UNIVERSITÄTS KLINIKUM jena

DATENSCHUTZKONZEPT

für projektbasierte Nutzung von Krankenversorgungsdaten in der biomedizinischen Forschung

Version: 1.0

Stand: 19.04.2021

UNIVERSITÄTS KLINIKUM Jena

Inhaltsverzeichnis

1 Einleitung

1.1 Hintergrund

Im Zuge der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung (2016–2026) [1] etablieren die Universitätsklinika in Deutschland neue Infrastrukturen und Verfahren für die Zusammenführung und Bereitstellung von patientenbezogenen Daten für deren Austausch und weitere Nutzung in biomedizinischen Forschungsprojekten. Das betrifft sowohl Versorgungsdaten, welche im Rahmen der Behandlung am UKJ oder anderen Gesundheitseinrichtungen erhoben bzw. verarbeitet werden, als auch Daten der klinischen Forschung, die für Projekte mit Beteiligung des UKJ oder seiner Partnereinrichtungen erhoben bzw. verarbeitet werden.

Das vorliegende Datenschutzkonzept dient als Rahmendokument für die datenschutzrechtliche Beurteilung solcher Tätigkeiten in sogenannten Datennutzungsprojekten. Die Verarbeitung personenbezogener Daten vor dem beschriebenen Hintergrund erfolgt dabei am UKJ im Datenintegrationszentrum (DIZ). Zweck des Datenschutzkonzepts ist es, dass in für jeweilige Datennutzungsprojekte zu verfassenden Datenschutzkonzepten und Datenschutzfolgeabschätzungen für die Grundprinzipien, Basisabläufe und generischen IT-Verfahren auf das vorliegende Dokument verwiesen werden kann. Die hier enthaltenen generischen Ausführungen sind dann für das jeweilige Datennutzungsprojekt zu konkretisieren.

1.2 Rahmenbedingungen und Vorlagen

Die Festlegungen und Inhalte im vorliegenden Datenschutzkonzept orientieren sich an zwei übergeordneten Dokumenten, die für die Verarbeitung personenbezogener Daten in beschriebenen Datennutzungsprojekten maßgeblich sind:

- Richtlinie zur Umsetzung der gesetzlichen Datenschutzanforderungen am UKJ, insbesondere Abschnitt 4.1.7 (Spezielle Hinweise zum Datenschutz für Forschende) [2]
- Datenschutzkonzept des SMITH-Konsortiums [3], in dessen Rahmen und Förderung die entsprechenden Verfahren am UKJ etabliert wurden

Struktur und Inhalte des Datenschutzkonzepts wurden außerdem mit Hilfe der folgenden Vorlagen und Empfehlungen erarbeitet:

- Leitfaden zum Datenschutz in medizinischen Forschungsprojekten der TMF e.V. [4]
- Vorlage Datenschutz- und IT-Sicherheitskonzept der unabhängigen Treuhandstelle der Universitätsmedizin Greifswald [5]
- Leitfaden für die Erstellung von Datenschutzkonzepten im Gesundheitswesen der GMDS-Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ und des ZTG [6]

2 Zweckbestimmung

Die übergeordneten Zwecke der datenverarbeitenden Verfahren im Rahmen von Datennutzungsprojekten sind:

- Verfügbarmachung von Inhalten der medizinischen Dokumentation aus den Primärsystemen des UKJ (Krankenhausinformationssystem, Patientendaten-managementsystem, Laborinformationssystem u.w.m.) für die Nutzung in standortbezogenen oder multizentrischen biomedizinischen Forschungsprojekten (Datennutzungsprojekten)
- Zusammenführung medizinischer Daten aus diesen und ggf. aus weiteren Datenquellen (z.B. zusätzliche Datenerfassungen im Rahmen konkreter Projekte oder Record Linkage z.B. mit Kostenträgerdaten) und Überführung in Interoperabilitätsstandards für einheitliche Persistenz, Kommunikation und Datenanalyse
- Datenspeicherung und Archivierung integrierter und interoperabler Datenformen im Rahmen der Krankenversorgung
- Rückführung von relevanten Ergebnissen aus Forschungsprojekten in die klinische Primärdokumentation und Versorgungsroutine

Zur Erfüllung dieser Aufgaben werden am Datenintegrationszentrum Jena in Zusammenarbeit mit dem Geschäftsbereich IT des UKJ eigene Hard- und Software-Infrastrukturen betrieben. Hierunter fallen sowohl auf dem Markt erhältliche Standardprodukte als auch projektspezifische Lösungen und Eigenentwicklungen.

