUAC im Einzelfall geprüft.

Die Rechtfertigung der Datenverarbeitung für wissenschaftliche Zwecke ist auch in DSGVO Art. 89 und §27 BDSG begründet und damit ebenfalls als öffentliches Interesse anzusehen. Insbesondere handelt es sich dabei um

> *„Die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken unterliegt geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung. Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen. In allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt“ DSGVO Art. 89 (1).*

Es gilt

> *„Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor“* (BDSG § 27).

Die Datenverarbeitung von Gesundheitsdaten im AKTIN Notaufnahmeregister fällt unter DSGVO Art. 9 (Verarbeitung besonderer Kategorien personenbezogener Daten) bzw. §22 BDSG und damit unter eine besondere Schutzwürdigkeit. Eine informierte Einwilligung als Rechtsgrundlage (DSGVO Art. 6 (1) lit. a bzw. Art. 9(2) lit. a) ist in dem Vorhaben nicht möglich. Zum einen wäre eine informierte Einwilligung in einer Notaufnahmesituation nicht möglich, zum anderen würde ein sogenannter Selektions-Bias hinsichtlich der Einwilligungsfähigkeit die Studienergebnisse verfälschen. DSGVO Art. 89, DSGVO Art. 9(2) lit. i und BDSG §22 (1) sehen abweichend von DSGVO Art 9 (1) eine Rechtfertigung der Verarbeitung von Daten zu wissenschaftlichen Zwecken vor, soweit diese für den Zweck der Forschung, respektive die Beantwortung der Forschungsfrage erforderlich sind. Insbesondere wenn diese

> *„c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Absatz 2 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten, oder*
>
> *d) aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist“* (BDSG §22 (1)).

Dies geschieht jeweils unter der Bedingung, dass angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person nach §22 (2) S. 2 bzw. DSGVO Art. 9(2) lit. i erfolgen. Diese Maßnahmen sind:

- Pseudonymisierte Speicherung der gesamten Daten innerhalb des Gesundheitseinrichtung bzw. Notaufnahme im Behandlungskontext.
- Zweistufige Datenübermittlung nach Maßgabe der Datensparsamkeit: Es werden nur die (anonymen) Daten an das TDAC übermittelt, die für die Beantwortung der Fragestellung erforderlich sind. Dort werden die Daten in einem geschützten Bereich verarbeitet und erst nach Sicherstellung einer hinreichenden k-Anonymität an Dritte übermittelt.
- Einzelfallüberprüfung der Datenanfragen durch ein wissenschaftliches Kontrollgremium (DUAC) und teilnehmenden Standorten in Verbindung mit den genannten Öffnungsklauseln sowie gemäß DSGVO Art. 6 (4).
- Technische Maßnahmen (s.u.) zur Datensicherheit

Für die beteiligten Notaufnahmen bzw. datenbereitstellende Krankenhäuser gelten die lokalen Gesetze in Verbindung mit den genannten Öffnungsklauseln einzelfallabhängig von der jeweiligen Datenabfrage. Es gelten die Landeskrankenhaus- bzw. Landesdatenschutzgesetze der jeweiligen Bundesländer, in denen die Daten erhoben werden.

Neben der Datenschutzgesetzgebung gilt die ärztliche Schweigepflicht (§203 StGB). Da ausschließlich strukturierte und anonymisierte Daten nach außen übermittelt werden, ist nicht davon auszugehen, dass eine Geheimnisoffenbarung entgegen §203 (1) StGB stattfindet.

Informationen nach DSGVO Art. 14 werden auf der Webseite http://www.aktin.org veröffentlicht und von den Standorten für die Patienten*innen bereitgestellt.

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 Einweg-pseudonymisiert unter der Datenhoheit der behandelnden Einrichtung, d.h. der Notaufnahme des jeweiligen Krankenhauses, gesammelt. Für Datenanfragen zu Forschungszwecken gelten die Anweisungen des DUAC, welches datenschutzrechtliche und ethische Standards garantiert. Es verlassen nur anonymisierte Daten die datenbereitstellenden Einrichtungen, nachdem diese einer Übermittlung zugestimmt haben.

