Fragen (und Antworten) zum Datenschutzkonzept AKTIN

1. **Was bedeutet *mehrstufiges Anonymisierungsverfahren* im Notaufnahmeregister?**

   Die Daten im AKTIN-Notaufnahmeregister durchlaufen ein mehrstufiges Anonymisierungsverfahren bestehend aus verschiedenen technischen und organisatorischen Maßnahmen. Die Daten werden lokal einweg-pseudonymisiert gesammelt und anonymisiert abgefragt. Sowohl in der Datenabfrage als auch in der darauffolgenden Aufbereitung durch das Trusted Data Analyzing Center wird die k-Anonymität der Daten durch Datenreduktion/-vergröberung und der Zusammenführung von Fällen aus mehreren Kliniken sukzessive erhöht, bevor die Daten dann für wissenschaftliche Auswertungen an Forscher*innen weitergegeben werden. Zur Datenreduktion gehört z. B. die Ersetzung des Geburtsdatums durch das berechnete Alter der Patient*innen.

2. **Wo und in welchen Arbeitsschritten wird die *k-Anonymität* der Daten im Notaufnahmeregister erhöht**?

   Die k-Anonymität der Daten im AKTIN-Notaufnahmeregister wird zu verschiedenen Zeitpunkten und in verschiedenen Arbeitsschritten sukzessive erhöht. Die lokale Verarbeitung von Daten im Verantwortungsbereich der teilnehmenden Kliniken findet einweg-pseudonymisiert statt. Für wissenschaftliche Auswertungen können die Daten gemäß der Maßgaben des Data Use and Access Committee und nach Zustimmung der lokalen Verantwortlichen der jeweiligen Klinik abgefragt werden. Bei einer solchen Datenabfrage werden die Daten durch Entfernen aller identifizierenden Daten wie z.B. einweg-pseudonymisierte IDs anonymisiert. In den Datenabfragen (SQL Syntax) – d.h. noch lokal in den Kliniken – wird eine Datenreduktion umgesetzt. Die Prüfung der Abfrage findet lokal statt, bevor die abgefragten Daten zentral im AKTIN Broker gesammelt werden. Anonyme Daten von verschiedenen Standorten werden extern aggregiert; es kann so ggf. die k-Anonymität durch Zusammenführung von Fällen aus mehreren Kliniken erhöht werden. Anschließend werden die Daten inhaltlich vom Trusted Data Analyzing Center

aufbereitet (TDAC). Das TDAC prüft auf k-Anonymität bzw. l-Diversität und führt ggf. eine weitere Datenreduktion und Datenaggregation durch. Die anonymisierten Daten können dann für wissenschaftliche Auswertungen an Forscher*innen weitergegeben werden.

3. Wer ist verantwortlich für die Entscheidung über die *Datenbereitstellung* in den Notaufnahmen?

Standortkoordinatoren*innen sind verantwortlich für die Entscheidung über die Datenbereitstellung in den Notaufnahmen. Diese Standortkoordinatoren*innen werden vom Standort (der Klinik) 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.

4. Ist der *Zugriff* auf personenbezogene Daten nur in der zugehörigen Notaufnahme möglich?

Das lokale Datawarehouse (DWH) sollte grundsätzlich so konfiguriert werden, dass nur in der zugehörigen Notaufnahme bzw. im zugehörigen Klinikum zugegriffen werden kann. Die entsprechenden Firewall-Einstellungen müssen vom Standort umgesetzt werden. Der Zugriff auf die Benutzeroberflächen der AKTIN-DWH-Software ist an ein Rechte- und Rollenkonzept mit Zugriffsrechten gebunden. Im DWH werden nur einweg-pseudonymisierte Daten gespeichert. Die Mitarbeiter der Notaufnahme haben keinen direkten Zugriff auf diese Pseudonyme. Einzig der Datenbank-Administrator kann die Pseudonyme technisch bedingt einsehen. Eine direkte Zuordnung der Daten zu Patienten*innen ist nicht möglich.

5. **Wie wird sichergestellt, dass nur zuständige Mitarbeiter*innen Zugriff auf die Daten haben?**

   Ein Rechte- und Rollenkonzept mit Zugriffsrechten ist in der AKTIN-DWH-Software integriert. Mitarbeiter*innen haben nur mit persönlichen Account und zugehörigen Passwort Zugriff. Accounts (und somit Kriterien für die Authentifizierung) werden von den Standorten selbst verwaltet. Automatische Schutzmaßnahmen bei Passwörtern wie Mindestanforderungen an Inhalt und Länge, Aktualisierungen und Sperren bei falschen Logins werden in einer neuen Version der AKTIN DWH Software umgesetzt.

