Data management in the AKTIN Emergency Department Data Registry

Data protection concept

Disclaimer: This document is an English translation of the Data Protection Concept for the AKTIN Emergency Department (ED) Registry, provided for the convenience of non-German speaking users. Please note that this translation is intended for informational purposes only and may not capture every detail or nuance of the original German text. It is not legally binding. For all legal and formal purposes, the original German version of the document should be referred to as the authoritative source.

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

Contact

Jonas Bienzeisler
Institute of Medical Informatics
RWTH Aachen University Hospital
Address: Pauwelsstraße 30 • D 52074 Aachen
Phone: +49 241 80-88870
Email: jbienzeisler@ukaachen.de

Prof. Dr. Rainer Röhrig
Institute of Medical Informatics
RWTH Aachen University Hospital
Address: Pauwelsstraße 30 • D 52074 Aachen
Phone: +49 241 80-88790
Email: rroehrig@ukaachen.de

Content

List of abbreviations and symbols

DWH	Data warehouse
TempID	Temporary ID
IDAT	Patient-Identifying Data
MDAT	Medical data
PSN	Pseudonym

Glossary

Pseudonym/pseudonymization: "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately and is subject to technical and organizational measures that ensure that the data cannot be attributed to a data subject." (Art. 4 No. 5 GDPR)

AKTIN Broker: *Web frontend* application for the central distribution of requests to the local *DWHs* and the merging of the results. Used for data and study management in the AKTIN infrastructure and consists of *a Query Broker* and Data *Aggregator* component.

Anonymization: Information that does not relate to an identified or identifiable natural person, or personal data that has been de-identified in such a way that the data subject cannot or can no longer be identified (Recital 26, GDPR).

K-anonymity: Property of de-identified records. The data of individuals are generalized to such an extent that there are at least k-1 data twins for each field in the data set.

Data Aggregator: Component of the AKTIN broker for collecting query results. The associated queries are delivered by the *Query Broker* to all locations.

Data warehouse: A central database optimized for analysis purposes that brings together data from multiple, usually heterogeneous sources. In short, DWH; literally "data warehouse".

Location: Hospital participating in the AKTIN Emergency Department Data Registry.

***Query Broker*:** Component of the AKTIN broker for distributing data queries to all locations. The associated results are collected by the data *aggregator* .

Trusted Data Analytics Center (TDAC): Independent institution for the evaluation, processing and data protection-compliant forwarding of the collected medical data to researchers. Ensures through technical and organizational measures that the data cannot be linked to other data sources. Operated by the Department for Trauma Surgery at the Otto von Guericke University Magdeburg.

AKTIN-IT: Working group responsible for the operation and development of the technical infrastructure of the Emergency Department Data Registry. Is established at the Institute of Medical Informatics at RWTH Aachen University Hospital.

Data Use and Access Committee **(DUAC):** Scientific control committee for the examination of applications for data evaluation to the AKTIN Emergency Department Data Registry in the context of research projects. Examines these with regard to ethical and data protection aspects and releases corresponding data extracts.

1. The project

The AKTIN Emergency Department Data Registry was created from the AKTIN project "Improvement of health services research in acute medicine in Germany through the establishment of a national Emergency Department Data Registry". The project was carried out between 2013 and 2019 with BMBF funding under the auspices of DLR. For the continuation of the project and the future operation of the AKTIN Emergency Department Data Registry, the association AKTIN e.V. was founded. Members of this association are RWTH Aachen University, the Medical Faculty of the Otto von Guericke University Magdeburg, participating hospitals and the medical societies DIVI e.V. and DGINA e.V. The AKTIN Emergency Department Data Registry is operated by AKTIN e.V. with the participation of the Institute of Medical Informatics at RWTH Aachen University Hospital and the Department for Trauma Surgery of the Faculty of Medicine of the Otto von Guericke University Magdeburg.

1.1. Background

Emergency care in Germany has been in a state of upheaval for several years. Apart from random data collection in the context of individual surveys or studies, there are no regular and cross-institutional data collections in clinical emergency medicine. However, valid and comprehensive data collection on the number, reasons for presentation and the care situation of emergency patients is necessary to evaluate the measures. Organizationally relevant key figures that can be used to assess the process and result quality of emergency departments are insufficiently available in Germany in an international comparison, apart from individual cases. There is also a lack of data for systematic analyses of different forms of care using organisational and medical key figures as a basis for the necessary process of organisational development in clinical emergency care. Meaningful health care research in the acute and emergency medical field is hardly possible without this data basis.

In the AKTIN Emergency Department Data Registry, the digital documentation of all emergencies of participating hospitals is recorded in a uniform and standardized way. The collection of data in the routine care of patients with the greatest possible avoidance of redundancy enables the use of extensive, up-to-date and comprehensive data sets for questions of quality management, secondary use, health reporting and the surveillance of infectious and non-infectious disease events. The basis for data collection in the AKTIN Emergency Department Data Registry is the emergency department data set developed by the Emergency Documentation Section of the German Interdisciplinary Association for Intensive Care and Emergency Medicine (DIVI) for standardized, structured documentation in the emergency department.

In order to bring together the relevant data for the various issues, a GDPR-compliant decentralized registry infrastructure was implemented for the AKTIN Emergency Department Data Registry. Data collected in routine clinical practice is automatically stored in *decentralized* data warehouses (DWH) of the participating locations. The data is pseudonymised and stored in a decentralised manner within the treatment context. This is done in accordance with the regulations of the respective country. For the purposes of quality assurance and health services research, this data is available to the hospitals via a user interface. For scientific questions, the collected data can be made available via a *central* AKTIN broker – but only after

a *scientific control body* – the *Data Use and Access Committee (DUAC)* – has reviewed and approved a corresponding request. The data analysis is then carried out at the *Trusted Data Analytics Center* (TDAC) in Magdeburg.