Die technisch-organisatorischen Maßnahmen bei den datenbereitstellenden Projektpartnern selbst sind nicht Bestandteil dieses Datenschutzkonzepts, da der Schutzbedarf dort unabhängig vom Projekt besteht und bereits entsprechend umgesetzt ist (siehe Anlage 1 - Studienzentren). Insbesondere handelt es sich dabei primär um Datenverarbeitungen mit anderen Zwecken und Rechtsgrundlagen außerhalb der Regelungskompetenz des AKTIN-Notaufnahmeregisters.

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.

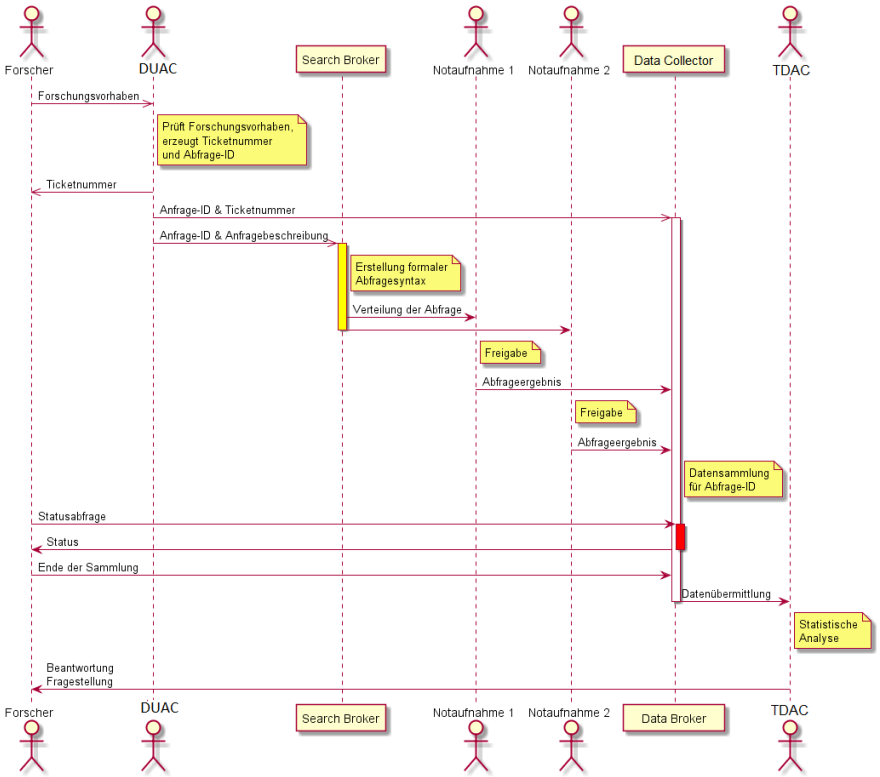

Abbildung 1: Prozessübersicht gemäß dem Rollen- und Rechtekonzept

2.1.1. Data Use and Access Committee (DUAC)

Das DUAC kontrolliert Forschungsanfragen, bevor diese an die Standorte übermittelt werden. Diese Rolle ist weniger technisch als eher wissenschaftlicher Natur. Dem DUAC gehört mindestens ein Mitarbeiter des Trusted Data Analyzing Center an.

2.1.2. Search Broker (SB)

Die Search Broker setzen die vom DUAC genehmigten Anfragen in Datenbankabfragen und standardisierte Terminologie um und stellt diese im Query Broker ein. Sie übermitteln die Abfragen anschließend an die Standortkoordinatoren mittels AKTIN Broker. Ein Search Broker ist Teil des IT-Teams am Institut für Medizinische Informatik am Universitätsklinikum RWTH Aachen.

2.1.3. Standortkoordinator*in

Die Standortkoordinatoren*innen haben die Befugnis das lokale Datenmanagement in einem Standort zu verantworten. Standortkoordinatoren*innen werden vom Standort bestimmt. Ggf. kann die Rolle von einem oder mehreren Personen gemeinsam ausgefüllt werden. Sie sind für die Umsetzung und Einhaltung aller ethischen, rechtlichen, vertraglichen und organisatorischen Vorgaben zum Datenmanagement verantwortlich. Sie verantworten somit eine lokale Prüfung jeder Abfrage, sowie die Festsetzung und Prüfung der Einhaltung der geltenden Kriterien der Anonymität durch die eigene Institution. Der/die Standortkoordinatoren*innen müssen einer Forschungsabfrage zustimmen, bevor sie auf den Daten des entsprechenden Standorts durchgeführt wird. Sie können die Ergebnistabellen einsehen bevor diese verschickt werden.