6. **Welche Informationen werden den Betroffenen bereitgestellt und wie haben diese Zugriff darauf?**

   Das AKTIN-Notaufnahmeregister stellt den Kliniken alle notwendigen Informationen zur AKTIN-Infrastruktur (technische Dokumente, Datenschutzkonzept, Satzung, Publikations- und Geschäftsordnungen) zur Verfügung. Die Information der Patient*innen ist individuell von den Kliniken zu erstellen und an die erforderlichen formalen Grundlagen jeder Klinik und jedes Bundeslandes anzupassen.

7. **Können Daten von Patienten*innen gelöscht werden, wenn diese durch Anonymisierung ja eigentlich nicht zurück verfolgbar sind?**

   Es werden einweg-pseudonymisierte Daten im lokalen Datawarehouse (DWH), d.h. innerhalb der Notaufnahme gespeichert. Eine direkte Zuordnung dieser Daten zu Patienten*innen ist nicht möglich. Der Widerspruch eines Patienten*in kann im AKTIN Consent Manager mittels Fall- oder Patientennummer registriert und die Daten des Patienten*in anschließend per SQL Syntax gelöscht werden. Das AKTIN IT Team stellt eine entsprechende Syntax zur Verfügung. Eine automatisierte Löschfunktion wird in einer neuen Version der AKTIN DWH Software umgesetzt.
   Anonymisierte Daten, die im Trusted Data Analyzing Center oder für die Auswertung bei Forscher*innen vorliegen, können nicht mehr gelöscht werden, da eine Zuordnung nicht mehr möglich ist.

8. **Wann und wie erfolgt die Löschung von personenbezogenen Daten im Notaufnahmeregister?**

   Die lokale Verarbeitung von Daten findet im Versorgungskontext und im Verantwortungsbereich der teilnehmenden Kliniken statt. Eine Löschung von personenbezogenen Daten erfolgt dementsprechend nach Maßgabe des Hauses. Momentan können Daten per SQL Syntax aus den Datenbanken gelöscht werden. Das AKTIN IT Team stellt eine entsprechende Syntax zur Verfügung. Eine automatisierte Löschfunktion (nach konfigurierbaren Zeitraum) wird in einer neuen Version der AKTIN DWH Software umgesetzt.
   Anonymisierte Daten die im Trusted Data Analyzing Center oder für die Auswertung bei Forscher*innen vorliegen können nicht mehr gelöscht werden, da eine Zuordnung nicht mehr möglich ist.

9. **Wer stellt anhand welcher Kriterien fest, welche Forscher*innen Datenauszüge beantragen können?**

   Für wissenschaftliche Auswertungen können Daten nur gemäß der Maßgaben des Data Use and Access Committee (DUAC) bei den teilnehmenden Kliniken von externen Forscher*innen angefragt werden. Forscher*innen müssen nicht einem Standort oder Projekt angehören. Das DUAC stellt fest bzw. kontrolliert, wer ein geeignete/r Forscher*in ist.
   Die im lokalen Datawarehouse gespeicherten Daten befinden sich grundsätzlich im Besitz der jeweiligen Institution. Für standortbezogene Forscher*innen, d.h. solchen, die im Standort beschäftigt werden, gelten demnach die Maßgaben des Standortes.

10. **Welche Grundlagen für eine Datenweitergabe an Forscher*innen in sog. Auswertestellen gibt es?**

    In besonderen Fällen (z. B. bei periodischen Abfragen im Rahmen von Infektionssurveillance) kann eine Weitergabe von anonymisierten Rohdaten an Forscher*innen eingerichtet werden, wenn dies zuvor vom Data Use and Access

Committee (DUAC) genehmigt wurde und entweder eine hinreichende Anonymisierung 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. Es gelten die Maßgaben des DUAC.

11. Wird ein Vertrag zur Auftragsverarbeitung mit AKTIN e.V. oder mit der RWTH Aachen geschlossen?

Es wird angestrebt, Verträge zur Auftragsverarbeitung zwischen RWTH Aachen und den beteiligten Standorten zu schließen. Die genaue Ausgestaltung befindet sich in Klärung.

12. Was bedeutet Zuordnungslisten im Hinblick auf die Vertraulichkeit des Search Brokers? Wer hat Zugang zu diesen Listen?

Es werden nur einweg-pseudonymisierte Daten im lokalen Datawarehouse gespeichert. Eine direkte Zuordnung dieser Daten zu Patienten*innen ist nicht möglich. Es gibt somit keine Zuordnungslisten (bei den im Datenschutzkonzept Version 2.0 vom 24.08.2020 unter Punkt 2.4. erwähnten Zuordnungslisten handelt es sich um einen Fehler, der in der neuen Version des Datenschutzkonzepts Version 2.1 vom 24.09.2020 korrigiert wurde).