DATENSCHUTZKONZEPT

zum Deutschen Reanimationsregister

VERSION 1.1 (25.06.2019)

1. Ziele und Strukturen des Projekts

Das „Deutsche Reanimationsregister" ist die größte überregionale Datenbank für die Erfassung von Reanimationsmaßnahmen. Zur Erfassung und zur Analyse sowohl im Rettungsdienst als auch in der Klinik durchgeführten Reanimationen wurde im Mai 2007 das Deutsche Reanimationsregister durch die Deutsche Gesellschaft für Anästhesiologie und Intensivmedizin e.V. (DGAI) gegründet. Das primäre Ziel des Deutschen Reanimationsregisters ist die Datenbereitstellung für das lokale, regionale und überregionale Qualitätsmanagement im Rettungs- und Notarztdienst, sowie in der innerklinischen Notfallversorgung.

Die Daten sollen einerseits für wissenschaftliche Zwecke anonymisiert aufgearbeitet werden und andererseits für die Qualitätssicherung für die einzelnen Rettungsdienste und Kliniken verwendet werden.

Die Teilnahme am Deutschen Reanimationsregister ist freiwillig.

In den jeweiligen teilnehmenden Standorten werden Patienten eingeschlossen, welche präklinisch reanimiert wurden oder innerklinisch eine Notfallversorgung erhalten haben. Da die Daten ausschließlich anonymisiert in die Online-Datenbank eingegeben werden können, werden die Patienten nicht aufgeklärt.

2. Einordnung der Datenerhebung

Es handelt sich um ein klinisches Modul im Sinne der Definition der AG Datenschutz der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) (s. Leitfaden zum Datenschutz in medizinischen Forschungsprojekten), bei der eine direkte Eingabe der Daten in eine elektronische Online-Datenbank erfolgt.

3. Verantwortung und Partner

Juristische Verantwortung

Juristische Person und Träger ist die Deutsche Gesellschaft für Anästhesiologie und Intensivmedizin e.V. (DGAI).

Die Verträge zur Datenverarbeitung im Auftrag und mit den teilnehmenden Standorten werden durch die DGAI geschlossen. Sollte es zur Kündigung des Kooperationsvertrags kommen, verbleiben die bisherigen, eingegebenen anonymisierten Daten in der Datenbank.

Projektpartner und Dienstleister
Auswertung der Daten erfolgt durch:

Das Organisationskomitee des Deutschen Reanimationsregisters
Sprecher: Prof. Dr. Jan-Thorsten Gräsner
Institut für Rettungs- und Notfallmedizin
Direktor: Prof. Dr. Jan-Thorsten Gräsner
Universitätsklinikum Schleswig-Holstein
Arnold-Heller-Straße 3 – Haus 808 – 24105 Kiel
Besucheradresse: Holzkoppelweg 8-12 – 24118 Kiel
Tel.: +49 (0) 431 500 31500

Die Realisierung der online-Datenbank mit Eingabemaske, Datenpflege, Rechtemanagement, Benchmarking und Export erfolgt durch:

Visionet GmbH
Karolinenstr. 52b
D - 90763 Fürth
Tel.: 0911/148894-0
Fax: 0911/148894-99
info@visionet.de
Geschäftsführer: Stefan Lindner
Ansprechpartner dort ist Herr Dietrich Streifert
Die Firma Visionet GmbH wird durch die DGAI als juristisch verantwortliche Person des Registers vertraglich beauftragt (Datenverarbeitung im Auftrag).

Datenübermittlung
Im Falle einer gewünschten wissenschaftlichen oder anders begründeten Auswertung können durch die beteiligten Kliniken Anträge an den Wissenschaftlichen Beirat zur Auswertung gestellt werden (s. Workflow: Wissenschaftliche Auswertung). Die Kontaktaufnahme kann über die Deutsche Gesellschaft für Anästhesiologie und Intensivmedizin e.V. (DGAI), über das Organisationskomitee des Deutschen Reanimationsregisters (OK) oder über die Koordination des Deutschen Reanimationsregisters (KoRe) erfolgen. Die Anfragen werden an KoRe zur weiteren Bearbeitung weitergeleitet. Nachdem ein Aktenzeichen vergeben wurde, wird der Antrag von KoRe an den Wissenschaftlichen Beirat weitergeleitet, welcher nun 10 Tage Zeit hat zu prüfen. Nach Ablauf der Frist wird das OK informiert und ein Ansprechpartner wird benannt. Die Bereitstellung der angefragten Daten wird durch den Ansprechpartner im OK oder KoRe durchgeführt. Nach dem Datentransfer muss der Antragstellende die Auswertung vom Ansprechpartner gegenlesen lassen. Je nach Review wird der Prozess zwischen Antragsteller und Ansprechpartner wiederholt oder das OK und der Wissenschaftliche Beirat erhalten das fertige Dokument.