2.1.4. Data Collector (DC)

Nur ein Data Collector hat die Berechtigung, im Data Aggregator gesammelte anonyme Rohdaten bzw. Abfrageergebnisse über den AKTIN Broker abzurufen. Der Data Collector ist zuständig für die Weiterleitung der Abfrageergebnisse der Standorte, die im Data Aggregator gesammelt werden, an das TDAC. Der/die Forscher*in kann beim Data Collector den Stand der Rückmeldungen erfragen und das Ende der Datenerhebung bzw. –sammlung festlegen. Außerdem können die Ergebnisse von technischen Anfragen an das AKTIN IT Team weitergeleitet werden.

2.1.5. Trusted Data Analyzing Center (TDAC)

Die Aufgabe der Mitarbeiter des TDAC ist die Prüfung, Aufbereitung, Aggregation und Auswertung der gesammelten Anfrageergebnisse. Die Mitarbeiter des TDAC erhalten die gesammelten anonymen Rohdaten bzw. Abfrageergebnisse und werten diese aus. Das TDAC stellt sicher, dass im Falle einer Weitergabe von Daten an den/die Forscher*in die Kriterien der k-Anonymisierung und l-Diversität eingehalten werden.

2.1.6. Datenschutzbeauftragter (DS)

Der AKTIN e.V. ernennt eine/n Datenschutzbeauftragte/n, der/die in seiner Arbeit unabhängig von allen anderen Leitungsgremien mit Einfluss auf Datenmanagementstrukturen ist. Der/die Datenschutzbeauftrage ist ein unabhängiges Kontrollorgan für alle datenverarbeitenden Stellen wie auch für An- und Abfragen und das DWH.

2.1.7. Forscher*in

Der/die Forscher*in kann über die AKTIN Geschäftsstelle Forschungsanfragen anmelden und so Datenauszüge beantragen. Alle Anfragen werden protokolliert.

2.1.8. Auswertestelle

Im besonderen Fällen (z.B. bei periodischen Abfragen im Rahmen von Infektionssurveillance) kann auch eine Weitergabe von anonymisierten Rohdaten an Forscher*innen eingerichtet werden, wenn dies zuvor vom DUAC genehmigt wurde und entweder die hinreichende Anonymisierung grundsätzlich bereits anhand der Abfrage gegeben ist (z.B. Struktur der Daten, automatisierte Anonymisierung) oder eine andere Rechtsgrundlage (beispielsweise aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren im Falle einer Pandemie nach § 22 Abs. 1 Nr. 1 lit. c BDSG in Verbindung mit Art. 9 Abs. 2 lit. g DSGVO) für die Datenübertragung vorliegt. Von den Forscher*innen wird dann eine

Auswertestelle eingerichtet. Dies ist entsprechend in der Anfrage an das DUAC zu beschreiben; ggf. muss ein zusätzliches Datenschutzkonzept erstellt werden.

2.1.9. Rollenkonflikte

Alle Rollen können in einigen Fällen geteilt werden. Die Rolle des Datenschützers darf an einem teilnehmenden Standort ausgeübt werden, nicht jedoch in Kombination mit anderen datenverarbeitenden Stellen, da diese ja überwacht werden sollen. Der Datenschutzbeauftragte muss unabhängig sein - er kann einem Standort zugehörig sein, darf aber keinen operativen Auftrag in der Datenverarbeitung haben.

Tabelle 1 Rollen die geteilt werden können: Standortkoordinator (Standort) Datenschützer (DS), Data Use and Access Committee (DUAC), Search Broker (SB), Data Collector (DC), Trusted Data Analyzing Center (TDAC).

	Standort	Datenschutz	DUAC	Search Broker	Data Collector
Standort					
Datenschutz	Ja				
DUAC	Ja	Nein			
Search Broker	Ja	Nein	Ja		
Data Collector	Nein	Nein	Ja	Nein	
TDAC	Nein	Nein	Ja	Nein	Ja

2.2. Datenflüsse und IT Infrastruktur

Die Infrastruktur des AKTIN-Notaufnahmeregisters besteht aus einer dezentralen Datenerhebung in den Notaufnahmen, die über eine zentrale IT Komponente – dem AKTIN Broker – verfügbar gemacht werden können.

