Fragen (und Antworten) zum Datenschutzkonzept AKTIN

FAQ

1. Was heißt mehrstufiges Anonymisierungsverfahren (k-Anonymisierung) im Notaufnahmeregister? Punkt 1.3/ 1.7.1

Die Daten im AKTIN-Notaufnahmeregister durchlaufen ein mehrstufiges Anonymisierungsverfahren. Die Daten werden lokal einwegpseudonymisiert 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 und Zunahme von Fällen sukzessive erhöht.

2. Wann (zu welchem Zeitpunkt/ Arbeitsschritte) und wo (intern/ extern) wird die k-Anonymisierung durchgeführt? Punkt 2

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 einwegpseudonymisiert statt. Für wissenschaftliche Auswertungen können die Daten gemäß der Maßgaben des Data Use and Access Committee und nach Zustimmung der lokale Verantwortlichen der jeweiligen Klinik abgefragt werden. Bei einer solchen Datenabfrage werden die Daten durch entfernen aller identifizierenden Daten wie z.B. einwegpseudonymisierte 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 Zunahme von Fällen erhöht werden. Anschließend werden die Daten inhaltlich vom Trusted Data Analyzing Center aufbereitet. Das TDAC prüft auf K-Anonymität bzw. I-Diversität und führt ggf. eine weitere Datenreduktion und Datenaggregation durch. Die anonymisierten Daten können dann für wissenschaftliche Auswertungen an Forscher weitergegeben werden.

3. Wie genau wird die Anonymität erzeugt?

Die Daten im AKTIN-Notaufnahmeregister durchlaufen ein mehrstufiges Anonymisierungsverfahren. Für wissenschaftliche Auswertungen können Daten gemäß der Maßgaben des Data Use and Access Committee und nach Zustimmung der lokale Verantwortliche der jeweiligen Klinik abgefragt werden. Bei einer solchen Datenabfrage werden die Daten durch entfernen aller identifizierenden Daten wie z.B. einwegpseudonymisierter IDs anonymisiert. Eine zusätzliche Datenreduktion und Datenaggregation wird in den Abfragen selbst und in der anschließenden Aufarbeitung durch das Trusted Data Analyzing Center umgesetzt, bevor die Daten dann für wissenschaftliche Auswertungen an Forscher weitergegeben werden.

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

Es werden nur einwegpseudonymisierte Daten im lokalen Datawarehouse (DWH) gespeichert. Eine direkte Zuordnung dieser Daten zu Patienten*innen ist nicht möglich. Auf das DWH kann grundsätzlich nur in der zugehörigen Notaufnahme bzw. im zugehörigen Klinikum zugegriffen werden.

5. Wer ist verantwortlich für die Entscheidung über die Datenbereitstellung in den Notaufnahmen? Punkt 1.7.2

Standortkoordinatoren*innen sind verantwortlich für die Entscheidung über die Datenbereitstellung in den Notaufnahmen. 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.

6. Wie wird sicher gestellt das nur zuständige Mitarbeiter Zugriff auf die Daten haben? Stichwort: Kriterien für die Authentifizierung

Ein Rechte- und Rollenkonzept mit Zugriffsrechten ist im AKTIN Datawarehouse (DWH) integriert. Mitarbeiter 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.

7. Vertrag zur Auftragsverarbeitung mit AKTIN e.V. oder RWTH Aachen? Punkt 1.3 / 2.2.1

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

8. Was werden den Patienten für Informationen bereitgestellt und wo werden diese bereitgestellt? Punkt 1.7.2 / 3.1

Ein Musterentwurf der Patienteninformation stellt AKTIN zur Verfügung. Der Klinik obliegt die Verantwortung den Patienten Informationen in der Notaufnahme und im Behandlungsvertrag bereitzustellen. Nach Gründung werden Flyer vom AKTIN e.V. zur Verfügung gestellt.

9. Können Daten von Patienten gelöscht werden, wenn diese durch Anonymisierung ja eigentlich nicht zurück verfolgbar sind, oder Löschung nur innerhalb des KIS?

Es werden einwegpseudonymisierte 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 kann im AKTIN Consent Manager mittels Fall- oder Patientennummer registriert und die Daten des Patienten anschließend durch das AKTIN IT Team gelöscht werden. Eine

automatisierte Löschfunktion wird in einer neuen Version der AKTIN DWH Software umgesetzt.
Annonymisierte Daten die im Trusted Data Analyzing Center oder für die Auswertung bei Forschern vorliegen können nicht mehr gelöscht werden, da eine Zuordnung nicht mehr möglich ist.

10. Wann/ Wie /Durch wem erfolgt die Löschung von Patientendaten?

Eine Löschung von Patientendaten erfolgt nach Maßgabe des Hauses. Momentan können Daten per SQL Syntax aus den Datenbanken gelöscht werden. Eine automatisierte Löschfunktion (nach konfigurierbaren Zeitraum) wird in einer neuen Version der AKTIN DWH Software umgesetzt.
Annonymisierte Daten die im Trusted Data Analyzing Center oder für die Auswertung bei Forschern vorliegen können nicht mehr gelöscht werden, da eine Zuordnung nicht mehr möglich ist.