1.2. Purpose of data processing

Data from the AKTIN Emergency Department Data Registry are collected for the following purposes:

1. In-house quality management
2. Cross-institutional quality management and benchmarking
3. Cross-institutional health care research in emergency and acute medicine
4. Public health surveillance by the Robert Koch Institute (RKI) and the state health authorities
5. Preparation of health reports
6. Data collection and export to specialised registries within the framework of contracts to be drawn up

The aim is to achieve the highest possible quality management, high-quality research, and health and infection surveillance in emergency and acute medicine, and to process this data in full compliance with the legal standards and recommendations applicable in Germany and the EU.

1.3. Scope of data processing

Within the framework of the AKTIN Emergency Department Data Registry, data is continuously collected prospectively. This takes place in the participating locations when participation in the registry begins, in individual cases data can also be transmitted retroactively to the local DWH systems. The data is collected in emergency departments that have established a uniform documentation standard. The participating hospitals store the selected data on each patient in the emergency department in a local DWH. This is part of the infrastructure of the AKTIN Emergency Department Data Registry, but is administered by the locations themselves. The data and the server on which it is located are owned or controlled by the sites. The data is collected independently by the respective location. For scientific questions, the data can be retrieved centrally via the AKTIN broker (see Appendix 1 – Study Centers).

The data is always exported de-identified. The principles of data minimization are applied to the queries to the locations. The data analysis is carried out in the TDAC. There, technical and organizational measures are taken to ensure that the data cannot be linked to other data sources. Only aggregated data is transmitted to third parties, partners not involved in the project. Exceptions, e.g. in the context of health reporting or on the basis of contracts, are possible after examination by the DUAC. Each data query requires a study protocol, which is checked by the DUAC for compliance with scientificity, ethical principles and the data protection concept, including data minimization.

For technical operation, for the purpose of quality assurance and for technical support, data is also processed by AKTIN-IT at the Institute of Medical Informatics at RWTH Aachen University Hospital. To ensure technical operation and for quality assurance purposes, anonymous import

statistics of each active DWH are automatically transmitted to the AKTIN broker (start of the AKTIN DWH, last successful/failed import, the number of imported/updated/failed/incorrect cases since start, version of the software components used). The AKTIN IT team also processes data in the context of support requests from the participating hospitals. The purpose and scope of the data collection depend on the respective support request. As far as possible, de-identified data is processed, which is deleted after the technical support has been completed. If access to personal data becomes necessary in the context of technical support, a separate agreement on order processing must be concluded between Uniklinik RWTH Aachen and the respective location.

Any data processing that goes beyond this (and beyond this data protection concept) requires an independent legal basis and an adequate data protection concept as well as the consent of the DUAC.

1.3.1. Data collection in accordance with TMF's Data Protection Guide

The data collection or the organizational separation of identifying and medical data follows the recommendations of the Technology and Methods Platform for Networked Medical Research (TMF). Data collection is carried out in accordance with the basic model (with decentralised patient lists) of the Guidelines for Data Protection in Medical Research Projects – Generic Solutions of TMF 2.0 . The data is transferred pseudonymized on site to a local data warehouse, which is under the data sovereignty of the treating facility, the emergency department of the respective hospital. For evaluations, the data is made available via the AKTIN broker in an de-identified form.[1]

One deviation from the TMF data protection guidelines lies in the waiver of explicit consent of the data subjects, who are often not even capable of giving consent. However, the complete inclusion of all treated patients is necessary, especially because of participation in infection surveillance.

1.4. Organizational Structure and Responsibilities

The AKTIN Emergency Department Data Registry is operated by AKTIN e.V. in cooperation with the Institute of Medical Informatics at RWTH Aachen University Hospital (IMI) and the Department for Trauma Surgery at Otto von Guericke University Magdeburg (KCHU) (see Appendix 2 – Contact Data Protection). According to SGB V §287a, the association is primarily responsible for data collection in the AKTIN Emergency Department Data Registry within the meaning of §27 BDSG. The actual data processing is carried out under joint responsibility within the meaning of Article 26 GDPR by the respective study center, AKTIN-IT and the Trusted Data Analytics Center.

1.4.1. AKTIN Office

The AKTIN Office is operated by the KCHU. The AKTIN Office supervises the (non-technical) organizational processes in the AKTIN Emergency Department Data Registry, e.g. the approval process for research requests.

1.4.2. Centers

The emergency departments of hospitals that operate an AKTIN-DWH – so-called participating locations – participate in the data collection within the framework of the AKTIN Emergency

Department Data Registry. A location with multiple emergency departments may include multiple DWH. Contracts are concluded before working with locations. Local data management is the responsibility of site coordinators. They are responsible for implementing and complying with all ethical, legal, contractual and organizational requirements for data management (see Appendix 1 - Study Centers).

1.4.3. AKTIN-IT

AKTIN-IT at IMI is responsible for the operation of the technical infrastructure of the AKTIN Emergency Department Data Registry, the technical implementation of data queries via the AKTIN broker (in accordance with the specifications and instructions of the DUAC) and the IT support of the locations.

1.4.4. Trusted Data Analytics Center

KCHU operates the *Trusted Data Analytics Center* (TDAC). The data provided by the project partners providing the data will be processed and, if necessary, forwarded. The TDAC carries out the analyses and uses technical and organisational measures to ensure that the data cannot be linked to other data sources. Aggregated data may be transmitted to third parties, partners not involved in the project, as part of research requests. Exceptions, e.g. in the context of health reporting or on the basis of contracts, are possible after examination by the DUAC.

1.4.5. Data Use and Access Committee

Scientists can request the provision of a dataset from an independent scientific control committee – the *Data Use and Access Committee (*DUAC). Such a request is made for a specific scientific question. The committee examines the application with regard to ethical and data protection aspects. In the event of a positive evaluation, the respective data excerpt is then created in accordance with the specifications of the Review Board and forwarded for the purpose of evaluation with regard to the question. The exact procedure is laid down in rules of procedure. Only the necessary data will be requested and evaluated in compliance with data protection.

1.4.6. External cooperations

External cooperations are planned. An *evaluation point* can be set up by external partners. Such cooperation must be contractually regulated and approved by the DUAC. Data will be passed on to cooperation partners in the same way as data will be passed on to scientists as specified in Section 2.2.6.