2.2.1. Dezentrale Datenerhebung in der Notaufnahme

Die Notaufnahmen der teilnehmenden Krankenhäuser verwenden elektronische Systeme zur Erfassung der medizinischen Routinedokumentation gemäß Datensatz Notaufnahme. Zusätzlich betreibt jedes Krankenhaus eine einheitliche DWH-Software auf einem eigenen dedizierten Server. Die DWH-Software wird vom AKTIN-Notaufnahmeregister bereitgestellt. Mittels einer Exportschnittstelle werden die entsprechenden Daten aus dem Informationssystem der Notaufnahme digital exportiert und als standardisierte HL7-CDA-Dokumente abgelegt. Diese CDA-Dokumente werden anschließend auf den DWH-Server übertragen. Diese Dokumente können über zwei mögliche standardisierte Übertragungswege importiert werden: Zum einen über einen HL7-FHIR REST Endpunkt und zum anderen über eine IHE XDS.b Dokumenten-Empfänger SOAP-API. Nach Entgegenahme erfolgt eine automatisierte syntaktische und inhaltliche Validierung des gesendeten Inhalts des Notaufnahmeprotokolls (HL7-CDA) über umfangreiche Schematron-Regeln.

Das DWH enthält keine unmittelbar Patienten*innen-identifizierenden Merkmale (wie z.B. Pat-ID, Name, Vorname), jedoch eine Nummer, die mit einem kryptographischen Einwegverfahren (Hash)

standortspezifisch[1] erzeugt wird. Dieses Pseudonym kann nicht dazu verwendet werden, um auf die Identität des/der Patienten*in zu schließen, erlaubt es jedoch Folgedaten den passenden Datensätzen zuzuordnen. Die lokalen Mitarbeiter haben keinen direkten Zugriff auf den Einweg-Hash. Nur der Datenbank Administrator kann dieses Pseudonym technisch bedingt einsehen. Zugriff auf die Daten haben nur berechtigte Mitarbeiter*innen der patientenführenden Abteilung über die Benutzeroberfläche des DWH.

Zusätzlich zu Notaufnahmedaten haben teilnehmende Krankenhäuser die Möglichkeit, weitere Daten aus dem stationären Aufenthalt (wie z.B. Entlassungsgrund, Entlassungszeit, Hauptdiagnose, Nebendiagnosen, Prozeduren, Operationstag, Beatmungsstunden) zu ihren Notaufnahmepatienten*innen in das lokale Datawarehouse zu integrieren. Die Zuordnung zu den vorhandenen Daten erfolgt über das kryptographische Einwegverfahren wie oben beschrieben. Derartige Daten können anschließend auch für Berichte, Benchmarks und zentrale Abfragen verwendet werden. Auf Anfrage bzw. im Auftrag des Krankenhauses kann die DWH-Software von dem IT-Support des AKTIN-Notaufnahmeregisters gewartet werden.

Das lokale Data Warehouse kann von den lokalen Mitarbeitern für eigene Fragestellungen genutzt werden. Der Zugriff erfolgt authentifiziert personenbezogen über die Benutzeroberfläche des DWH. Die Mitarbeiter können Abfragen über alle gespeicherten Parameter durchführen, haben jedoch keinen Zugriff auf den generierten Einweg-Hash.