Die Ausgabe der Rohdaten an einen Standort ist nicht geplant. Der jeweilige Standort hat jedoch immer Zugriff auf die Rohdaten, welche vom Standort selbst eingegeben worden sind, und kann diese ohne Anfrage verwenden. Sollte zukünftige eine andere Art der Auswertung und Datenübermittlung geplant werden, kann dies lediglich nach Absprache mit dem Datenschutzbeauftragten und dem Träger des Registers (DGAI) erfolgen.

Datenschutzbeauftragter des Registers
Ein Datenschutzbeauftragter gemäß Art. 37, EU-DSGVO wurde von der DGAI bestellt.

Kontaktdaten des Datenschutzbeauftragten:
Herr Thomas Fahrmayr
MCN Medizinische Congressorganisation Nürnberg AG
Neuwieder Str. 9
90411 Nürnberg
datenschutz@dgai-ev.de

Datenschutz der teilnehmenden Standorte
Die am Deutschen Reanimationsregister teilnehmenden Standorte müssen die erfassten Patientendaten, welche insbesondere mit den Dokumentationsprotokollen des Deutschen Reanimationsregisters aufgenommen werden, nach den jeweils Standortinternen datenschutzrechtlichen Vorgaben gemäß der geltenden DSGVO sicher und vertraulich verarbeiten. Gerade im Bereich der innerklinischen Notfallversorgung sind die patientenbezogenen Daten nach internen datenschutzrechtlichen Vorgaben gemäß der DSGVO aufzubewahren.

4. Rechtliche Grundlagen der Datennutzung
Nach der bisherigen gutachterlichen Bewertung (s. Anhang Datenschutzrechtliches Gutachten zum Reanimationsregister) fällt die Datenverarbeitung durch das Reanimationsregister der DGAI nicht unter den Anwendungsbereich der datenschutzrechtlichen Normen. Dies deshalb, da die in den einzelnen Modulen erhobenen Daten der Patienten weder isoliert noch in der Zusammenschau eine Bestimmung des betroffenen Patienten ermöglichen. Die Daten sind derart verändert („anonymisiert"), dass ein Rückschluss auf die einzelne Person nicht mehr möglich ist. Auch das aktuelle Gutachten (s. Anhang Gutachten Reanimationsregister und Thoraxregister) sieht die Anonymisierung und zeigt aus diesem Grund eine Nicht-Anwendung der DSGVO. Da es sich um ein bundesweites Register handelt, ist eine übergreifende Regelung in den Landesdatenschutzgesetzen nicht vorhanden.

5. Datenfluss
Datenerfassung - Präklinik
Die Datenerfassung erfolgt zunächst auf dem Registerbogen schriftlich (s. Anhang Erstversorgung). Bei den Daten handelt es sich um Informationen über die Reanimationsbehandlung, der Vermuteten Ursache, der Einsatzzeiten und des Einsatzortes, der Kernmaßnahmen und Ablauf der Reanimationsbehandlung sowie Informationen über das primäre Reanimationsergebnis. Es gibt keine Patientenspezifischen Informationen, außer dem Einsatzdatum und dem Geburtsdatum des Patienten. Das Geburtsdatum wird jedoch in der Online-Datenbank automatisch auf den 01. des Geburtsmonats abgerundet. Dementsprechend werden die Daten nach der Papierprotokoll-Erfassung in anonymisierter Form in die Online Datenbank eingegeben. Die Patientenidentifikation wird dabei von der Datenbank generiert und wird auf dem Papierprotokoll notiert. Das Papierprotokoll verbleit beim Rettungsdienststandort und wird dort aufbewahrt. Anhand des Einsatzdatums und der Patientenidentifikation kann somit nur der Standort auf den Einsatz zurückgreifen.