1.5. Accumulated data and associated risks

The data standard is the emergency department data set in the current version, currently V2015.1 (as of 06/2023). The data to be collected was compiled by the Emergency Documentation Section of the German Interdisciplinary Association for Intensive Care and Emergency Medicine (DIVI). The DIVI is an umbrella organization of the 18 professional societies involved in intensive care and emergency medicine in Germany with individual membership. [2]

In addition, event- or project-related inpatient treatment data (individual items from the data set in accordance with § 21 KHEntgG, see Annex 8 – Billing Data Record) can *be made available* as an option.A suitable occasion can be determined by the DUAC. Each location

then decides independently on the content and scope of the inpatient treatment data processed. In particular, only certain items may be made available by the locations (without justification), but specifications for the structure and a minimum data set apply (see Annex 8 – Billing Data Record). The data can be imported into the local AKTIN DWH via a user interface in the AKTIN DWH Manager. The data is then processed in the same way as the data generated in the emergency department data set.

1.5.1. Categories

The data is health data within the meaning of Article 9 (1) and Article 4 No. 15 GDPR. All data categories listed are necessary in the sense of data minimization and for the purposes of data processing. The use of the data is intended exclusively for these purposes. This data will not be used in any other way than for the purposes described. It is guaranteed that the provisions of data protection are complied with and that only the data required for the respective purpose is evaluated.

1.5.2. Protection needs and risk classification

The health data collected in the project is personal data of the special category within the meaning of the GDPR. In particular, there is a very high need for protection for data from emergency departments. For all data that is collected, measures apply according to the highest protection requirements. It is technically and organizationally ensured (by means of the DUAC) that identifying medical data cannot be merged outside the emergency department, where the patient is personally known.

The exact technical and organizational measures – according to the protection requirements or the protection classes – can be found in Chapter 2.

1.5.3. Re-identification options

The data is available for evaluation in de-identified form within the meaning of Article 4 No. 5 GDPR.

The data is generally published without personal reference. Only aggregated results are published, which in particular do not allow any conclusions to be drawn about individual:

- Patients
- Hospital staff

1.5.4. Residual risk

Even if technical and organisational measures (Chapter 2) ensure that identifying and medical data cannot be merged, this cannot be completely ruled out. The TDAC could be leaked personal data through inadequate anonymization. As part of IT support, the IT team could be able to view disposable pseudonyms from various institutions and then resolve the pseudonyms through brute force procedures, such as trial encryption. IT support would then have access to potentially personal case or patient numbers. It is not possible to merge across several locations. Due to this residual risk, the employees of the TDAC or the IT team are prohibited from assigning the collected data to a data subject in the form of service instructions or confidentiality agreements.

1.6. Ethical and regulatory requirements

Research on humans and the processing of associated data is necessary for the development and safety of medicine and is therefore of great interest to society. The interests of the patients must be safeguarded at all times.

The data protection regulations of the European Union (EU), the federal government and the respective state are complied with at all times. In those places where an area-specific law regulates the encroachment on the right to informational self-determination in a more specific way than a more general data protection law, reference is made to the corresponding legal basis. The AKTIN Emergency Department Data Registry undertakes to update the data protection agreement by means of new annexes if this becomes necessary due to technical developments or changes in the law. The EU General Data Protection Regulation (GDPR), the respective applicable state laws (e.g. state data protection and hospital laws) and the Federal Data Protection Act (BDSG) apply to data protection. In the event of serious disruptions to the processing process, suspicion of data protection violations or other irregularities in the processing of the data (cf. GDPR Art. 4 (12) as well as Art. 33, Art. 34), data subjects, the data owners and the supervisory authority will be informed immediately by the AKTIN Emergency Department Data Registry by the AKTIN Office. Data subjects who cannot be contacted will be informed via a website (http://www.aktin.org).

With regard to scientific quality, the guidelines for safeguarding good scientific practice of the German Research Foundation are complied with. The WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects applies.[3][4]

The infrastructure of the AKTIN Emergency Department Data Registry was positively assessed by the ethics committee of the Medical Faculty of the University of Magdeburg (see Annex 5 - Ethics vote, vote 160/15). The registry is registered in the German Register of Clinical Trials (study ID: DRKS00009805).

1.7. Legal basis for data processing

1.7.1. Preamble to the legal assessment of the AKTIN infrastructure

The AKTIN infrastructure is a special case in the registry landscape. The data is pseudonymised and stored within the hospitals within the treatment context in a decentralised manner in accordance with the regulations of the respective state. All data remains within the patient-managing department (usually the emergency department). The responsibility for carrying out the data queries in the DWH systems lies with the locations. The technology gives them insight into the queries as well as the data to be transmitted and can check whether queries and data to be transmitted comply with the laws applicable to the location, as well as internal and external regulations. Only after approval by the hospital will the data be merged centrally.

The data are transmitted to third parties, in this case the central infrastructure of the AKTIN Emergency Department Registry, with de-identified, partial data sets, whereby the k anonymity of the data increases in the multi-stage processing chain. This ensures that at every step in the processing chain, re-identification of data subjects is excluded. At the latest from the point of complete anonymization of the data, the processing no longer falls under data

protection legislation. In the case of data queries in the context of scientific questions, the aim is to achieve this state as early as possible in the processing chain. This means that central data processing in many research projects does not fall under data protection legislation. If data sets that have not yet been fully de-identified are transmitted to the central AKTIN infrastructure, the legal basis for data processing described in the following paragraph applies.

1.7.2. Legal basis for processing data without consent.

The medical data is collected independently by the sites for billing, documentation or accountability purposes and then used for quality assurance purposes or scientific purposes themselves or by third parties. It can be assumed that the purpose is compatible according to GDPR Art. 6 (4).

After an assessment by the DUAC, data requests are transmitted to the sites, which independently decide on participation and data provision. The participating locations determine for themselves which employees – so-called *location coordinators* - have the appropriate powers. Thus, the decision on the use of the data lies with the locations as data owners (according to GDPR Art. 6 (4)), while the responsibility for the technical implementation, data consolidation and data analysis lies with the AKTIN Emergency Department Data Registry. The processing of personal data must therefore be assumed to be joint responsibility within the meaning of Article 26 of the GDPR. The fundamental decisions on the purposes and means of processing within the framework of the AKTIN Emergency Department Data Registry are made by AKTIN e.V.