2.2.2. Zentrale Datenerhebung

Alle Anfragen für Datenauszüge für Forschungsvorhaben und Fragestellungen (z.B. für Forschung, Qualitätssicherung) werden durch ein Review-Verfahren durch das DUAC geprüft und anschließend an die Standorte weitergeleitet. Der *Query Broker* ist die Kommunikationsschnittstelle und verteilt die Anfragen für Datenauszüge als SQL-Query an alle Standorte. In jeder Klinik muss der Fragestellung bzw. der SQL-Query von den Standortkoordinatoren*innen explizit zugestimmt werden bevor eine Abfrage durchgeführt und Daten exportiert werden. Die Exporte der Standorte werden an einer zentralen, unabhängigen Stelle (dem *Data Aggregator*) gesammelt und können dann vom TDAC abgerufen werden. Dort erfolgen Aufbereitung und Auswertung sowie Übermittlung der aggregierten Ergebnisse bzw. vergröberten Datensätze nach Prüfung einer vorab festgelegten ausreichenden Anonymität und Diversität an den Forscher*in. Zusätzlich zu herkömmlichen verteilten Abfragen können periodisch wiederkehrende SQL-Queries erstellt werden. Die Anwender haben die Möglichkeit, wiederkehrende Abfragen über eine einmalige Zustimmung für weitere Ausführungen vollautomatisch freizugeben, wobei ein Widerspruch der Zustimmung möglich ist. Die Aufgaben des Data Aggregator und Query Broker werden über eine Webanwendung – den AKTIN-Broker – umgesetzt. Über diesen können Abfragen eingestellt und die Ergebnisse gesammelt werden. Der AKTIN-Broker wird auf einem dedizierten Server vom Institut für Medizinische Informatik am Uniklinikum RWTH Aachen betrieben. Es wird ein virtueller Server im Rechenzentrum des Uniklinikum RWTH Aachen eingesetzt.

[1] Innerhalb der gleichen Notaufnahme werden für den gleichen Patienten*in identische Nummern berechnet. In unterschiedlichen Notaufnahmen unterscheiden sich die Nummern für den gleichen Patienten*in. Nummern lassen sich standortübergreifend nicht vergleichen.

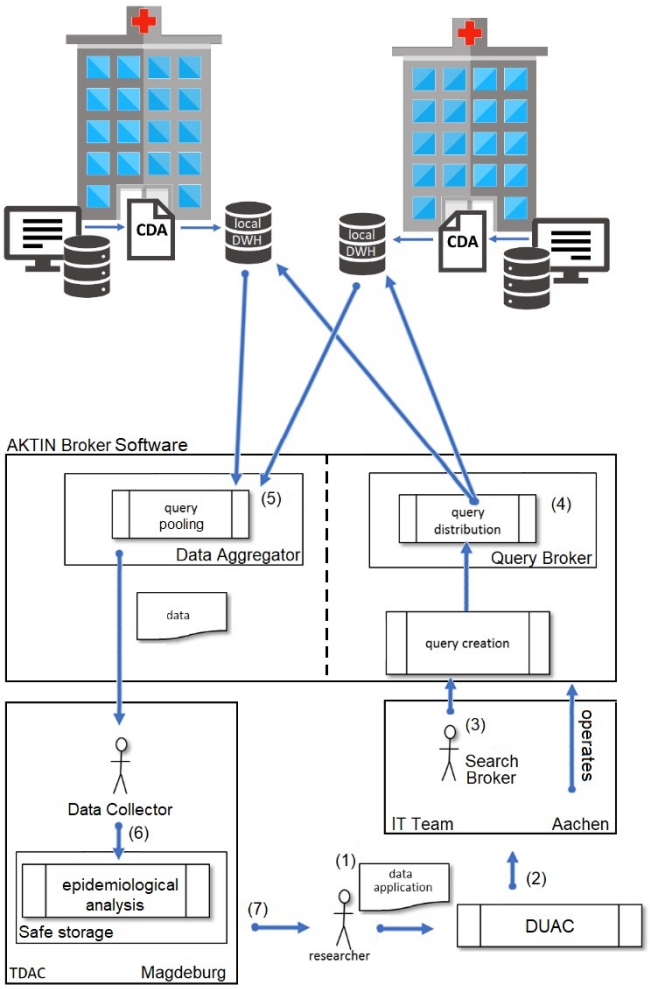

Abbildung 2: Architekturübersicht

(1) Antrag auf Datenabfrage
(2) Prüfung durch DUAC und Weitergabe an Search Broker.
(3) Erstellung der digitalen Abfrage durch den Search Broker.
(4) Verteilung der Abfrage an teilnehmende Notaufnahmen über den Query Broker.
(5) Sammlung anonymisierter Datenexporte.
(6) Übermittlung gesammelter Rückmeldungen an die auswertenden Wissenschaftler im TDAC für Analysen.
(7) Übermittlung der Auswertungsergebnisse an Forscher*innen.