Datenerfassung – Klinik

Die Dokumentation erfolgt auch hierbei zunächst schriftlich auf dem Registerbogen (s. Anhang Dokumentation Notfallteam).

Bei den Daten handelt es sich nicht generell um Reanimationsmaßnahmen, sondern auch um Maßnahmen im Rahmen einer Notfallbehandlung. Dazu werden die Einsatzzeiten, Alarmierungsgrund und Einsatzort abgefragt. Auch werden Daten zur Krankenhausbehandlung, Erstbefund bei Eintreffen am Notfallpatienten, Maßnahmen und Verlauf der Behandlung und Übergabe dokumentiert. Im Anschluss werden die Daten manuell in die Datenbank des Deutschen Reanimationsregisters eingegeben. Es gibt keine Patientenspezifischen Informationen, außer dem Einsatzdatum und dem Geburtsdatum des Patienten. Das Geburtsdatum wird jedoch in der Online-Datenbank automatisch auf den 01. des Geburtsmonats abgerundet. Dementsprechend werden die Daten nach der Papierprotokoll-Erfassung in anonymisierter Form in die Online Datenbank eingegeben. Die Patientenidentifikation wird dabei von der Datenbank generiert und wird auf dem Papierprotokoll notiert. Das Papierprotokoll verbleit in der Klinik und wird dort aufbewahrt. Anhand des Einsatzdatums und der Patientenidentifikation kann somit nur der Standort auf den Einsatz zurückgreifen.

Datenerfassung – Cardiac Arrest Center

Die Dokumentation erfolgt auch hierbei zunächst schriftlich auf dem Registerbogen (s. Anhang Cardiac Arrest Center Datensatz).

Bei den Daten handelt es sich um die weiterversorgende Behandlung von innerklinisch oder präklinisch reanimierten Patienten. Die erfassten Daten beinhalten den Aufnahmestatus, die innerklinischen Maßnahmen, erweiterte Maßnahmen wie die eCPR und das Temperaturmanagement und schließen mit dem Ergebnis und den neuroprognostischen Tests ab.

Im Anschluss an die Papier-Dokumentation werden die Daten manuell in die Datenbank des Deutschen Reanimationsregisters eingegeben. Es gibt keine Patientenspezifischen Informationen, außer dem Einsatzdatum und dem Geburt datum des Patienten. Das Geburtsdatum wird jedoch in der Online- Datenbank automatisch auf den 01. des Geburtsmonats abgerundet. Dementsprechend werden die Daten nach der Papierprotokoll-Erfassung in anonymisierter Form in die Online Datenbank eingegeben. Die Patientenidentifikation wird dabei von der Datenbank generiert und wird auf dem Papierprotokoll notiert. Das Papierprotokoll verbleit in der Klinik und wird dort aufbewahrt. Anhand des Einsatzdatums und der Patientenidentifikation kann somit der nur Standort auf den Einsatz zurückgreifen.

Der Inhaber der jeweiligen Daten ist somit jeweils der Rettungsdienst bzw. die Klinik und wird dort nach den gültigen internen datenschutzrechtlichen Regelungen und der DSGVO aufbewahrt.

Weiterleitung / Zugriffsregelungen

Es werden keine Patientendaten weitergeleitet, auch nicht pseudo- oder anonymisierte Daten.
Die Zugriffsregelung erfolgt durch ein Rollenmanagement der Online-Datenbank:

- **Systemadministrator**
  Berechtigung zur systemweiten Auswertung. Export aller Datensätze. Erstellen von Standorten und Benutzern. Zuweisen von Rollen eines Benutzers bzgl. aller Standorte. Die Rolle Systemadministrator kann für die Pflege und Administration die Kontaktdaten der einzelnen Benutzer, welche durch die Standortverantwortlichen der Standorte angelegt wurden, einsehen.
- **Standortverantwortlicher (Administrator des Standorts/Clusters):**
  Fälle lesen. Fälle erstellen und ändern. Fälle freigeben. Fälle auswerten. Fälle exportieren. Der Standortverantwortliche kann des Weiteren nach interner Zustimmung des anzulegenden Benutzers, die Benutzer für seinen Standort anlegen und verwalten.
- **Notarzt:**
  Eigene Fälle lesen. Eigene Fälle erstellen und ändern. Fälle auswerten. Fälle exportieren.
- **Auswerter:**
  Fälle lesen. Fälle auswerten. Fälle exportieren.
- **Fallbearbeiter:**
  Eigene Fälle lesen. Fälle des Standortes erstellen und ändern. Kann keine Fälle freigeben/auswerten/exportieren.
- **Importer:**
  Eigene Fälle lesen. Fälle auswerten. Fälle exportieren.
- **Freigeber:**
  Eigene Fälle lesen. Eigene Fälle erstellen und ändern. Fälle freigeben.
- **Falleingabe:**
  Eigene Fälle lesen. Eigene Fälle erstellen und ändern.