The legal basis for the processing of the data is:

- EU GDPR (EU-V 2016/679)
- Federal Data Protection Act
- Criminal Code (StGB)
- For processing in hospitals, the respective state legislation must also be taken into account.

In principle, the data processing of health data falls under GDPR Art. 9 (Processing of special categories of personal data) or §22 BDSG as well as valid state laws. The lawfulness of the data processing of data that does not belong to the special category of personal data is regulated by GDPR Art. 6 (1) lit.e. well-founded.

> "The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (GDPR Art. 6 (1) lit. e).

The provision of such data for cross-institutional quality assurance in emergency care (benchmarking) and to answer scientific research questions on emergency care or in the context of health reporting is in the public interest.

In addition, data can be provided in accordance with GDPR Art. 6 (1) lit. f.:

> *"the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data*

> *subject which require the protection of personal data, in particular where the data subject is a child"* (GDPR Art. 6 (1) lit. f).

The processing is lawful because the data is provided on the basis of a legitimate (scientific) interest of the cooperation partners involved or a third party. Effective protection of the identity and interests of the data subjects / patients is guaranteed at all times and is checked by the DUAC on a case-by-case basis.

The justification of data processing for scientific purposes is also based on GDPR Art. 89 and §27 BDSG and is therefore also to be regarded as a public interest. In particular, these are:

> *'Processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes shall be subject to appropriate safeguards for the rights and freedoms of the data subject in accordance with this Regulation. These safeguards ensure that technical and organisational measures are in place to ensure, in particular, respect for the principle of data minimisation. These measures may include pseudonymization, if it is possible to fulfill these purposes in this way. In all cases where these purposes can be fulfilled by further processing, where the identification of data subjects is not or no longer possible, these purposes are fulfilled in this way" GDPR Art. 89 (1).*

The following applies:

> *'By way of derogation from Article 9(1) of Regulation (EU) 2016/679, the processing of special categories of personal data within the meaning of Article 9(1) of Regulation (EU) 2016/679 shall also be permitted without consent for scientific or historical research purposes or for statistical purposes, where the processing is necessary for those purposes and the interests of the controller in the processing outweigh the interests of the data subject in the exclusion of the processing. The controller shall provide for appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2) sentence 2"* (BDSG Section 27).

The data processing of health data in the AKTIN Emergency Department Data Registry falls under GDPR Art. 9 (Processing of special categories of personal data) or §22 BDSG and thus under a special need for protection. Informed consent as a legal basis (GDPR Art. 6 (1) lit. a or Art. 9(2) lit. a) is not possible in the project. On the one hand, informed consent would not be possible in an emergency department situation, and on the other hand, a so-called selection bias with regard to the ability to consent would falsify the study results. GDPR Art. 89, GDPR Art. 9(2) and BDSG §22 (1) or §27 provide for a justification of the processing of data for scientific purposes (GDPR Art. 9(2) lit j, BDSG §27) or in the field of public health (GDPR Art. 9(2) lit i, BDSG §22), insofar as this is necessary for the purpose of research, or the answer to the research question are necessary and are in the public interest. In particular, if these

> *'(c) is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or to ensure high standards of quality and safety in healthcare and medicinal*

> *products and medical devices; in addition to the measures referred to in subsection (2), in particular, the professional and criminal law requirements for the protection of professional secrecy must be complied with, or*
>
> *d) is absolutely necessary for reasons of considerable public interest"* (BDSG §22 (1)).

In each case, this is done on the condition that appropriate and specific measures are taken to safeguard the interests of the data subject in accordance with Section 22 (2) sentence 2 or GDPR Art. 9(2) lit. i in conjunction with Recital 54 GDPR. These measures are:

- Pseudonymised storage of all data within the healthcare facility or emergency department in the context of treatment.
- Two-stage data transmission in accordance with data minimization: Only the (de-identified) data that is necessary to answer the question is transmitted to the TDAC. There, the data is processed in a protected area and only transmitted to third parties after sufficient k anonymity has been ensured.
- Case-by-case review of data requests by a scientific control committee (DUAC) and federated data access authorization through participating sites in connection with the aforementioned opening clauses as well as in accordance with GDPR Art. 6 (4).
- Technical measures (see below) for data security

For the emergency departments or hospitals providing data, the local laws in conjunction with the aforementioned opening clauses apply on a case-by-case basis depending on the respective data request. The state hospital and state data protection laws of the respective federal states in which the data is collected apply.

In addition to data protection legislation, medical confidentiality applies (§203 StGB). Since only structured and de-identified data is transmitted to the outside world, it cannot be assumed that a disclosure of secrets takes place contrary to §203 (1) StGB.

Information in accordance with GDPR Art. 14 is published on the http://www.aktin.org website and made available to patients by the locations.

2. Technical and organizational measures

There is a very high need for protection for the processed data. All data processing is therefore based on a role and rights concept. All data is collected in a single-use pseudonymized form under the data sovereignty of the treating facility, i.e. the emergency department of the respective hospital. For data requests for research purposes, the instructions of the DUAC apply, which guarantees data protection and ethical standards. Only de-identified data leaves the data-providing institutions after they have consented to a transfer.

The technical and organisational measures taken by the project partners providing the data themselves are not part of this data protection concept, as the need for protection exists independently of the project and has already been implemented accordingly (see Annex 1 - Study centres). In particular, this primarily involves data processing with other purposes and legal bases outside the regulatory competence of the AKTIN Emergency Department Data Registry. The participating hospitals bear operational responsibility for the operation of the local infrastructure components (AKTIN-DWH and any interfaces).

2.1. Roles and rights

All data collected within the framework of the AKTIN Emergency Department Data Registry is subject to measures corresponding to a very high need for protection. The data is therefore stored locally and only transmitted to third parties after a standardized approval process by the DUAC. There is a strict role concept. With the help of the technical and organizational measures, the principles specified by Art. 32 GDPR (security of processing) are complied with.