2.2.3. Forschungsanfragen

Der Freigabeprozess für Forschungsanfragen wird von der AKTIN Geschäftsstelle organisiert. Forschungsanfragen können in einem formalen Antrag an das DUAC z. Hd. der AKTIN Geschäftsstelle gerichtet werden. Bei der Formulierung werden die Forscher*innen durch einen Katalog mit den für die Auswertung verfügbaren Daten unterstützt. Die Forschungsanfrage wird vom DUAC inhaltlich geprüft und ggf. in Abstimmung mit dem/der Forscher*in angepasst. Mit dem Einreichen der Forschungsanfrage erhält der/die Forscher*in eine Projekt-ID, die in der weiteren Kommunikation genutzt werden kann. Die Forschungsanfrage wird dann (mit Projekt -ID) an das AKTIN IT Team weitergegeben.

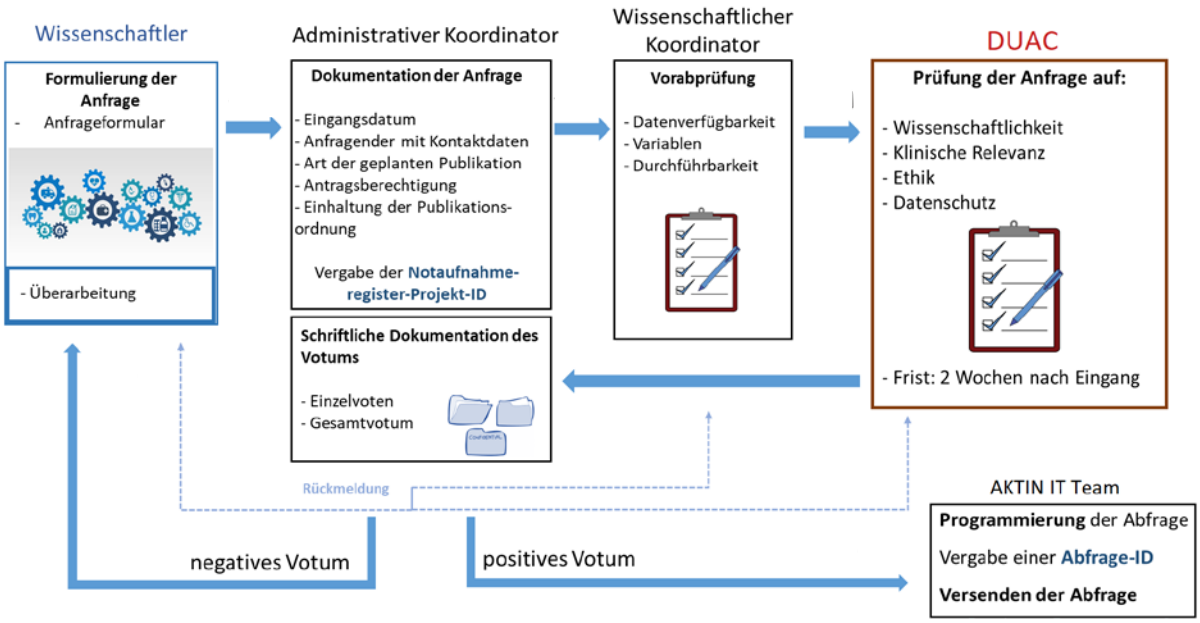

Abbildung 1: Freigabeprozess für Forschungsanfragen

2.2.4. Verteilung von Forschungsanfragen

Nach Erhalt einer Forschungsanfrage wird diese durch das AKTIN IT Team in eine SQL Abfrage übertragen. Die formale Abfrage wird dann zusammen mit der Abfragebeschreibung und der Abfrage-ID an alle teilnehmenden Krankenhäuser/Notaufnahmen per Query-Broker des AKTIN Broker verteilt. Alle teilnehmenden Standorte erhalten bezogen auf die Abfrage-ID das identische Abfragepaket. Sämtliche Forschungsanfragen (nur die Anfrage selbst – nicht die klinischen Datensätze) werden vom AKTIN-Broker archiviert und für einen Zeitraum von 10 Jahren nach Studienabschluss aufbewahrt.