Berechtigung zur Eingabe von Datensätzen der zugewiesenen Standorte. Freigabe der eigenen Datensätze für die Auswertung.

- **Systemadministration (KoRe):**
  Berechtigung für Auswertung und Export der Datensätze der zugewiesenen Standorte.
- **Standort:**
  Ein Zentrum wird definiert durch eine eindeutige Standort-Identifikation sowie Standortname und Adresse.
- **Benutzer:**
  Ein Benutzer wird definiert durch Benutzername, E-Mail-Adresse sowie Vorname, Nachname, Titel. Es erfolgt initial die Vergabe eines Passworts für den Benutzer. Das Passwort ist durch den Benutzer änderbar. Der Standortverantwortliche legt die Benutzer und deren Daten mit expliziter Zustimmung des Benutzers an.

6. Datenübermittlung zwischen Modulen

In der präklinischen Datenerfassung kann als Alternative zur Papierprotokollerfassung eine Datenübertragung über eine Schnittstelle mittels Exports in die Datenbank genutzt werden. Die Schnittstelle durchläuft einen Prozess mit technischer sowie medizinischer Zertifizierung und darf erst nach erfolgreicher Prüfung aktiv geschalten werden. In Zukunft wird eine regelmäßige Re-Zertifizierung angestrebt.

7. Technische Sicherheitsmaßnahmen

Der Betrieb der Datenbank erfolgt auf Servern (Rootserver), die ausschließlich für die Betreiber Berufsverband Deutscher Anästhesisten e.V. (BDA) und Deutsche Gesellschaft für Anästhesiologie und Intensivmedizin e.V. (DGAI) zur Verfügung steht.

Die Administration der Server und des Betriebssystems erfolgt durch die Wartungsfirma Visionet GmbH, welche mit einem Auftragsdatenverarbeitungsvertrag (kurz ADV) gemäß DSGVO verpflichtet wurde. Administrative Zugangsdaten zum Betriebssystem liegen den Betreibern BDA und DGAI vor. Die Serverhardware befindet sich in den Rechenzentren des Rechenzentrumsbetreibers Hetzner Online AG in Nürnberg oder Falkenstein in Deutschland. Der Betrieb ist durch Auslegung redundanter Server, redundanter Internetverbindungen über mehrere deutsche Austauschknoten (u.a. DE-CIX) und redundanter USV-Anlagen gesichert. Der gesicherte Zutritt zu den Serverräumen erfolgt videoüberwacht durch ein elektronisches Zutrittskontrollsystem mit Protokollierung. Die Zutrittsschlüsselvergabe an Mitarbeiter und Kunden wird protokolliert.

https://www.hetzner.de/pdf/ADV_TOM.pdf
https://www.hetzner.de/hosting/unternehmen/rechenzentrum/

IT-Grundschutz

Die Server sind gegen Attacken durch den Betrieb einer allgemeinen Firewall, einer Web Application Firewall, eines Intrusion Prevention Systems und einer Virenscannersoftware gesichert. Es erfolgt zeitnah eine Installation sicherheitsrelevanter Patches für das Betriebssystem und die darauf installierte Software. Die Fernwartung erfolgt über gesicherte Verbindungen per Netzwerkprotokoll SSH.

Verschlüsselte Übertragung

Der Zugriff durch die Anwender und Datenmanager erfolgt per Browser über eine gesicherte Verbindung (https). Es wird das Verschlüsselungsprotokoll TLS 1.2 verwendet. Das für das Verschlüsselungsprotokoll eingesetzte Zertifikat ist durch eine anerkannte Zertifizierungsstelle ausgestellt.

8. Datenminimierung / Löschen von personenbezogenen Daten

Ein erforderliches Löschkonzept gemäß DSGVO liegt vor und kann ggf. eingesehen werden.