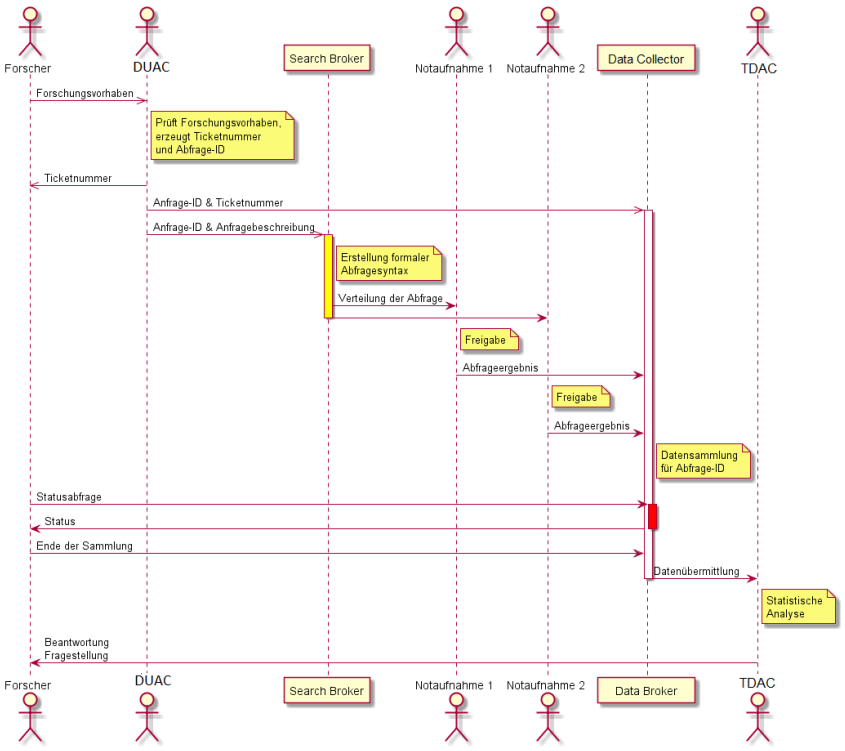

Figure 1 Process overview according to the role and rights concept

2.1.1. Data Use and Access Committee (DUAC)

The DUAC checks research requests before they are submitted to the sites. This role is less technical than scientific. The DUAC includes at least one employee of the Trusted Data Analytics Center.

2.1.2. Search Broker (SB)

The Search Brokers convert the queries approved by the DUAC into database queries and standardized terminologies and set them in the Query Broker. They then transmit the queries to the site coordinators using AKTIN brokers. The search brokers are part of the IT team at the Institute of Medical Informatics at RWTH Aachen University Hospital.

2.1.3. Location Coordinator

The site coordinators have the authority to be responsible for local data management in a location. Site coordinators are designated by the location. If necessary, the role can be filled by one or more persons together. They are responsible for implementing and complying with all ethical, legal, contractual and organizational requirements for data management. They are therefore responsible for a local review of each query, as well as for determining and checking compliance with the applicable criteria of anonymity by their own institution. The site coordinator(s) must agree to a research query before it is conducted on the data of the corresponding site. They can review the result tables before they are sent.

2.1.4. Data Collector (DC)

Only a data collector has the authorization to retrieve anonymous raw data or query results collected in the data aggregator via the AKTIN broker. The Data Collector is responsible for forwarding the query results of the sites collected in the Data Aggregator to the TDAC. The researcher can ask the Data Collector about the status of the feedback and determine the end of the data collection or collection. In addition, the results of technical inquiries can be forwarded to AKTIN-IT.

2.1.5. Trusted Data Analytics Center (TDAC)

The task of the TDAC staff is to check, process, aggregate and evaluate the collected query results. The TDAC staff receives the collected anonymous raw data or query results and evaluates them. The TDAC ensures that in the event of data being passed on to the researcher, the criteria of k-anonymization and l-diversity are met.

2.1.6. Data Protection Officer (DS)

AKTIN e.V. appoints a data protection officer who is independent of all other governing bodies with influence on data management structures. The Data Protection Officer is an independent supervisory body for all data processing bodies, as well as for data enquiries and the DWH.

2.1.7. Researcher

The researcher can register research requests via the AKTIN Office and thus request data extracts. All requests are logged.

2.1.8. Evaluation point

In special cases (e.g. in the case of periodic queries in the context of infection surveillance), a transfer of de-identified raw data to researchers can also be set up if this has been previously approved by the DUAC and either sufficient anonymisation is in principle already given on the

basis of the query (e.g. structure of the data, automated anonymisation) or another legal basis (e.g. for reasons of public interest in the area of public health, such as protection against serious cross-border health threats in the event of a pandemic pursuant to Section 22 (1) No. 1 (c) BDSG in conjunction with Art. 9 (2) (g) GDPR) for data transmission. An *evaluation point will then* be set up by the researchers. This is to be described accordingly in the request to the DUAC; an additional data protection concept may have to be drawn up.

2.1.9. Role conflicts

All roles can be shared in some cases. The role of data protection officer may be exercised at a participating location, but not in combination with other data processing bodies, as they are to be monitored. The data protection officer must be independent - he can belong to a location, but must not have an operational mandate in data processing.

Table 1: Roles that can be shared: Site Coordinator (Site), Data Protection Officer (DS), Data Use and Access Committee (DUAC), Search Broker (SB), Data Collector (DC), Trusted Data Analytics Center (TDAC).

	Location	Privacy	DUAC	Search Broker	Data Collector
Location					
Privacy	Yes				
DUAC	Yes	No			
Search Broker	Yes	No	Yes		
Data Collector	No	No	Yes	No	
TDAC	No	No	Yes	No	Yes

2.2. Data flows and IT infrastructure

The infrastructure of the AKTIN Emergency Department Data Registry consists of decentralized data collection in the emergency departments, which can be made available via a central IT component – the AKTIN broker.