2.2.5. Durchführung der Datenabfrage an jedem Standort

Im Zielsystem können die Abfrage vom Standortkoordinator über die AKTIN DWH Manager Benutzeroberfläche geöffnet und die Abfrageergebnisse angezeigt werden. Die Abfrageergebnisse enthalten keine Patienten*innen-identifizierenden Merkmale. Nach Kontrolle durch den Standortkoordinator*in können diese/r die Datenabfrage prüfen, sie ablehnen oder ihr zustimmen. Durch die Zustimmung wird eine Übermittlung der Abfrageergebnisse an den Data Aggregator ausgelöst. Zusätzlich zu den Abfrageergebnissen und der Abfrage-ID wird eine Standortidentifikation übermittelt. Abfragedurchführung und Ergebnisübermittlung können mehrfach als Serie wiederholt werden (z. B. wenn neue Patienten*innen hinzugekommen sind oder zu verschiedenen Zeitpunkten).

2.2.6. Übermittlung von Ergebnissen an Forscher*innen

Die Rohdaten können jederzeit nach Übermittlung vom TDAC über den AKTIN-Broker vom Data Collector abgerufen werden.

Die Daten werden im TDAC in einem geschützten Bereich verarbeitet. Die Mitarbeiter des TDAC bearbeiten zunächst die Fragestellung der Forscher*in anhand der gesammelten Daten. Zu diesem Zweck können Mitarbeiter der TDAC und Forscher*in in Dialog treten. Nach Abschluss der Auswertung erhalten Forscher*innen die aggregierten Ergebnisse. Falls Forscher*innen Datensätze benötigen, so wird vom TDAC ein hinreichender Grad an Anonymisierung sichergestellt (etwa k-anonymity, l-diversity, t-closeness). Der/die Forscher*in selbst hat keinen Zugriff auf die gesammelten Rohdaten. Die Weiterleitung von Daten an eine Auswertestelle erfolgt analog entsprechend den Anweisungen des DUAC und des ggf. erstellten Datenschutzkonzeptes.

2.3. 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 sonstige personenbeziehbare Daten über eine unverschlüsselte Internetverbindung oder ein anderes Medium übertragen.

2.4. Gewährleistung der Vertraulichkeit

Die Vertraulichkeit des Search Broker wird technisch gewährleistet, indem der Webserver und die Datenbank im entsprechend gesicherten und zertifizierten Rechenzentrum des UK RWTH Aachen betrieben werden. Dort gibt es insbesondere Schließ- und Alarmanlagen nach gängigen Standards, restriktiv konfigurierte Firewalls und Überwachungssoftware.

2.5. Gewährleistung der Integrität

Bei der Übertragung der 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. Diese Checksummen werden automatisch durch das Übertragungsverfahren erzeugt und überprüft.

Die Daten eines Falls (HL7 CDA) werden beim Import in das lokale AKTIN DWH auf Lesbarkeit, Übereinstimmung mit der konsentierten Datensatzbeschreibung, Vollständigkeit und Plausibilität getestet, soweit diese Prüfalgorithmen a-priori festgelegt werden können. Sind die Daten in einem Umfang fehlerhaft, dass eine Nutzung für die Zwecke der Evaluation nicht möglich ist (nur basierend auf den Vorgaben der Prüfalgorithmen, darüber hinaus können sie trotzdem nicht plausibel bzw. falsch sein), wird der Import des Falls abgelehnt.

2.6. Gewährleistung der Verfügbarkeit

Am Standort der UK Aachen ist die Verfügbarkeit der Daten durch den Betrieb im jeweiligen Rechenzentrum gesichert. Es gibt bzgl. der Notstromversorgung, redundanter Klimatisierung, Netzanbindung etc. gängige Vorkehrungen. In den lokalen DWHs gelten jeweils lokale Bestimmungen.

2.7. Gewährleistung der Belastbarkeit der Systeme

Die Belastbarkeit der Hardware bzw. des Rechenzentrums des Uniklinikum Aachen genügt den gängigen (höchsten) Anforderungen. Eine hohe Belastung der Systeme ist nicht zu erwarten, und auch kurzzeitige Ausfälle würden die Projektziele nicht gefährden. In den lokalen DWHs gelten jeweils lokale Bestimmungen.

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

Die Daten des AKTIN Brokers werden in täglichen Backups gesichert. Im Bedarfsfall können die vorliegenden Daten aus einem Backup wiederhergestellt werden. Die Backups werden für einen Monat gespeichert und anschließend automatisch gelöscht. In den lokalen DWHs gelten jeweils lokale Bestimmungen.

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

Eine jährliche Überprüfung (zu Beginn eines Kalenderjahrs, dokumentiert durch das IT Team) 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

In den lokalen DWHs gelten jeweils lokale Bestimmungen.