11. Sind Forscher nur projektbezogene / standortbezogene Forscher? Punkt 2.1.7

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

12. Welche anderen Grundlagen, für eine direkte Datenübertragung, 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.

13. Was bedeutet Zuordnungslisten im Hinblick auf die Vertraulichkeit des Search Brokers? Wer hat zu diesen „genau“ und warum Zugang? Punkt 2.4

Hierbei handelt es sich um einen Fehler im Datenschutzkonzept Version 2.0 vom 24.08.2020. Es werden nur einwegpseudonymisierte Daten im lokalen Datawarehouse gespeichert. Eine direkte Zuordnung dieser Daten zu Patienten*innen ist nicht möglich. Es gibt somit keine Zuordnungslisten.

14. Wieso ist eine Speicherung der Daten im lokalen Datawarehouse rechtlich vertretbar?

Die pseudonyme Haltung von Daten innerhalb der Kliniken im Behandlungskontext zu Qualitätssicherungszwecken ist erlaubt. Gemäß Art. 9 DSGVO (2) lit. i. ist eine solche Datenhaltung in einem lokalen Datawarehouse gerechtfertigt, wenn dies „der Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung […]“ dient. Darüber hinaus werden angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen

Person, insbesondere des Berufsgeheimnisses eingehalten, da alle Daten innerhalb der patientenführenden Abteilung (i. d. R. Notaufnahme) verbleiben.

15. Auf welcher Rechtsgrundlage erfolgt die Datenweitergabe, an das TDAC?

Grundlage für die Weitergabe zu Forschungszwecken ist keine Einwilligung, sondern Forschungsklauseln und Anonymisierung. Gemäß Art. 9 DSGVO (2) lit. i. ist eine Datenweitergabe aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gerechtfertigt. Eine Weitergabe an Forscher*innen erfolgt ohnehin nur anonymisiert und fällt deshalb nicht unter die DSGVO.

16. Muss ein lokaler Ethikantrag für jede Forschungsanfrage von externen Forscher*innen gestellt werden?

Nein. Es wird ein Ethikvotum für den Betrieb des Systems an jedem Standort eingeholt. Ein Ethikantrag für Forschungsanfragen von externen Forscher*innen wird in der Regel von den externen Forscher*innen selbst eingeholt; externe Forscher*innen erhalten allerdings nur anonymisierte Daten. Für eigene Forschungsanfragen muss ggf. ein eigener Ethikantrag gestellt werden. Es gilt die Publikationsordnung des AKTIN-Notaufnahmeregisters.

17. Wie häufig kommen kommt es zu Datenanfragen?

Erfahrungsgemäß werden pro Monat in etwa 1 bis 4 Abfragen an die teilnehmenden Notaufnahmen verschickt, die bestätigt werden müssen. Es gibt einmalige Abfragen und Serienabfragen. Serienabfragen müssen nur einmal bestätigt werden und werden dann automatisiert in vordefinierten Zeitabständen durchgeführt.

18. Gibt es eine allgemeingültige Methodik der Anonymisierung für alle Standorte?

Die Daten im AKTIN-Notaufnahmeregister durchlaufen ein mehrstufiges Anonymisierungsverfahren. Für wissenschaftliche Auswertungen werden die Daten gemäß der Maßgaben des Data Use and Access Committee vom TDAC durch Aggregation und Datenreduktion anonymisiert. Das genaue Verfahren ist immer von der Forschungsfrage abhängig. Es gilt das Prinzip der Datensparsamkeit.

19. Wie werden die Daten pseudonymisiert?

Die Daten werden beim Import in das lokale DWH und vor der Speicherung in einer postgresql Datenbank pseudonymisiert. Es werden identifizierende Inhalte wie Namen und Adresse entfernt und Einwegpseudonyme von Patienten, Fall- und Encounternummer berechnet. Dazu wird base64 Kodierung und SHA1 verwendet.

20. Was sind die Folgen eines Widerrufs durch Patienten*innen?

Betroffene können eine Löschung der sie betreffenden personenbezogenen Daten verlangen. Ein Widerruf führt zu einer Löschung der im lokalen AKTIN DWH gespeicherten medizinischen Daten des/der Patienten*in durch den jeweiligen Standort.

21. Gibt es eine Datenschutz-Folgenabschätzung?

Eine Datenschutz-Folgenabschätzung soll in den Fällen, in denen eine Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, helfen, die Risiken zu minimieren und durch Darstellung der Maßnahmen zur Reduzierung der Risiken auch für Dritte nachvollziehbar aufzeigen, wie Verantwortliche für die Datenverarbeitung mit diesen Risiken umgehen. Eine solche (allgemeine) Darstellung sowie eine Risikobewertung ist bereits Teil des Datenschutzkonzepts (vgl. Kapitel 1.5. Anfallende Daten und Risikobewertung). Ggf. kann es notwendig sein, dass eine zusätzliche, explizite Datenschutz-Folgenabschätzung von einzelnen Datenschutzbeauftragten*innen verlangt wird. Bitte sprechen Sie Ihren/ihre lokale/n Datenschutzbeauftragen*in an.

22. Gibt es eine Vorlage für eine Datenschutz-Folgenabschätzung?

Wenn es in einer teilnehmenden Klinik zusätzlich notwendig ist eine Datenschutzfolgeabschätzung zu erstellen, so sollten die lokalen Vorlagen dafür genutzt werden. Liegen diese nicht vor, empfehlen wir die Vorlagen der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie. Diese finden Sie unter https://www.gesundheitsdatenschutz.org/html/dsfa.php.