2.2.1. Decentralised data collection in the emergency department

The emergency departments of the participating hospitals use electronic systems to record routine medical documentation according to the Emergency Department dataset. In addition, each hospital operates a uniform DWH software on its own dedicated server. The DWH software is provided by the AKTIN Emergency Department Data Registry. Using an export interface, the corresponding data is digitally exported from the emergency department's information system and stored as standardised HL7-CDA documents. These CDA documents

are then transferred to the DWH server. These documents can be imported via two possible standardized transmission paths: On the one hand via an HL7 FHIR REST endpoint and on the other hand via an IHE XDS.b document receiver SOAP API. After receipt, an automated syntactic and content-related validation of the sent content of the emergency department protocol (HL7-CDA) is carried out using extensive Schematron rules.

The DWH does not contain any directly patient-identifying features (e.g. pat ID, surname, first name), but a number that is generated site-specific using a single-use cryptographic method (hash).[1] This pseudonym cannot be used to infer the identity of the patient, but it allows follow-up data to be assigned to the appropriate data sets. The local employees do not have direct access to the one-way hash. Only the database administrator can view this pseudonym for technical reasons. Only authorized employees of the patient-managing department have access to the data via the DWH user interface.

In addition to emergency department data, participating hospitals have the option of integrating further data from the inpatient stay (e.g. reason for discharge, discharge time, main diagnosis, secondary diagnoses, procedures, day of surgery, ventilation hours) on their emergency department patients into the local data warehouse. The assignment to the existing data is carried out via the cryptographic one-way procedure as described above. Such data can then also be used for reports, benchmarks and central queries. On request or on behalf of the hospital, the DWH software can be maintained by the IT support of the AKTIN Emergency Department Data Registry.

The local data warehouse can be used by local employees for their own questions. Access is authenticated on a personal basis via the DWH user interface. Employees can perform queries on all stored parameters, but do not have access to the generated one-way hash.

2.2.2. Central data collection

All requests for data extracts for research projects and questions (e.g. for research, quality assurance) are reviewed by DUAC and then forwarded to the sites. The *Query Broker* is the communication interface and distributes the requests for data extracts as SQL queries to all locations. In each hospital, the question or SQL query must be explicitly agreed to by the site coordinators before a query is carried out and data is exported. The exports of the sites are collected at a central, independent point (the *data aggregator*) and can then be retrieved by the TDAC. There, the aggregated results or coarsened data sets are processed and evaluated as well as transmitted to the researcher after checking that sufficient anonymity and diversity have been determined in advance. In addition to conventionally distributed queries, periodically recurring SQL queries can be created. Users have the option of releasing recurring queries for further executions fully automatically via a one-time consent, whereby a contradiction of consent is possible. The tasks of the Data Aggregator and Query Broker are implemented via a web application – the AKTIN Broker. This can be used to set queries and collect the results. The AKTIN broker is operated on a dedicated server by the Institute of Medical Informatics at RWTH Aachen University Hospital. A virtual server will be used in the computer center of the RWTH Aachen University Hospital.

[1] Within the same emergency department, identical numbers are charged for the same patient. In different emergency departments, the numbers for the same patient differ. The numbers cannot be compared across locations.

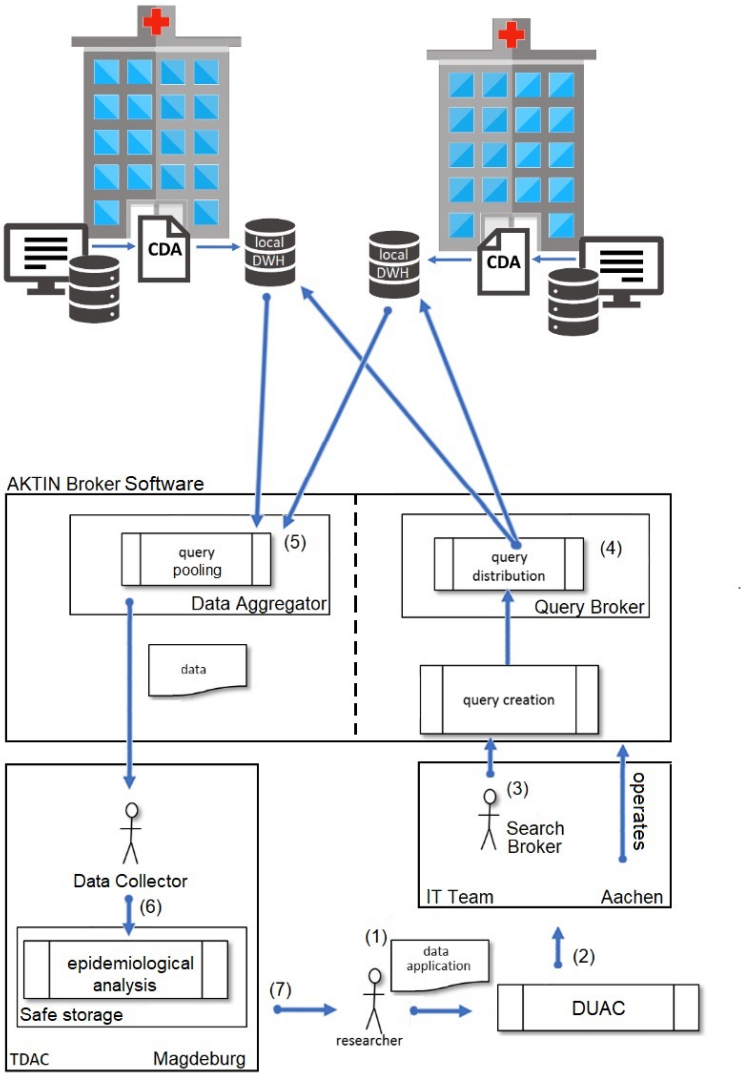

Figure 2: Architecture Overview

(1) Request for data retrieval(2) Review by DUAC and share with Search Broker. (3) Creation of the digital query by the Search Broker. (4) Distribution of the query to participating emergency departments via the Query Broker. (5) Collection of de-identified data exports. (6) Transmission of collected feedback to the evaluating scientists in the TDAC for analysis. (7) Transmission of the evaluation results to researchers.