2.10. 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.

In den lokalen DWHs gelten jeweils lokale Bestimmungen.

3. Betroffenenrechte

3.1. Erfüllung der Informationspflicht nach Art. 13/14 DSGVO

Für die Erhebung von personenbezogenen Daten gilt Artikel 14 DSGVO. Es werden nach Artikel 14 Abs. 1 und 2 DSGVO notwendige Informationen für die Öffentlichkeit auf der Webseite des Projekts zur Einsicht gestellt.

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. Im Rahmen der AKTIN Infrastruktur werden anonymisierte Daten erhoben.

Die Anfrage zur Datenauskunft kann nur über den jeweiligen Standort erfolgen, da nur das jeweilige Klinikum Zugriff auf identifizierende Daten hat. Sollten sich Betroffene direkt an das AKTIN-Office wenden, bekommen sie die Informationen nach Art. 13 bzw. 14 DSGVO und werden an das jeweilige Klinikum verwiesen (z. B. Kategorien der Daten, Rechtsgrundlage, 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.

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

Die Betroffenen können eine Löschung der sie betreffenden personenbezogenen Daten 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.

Die Anfrage zur Löschung sollte über den jeweiligen Standort erfolgen, da nur das jeweilige Klinikum Zugriff auf identifizierende Daten hat. Sollten sich Betroffene direkt an das AKTIN-Office wenden, werden Sie an das jeweilige Klinikum verwiesen. Der Ausschluss von Patienten wird im AKTIN Consent-Manager dokumentiert.

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.

3.3.1. Widerspruchsfolgen bzw. Folgen von Löschanfragen

Ein Widerspruch führt zu einer Löschung der im lokalen AKTIN DWH gespeicherten medizinischen Daten des/der Patienten*in durch den jeweiligen Standort.

3.4. Verantwortung für die Umsetzung der Betroffenenrechte

Für die Erfüllung der Betroffenenrechte übernimmt der Standort die Verantwortung im Sinne von Art. 26 DSGVO. Die beteiligten Projektpartner werden vertraglich verpflichtet, entsprechend des hier definierten Prozesses, an der Erteilung der Auskunft mitzuwirken. Die Dateneigner verpflichten sich ebenfalls zur Mitwirkung.

3.5. Datenlöschung

Datenübermittlungen bzw. -erhebungen finden seit 2015 statt. Es gelten die Lösch- und Aufbewahrungsfristen gemäß den rechtlichen Vorgaben am jeweiligen Standort.

Für Abfragen zusammengeführte Daten werden gelöscht, (1) sobald ein Forscher*in (oder die Auswertestelle) die gesammelten Daten abgerufen hat; oder (2) wenn innerhalb von 90 Tagen keine Interaktion mit Forscher*in oder TDAC erfolgt ist. Die Löschung kann durch den Forscher*in nicht aufgeschoben oder verhindert werden. Bei der Löschung wird die Abfrage-ID und Ticketnummer weiterhin aufbewahrt und als gelöscht gekennzeichnet. Alle anderen zugehörigen Daten werden

gelöscht. Sollten nach der Löschung weitere Abfrageergebnisse von Standorten geliefert werden, so werden diese sofort gelöscht. Für die Auswertungsdauer von (ggf. vollständig anonymen) Daten durch die Forscher*innen gelten Löschfristen gemäß den Vorgaben des DUAC und [3].

4. Vereinbarung zur gemeinsamen Verantwortlichkeit und Inkrafttreten

Das vorliegende Datenschutzkonzept wurde von allen Projektleitern der Projektmitglieder geprüft, die in den Prozess der Datenverarbeitung einbezogen sind.

5. Anlagen

Anlage 1 – Studienzentren

Anlage 2 – Ansprechpartner Datenschutz

Anlage 3 – Datensatzbeschreibung Datensatz Notfallregister

Anlage 4 – Ethikvotum

Anlage 5 – Geschäftsordnung DUAC

Anlage 6 – Publikationsordnung

Anlage 7 – Basismodul Notaufnahmeprotokoll

Anlage 8 – Datensatz Abrechnungsdaten

6. Literatur

[1] K. Pommerening, J. Drepper, K. Helbing, T. Ganslandt, *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.