2.2.3. Research Requests

The approval process for research requests is organized by the AKTIN Office. Research requests can be submitted in a formal application to the DUAC for the attention of the AKTIN Office. The researchers are supported in the formulation process by a catalogue with the data available for evaluation. The content of the research request will be reviewed by the DUAC and, if necessary, adapted in coordination with the researcher. With the submission of the research request, the researcher receives a project ID that can be used in further communication. The research request is then forwarded (with project ID) to the AKTIN IT team.

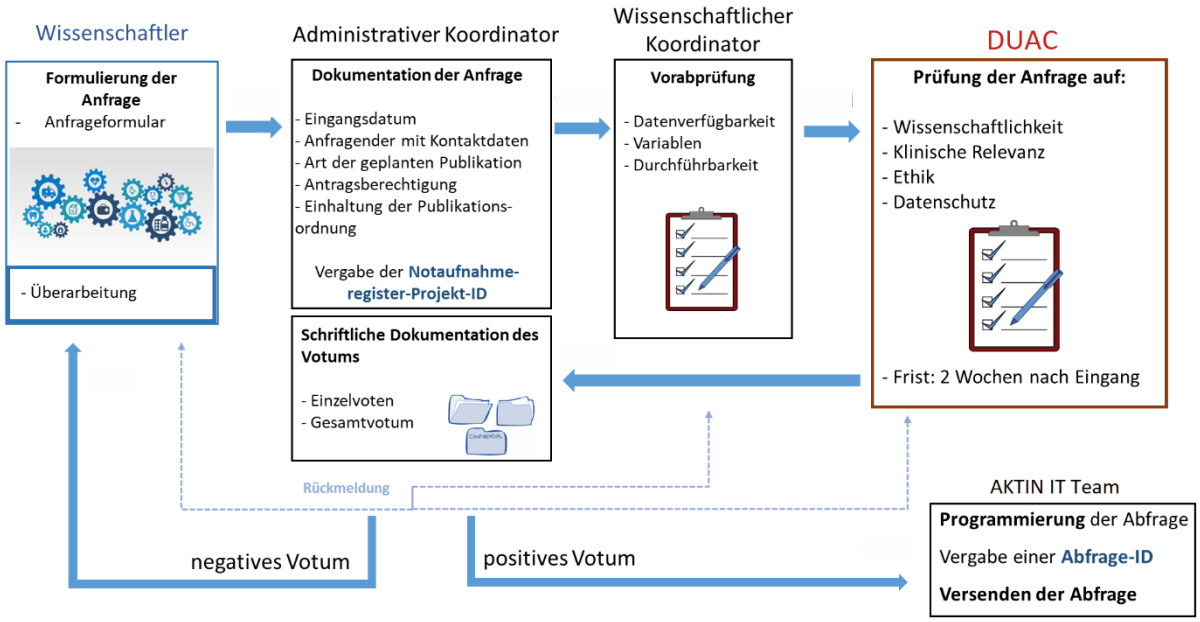

Figure 2: Approval process for research requests

2.2.4. Distribution of research requests

After receiving a research request, the AKTIN IT team transfers it to an SQL query. The formal query is then distributed to all participating hospitals/emergency departments together with the query description and the query ID via the AKTIN broker's query broker. All participating locations will receive the identical query package based on the query ID. All research requests (only the request itself – not the clinical records) are archived by the AKTIN broker and retained for a period of 10 years after study completion.

2.2.5. Execution of the data query at each location

In the target system, the query can be opened by the site coordinator via the AKTIN-DWH Manager user interface and the query results can be displayed. The query results do not contain any patient-identifying characteristics. After checking by the site coordinator, the site coordinator can reject or agree to the data request. Consent triggers a submission of the query results to the data aggregator. In addition to the query results and the query ID, a location identification is submitted. Query execution and result transmission can be repeated several times as a series (e.g. when new patients have joined or at different times).

2.2.6. Transmission of results to researchers

The raw data can be retrieved from the Data Collector at any time after transmission from the TDAC via the AKTIN broker.

The data is processed in a protected area in the TDAC. The TDAC staff will first work on the researcher's question based on the data collected. To this end, TDAC staff and the researcher can enter into dialogue. After completion of the evaluation, researchers receive the aggregated results. If researchers need data sets, the TDAC ensures a sufficient degree of anonymization (e.g. k-anonymity, l-diversity, t-closeness). The researcher himself or herself does not have access to the raw data collected. The forwarding of data to an evaluation point is carried out

analogously in accordance with the instructions of the DUAC and the data protection concept that may have been created.

2.3. Encryption

The transmission of data between the parties involved is always done with transport encryption (TLS 1.2 with SHA2). Pseudonyms, (temporary) IDs or other personal data will never be transmitted via an unencrypted internet connection or any other medium.

2.4. Guarantee of confidentiality

The confidentiality of the Search Broker is technically guaranteed by operating the web server and the database in the appropriately secured and certified data center of the University Hospital RWTH Aachen. In particular, there are locking and alarm systems according to common standards, restrictively configured firewalls and monitoring software.

2.5. Ensuring integrity

When the data is transferred, checksums are used to check whether the data has been transmitted correctly. For this purpose, a message digest procedure is used over the entire amount of data (user data and IDs), which detects any form of transmission errors (number of lines, incorrect transmission of content, etc.). In case of errors, the received data will be deleted and the transmission will be carried out again. These checksums are automatically generated and checked by the transfer method.

The data of a case (HL7 CDA) are tested for readability, compliance with the agreed data set description, completeness and plausibility when imported into the local AKTIN DWH, insofar as these check algorithms can be defined a priori. If the data is incorrect to such an extent that it is not possible to use it for the purposes of the evaluation (only based on the specifications of the test algorithms, beyond which it may still not be plausible or false), the import of the case will be rejected.

2.6. Ensuring availability

At the IMI, University Hospital Aachen, the availability of data is ensured by operation in the respective computer center. There are common precautions regarding emergency power supply, redundant air conditioning, grid connection, etc. Local regulations apply in each of the local DWHs.

2.7. Ensuring the resilience of the systems

The resilience of the hardware and the computer center of the University Hospital RWTH Aachen meets the common (highest) requirements. A high load on the systems is not to be expected, and even short-term failures would not jeopardize the project goals. Local regulations apply in each of the local DWHs.

2.8. Procedures for restoring the availability of data after a physical or technical incident

The AKTIN broker's data is backed up in daily backups. If necessary, the existing data can be restored from a backup. The backups are stored for one month and then automatically deleted. Local regulations apply in each of the local DWHs.

2.9. Procedures for periodic review, evaluation and evaluation of the effectiveness of technical and organisational measures

An annual review (at the beginning of a calendar year, documented by the IT team) of the effectiveness of the technical and organizational measures taken is part of the operating concept. The sites will be informed about the review and the result of the review. The following aspects are examined and, if necessary, Measures taken:

- Release statuses of the operating systems and application software used, including checking whether patches have been installed regularly
- Use of firewall and virus protection update procedures
- Evaluation of security incidents and incidents
- Do the measures still correspond to the state of the art (in particular developments regarding encryption technologies, etc.)
- Effectiveness of the backup procedures (recovery test if necessary)
- Training of persons entrusted with data processing

Local regulations apply in each of the local DWHs.

2.10. Written documentation of other measures

For the computer center of the RWTH Aachen University Hospital, there are various technical and process-oriented documentations that ensure state-of-the-art operation at the level of the technical infrastructure.

Local regulations apply in each of the local DWHs.

3. Rights of data subjects

3.1. Fulfilment of the obligation to provide information pursuant to Art. 13/14 GDPR

Article 14 GDPR applies to the collection of personal data. In accordance with Article 14 (1) and (2) GDPR, necessary information will be made available to the public on the project's website.

3.2. Fulfilment of the obligation to provide information pursuant to Art. 15 GDPR

Data subjects have the right to request information as to whether personal data concerning them is being processed. De-identified data is processed within the AKTIN infrastructure.

The request for data information can only be made via the respective location, as only the respective hospital has access to identifying data. If data subjects contact the AKTIN Office directly, they will receive the information in accordance with Art. 13 or 14 GDPR and will be referred to the respective hospital (e.g. categories of data, legal basis, contact details).

Negative information (if no processing has taken place in the project) is returned directly to the data subject. Further communication between the project partners is then not necessary.

3.3. Procedure in the event of objection pursuant to Art. 21 or deletion requests pursuant to Art. 17 GDPR

Data subjects may request the deletion of personal data concerning them. Since the scientific research purpose would not be "impossible or seriously impaired" by the expected small number of deletions or objections (Art. 17 para. 3 lit. d GDPR), the right of objection under Art. 17 or Art. 21 GDPR remains in place for the data subjects.

The request for deletion or objection should be made via the respective location, as only the respective hospital has access to identifying data. If those affected contact the AKTIN Office directly, they will be referred to the respective hospital. The exclusion of patients is documented in the AKTIN Consent Manager.

Negative information (if the person is not affected or the assignment is no longer possible) is returned directly to the person concerned. Further communication between the project partners is then not necessary. For data extracts that have already been created, it is not possible to identify data subjects, Articles 15 to 20 GDPR do not apply here.

3.3.1. Consequences of objection or deletion requests

An objection leads to the deletion[2] or blocking (for external data processing) of the patient's medical data stored in the local AKTIN-DWH in accordance with and by the respective hospital. Blocking (for external data processing) by the respective hospital is necessary if the objection

[2] The necessary SQL syntax can be requested by the AKTIN IT team.

affects data processing for purposes and legal bases outside the regulatory competence of the AKTIN Emergency Department Data Registry (e.g. general documentation and retention obligations, quality assurance purposes).

3.4. Responsibility for the implementation of the rights of data subjects

The location assumes responsibility for the fulfilment of the rights of the data subject within the meaning of Art. 26 GDPR. The project partners involved are obliged to participate in the provision of information in accordance with the process defined here.

3.5. Data deletion

Data transmissions and collections have been taking place since 2015. The deletion and retention periods in accordance with the legal requirements at the respective location apply.

Data merged for queries will be deleted (1) once a researcher (or the evaluation agency) has retrieved the collected data; or (2) if there has been no interaction with the researcher or TDAC within 90 days. The deletion cannot be postponed or prevented by the researcher. When deleted, the query ID and ticket number are still retained and marked as deleted. All other related data will be deleted. If further query results from locations are delivered after the deletion, they will be deleted immediately. For the evaluation period of (possibly completely anonymous) data by the researchers, deletion periods apply in accordance with the requirements of the DUAC and .[3]

4. Agreement on joint responsibility and entry into force

The present data protection concept was reviewed by all project managers of the project members who are involved in the data processing process. This data protection concept regulates the cooperation and the delimitation of responsibility between the data processing bodies in the sense of joint data processing agreement in accordance with Art. 26 GDPR. The data protection concept and the implicit obligations are recognized by participation in the AKTIN infrastructure or the AKTIN Emergency Department Data Registry. An explicit contract may also be entered into between the parties, which will then be deemed to be such an agreement instead.

5. Grounds

Appendix 1 – Study Centers

Appendix 2 – Contact Data Protection

Appendix 3 – Dataset description Dataset Emergency Department Data Registry V2015.2

Annex 4 – Ethics vote

Appendix 5 – Rules of Procedure DUAC in the currently valid version

Appendix 6 – Publication Regulations for the AKTIN Emergency Department Data Registry in the currently valid version

Appendix 7 – Basic Module Emergency Department Protocol V2015.2

Appendix 8 – Inpatient Treatment Data Record

6. Literature

[1] K. Pommerening, J. Drepper, K. Helbing, T. Ganslandt, *Guidelines for Data Protection in Medical Research Projects: Generic Solutions of 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, Core Data Set "Emergency Department" of the DIVI. **17** (2014), 671–681.

[3] German Research Foundation, 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.