Zu den beschriebenen Zwecken werden grundsätzlich personenbezogene Daten verarbeitet, insbesondere Gesundheitsdaten. Diese Daten werden zur besseren Verarbeitung und standortübergreifenden Auswertbarkeit unter Anwendung von Interoperabilitätsstandards des Gesundheitswesens aufbereitet und technischen Transformationsverfahren (u.a. Pseudonymisierung) unterzogen, bevor sie in konkreten Datennutzungsprojekten in jeweils zu spezifizierendem Umfang bereitgestellt werden.

3 Rechtliche Rahmenbedingungen

3.1 Rechtsgrundlagen

Für die Nutzung von Krankenversorgungs- und Forschungsdaten im Rahmen von Datennutzungsprojekten sind europäische, bundesweite und landesrechtliche regulatorische Vorgaben zu Schutz und Sicherheit von Gesundheitsdaten der versorgten Patienten als wichtigste Rahmenbedingungen zu beachten [vgl. 2, Abschnitt 2.7].

Das UKJ ist nach Maßgabe des §26 Thüringer Datenschutzgesetzes (ThürDSG) eine öffentliche Einrichtung, die am Wettbewerb teilnimmt und fällt damit neben der DSGVO auch unter den Regelungsbereich des Bundesdatenschutzgesetzes (BDSG).

In den Datennutzungsprojekten sind daher u.a. nachfolgende übergreifende und spezifische rechtliche Grundlagen anzuwenden:

- Landeskrankenhausgesetz (ThürKHG):
  - ThürKHG §27 (4):
    Verarbeitung von Patientendaten im Rahmen des krankenhausärztlichen Behandlungsverhältnisses, zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses; Beauftragung von Auftragsverarbeitern im Krankenhaus zur Erfüllung dieser Aufgaben
  - ThürKHG §27a:
    Datenverarbeitung für Forschungszwecke außerhalb des Krankenhauses; Einwilligungspflicht des Patienten (außer bei Nichtbeeinträchtigung schutzwürdiger Belange oder überwiegendem öffentlichen Interesse); Erfordernis zur Datentrennung / Pseudonymisierung / Anonymisierung)

- weitere gesetzliche Rahmenbedingungen:
  - EU-DSGVO (Art. 9 Abs. 2a sowie 2j):
    Verarbeitung besonderer Kategorien personenbezogener Daten
  - BDSG §27: Datenverarbeitung zu wissenschaftlichen oder historischen und zu statistischen Zwecken

- Vereinbarungen aus der Medizininformatik-Initiative für alle Universitätskliniken:
  - breite Patienteneinwilligung der MII („Broad Consent“) [7] als studien- und projektunabhängige Umsetzung von Einwilligungserfordernissen (vgl. Abschnitt 6.5)
  - übergreifende Nutzungsordnung zum Austausch von Patientendaten, Biomaterialien, Analysemethoden und -routinen für multizentrische Projekte [8]

- Vereinbarungen für die Tätigkeit des DIZ Jena:
  - →Geschäftsordnung des Datenintegrationszentrums
  - →Nutzungsordnung des Datenintegrationszentrums
  - →Datennutzungsvertrag des Datenintegrationszentrums
  - →Verfahrensbeschreibung datenverarbeitender Verfahren des DIZ

- mögliche projektspezifische Vereinbarungen:
  - projektspezifische Patienteneinwilligungen
  - Datennutzungsverträge
  - Auftragsverarbeitungs-Verträge
  - Software-Nutzungsverträge für IT-Verfahren

3.2 Ethische und soziale Rahmenbedingungen

Die Verwendung klinischer Routinedaten in Datennutzungsprojekten für die biomedizinische Forschung verlangt ein hohes Maß an Datenschutz und Datensicherheit sowie die Einhaltung ethischer Standards.

Bei der Durchführung von Forschungsprojekten sind die ethischen Grundsätze gemäß der Deklaration von Helsinki zu beachten sowie der rechtskonforme Umgang mit den medizinischen Behandlungsdaten und Forschungsdaten zu gewährleisten. Diese Gewährleistungen werden über das Votum einer beantragten klinischen Studie am Menschen durch die Ethikkommission der Friedrich-Schiller-Universität Jena an der Medizinischen Fakultät oder durch ein Votum anderer Forschungsethik-Kommissionen im Falle multizentrischer Projekte nachgewiesen.

Für Patienten, deren Daten im Rahmen zukünftiger Projekte für die biomedizinische Forschung zur Verfügung gestellt werden, ergibt sich meist kein direkter Nutzen. Für zukünftig erkrankte Personen ergibt sich jedoch ein möglicher Nutzen, insofern die Erkenntnisse aus den durchgeführten Datennutzungsprojekten zu einer Verbesserung der klinischen Routine und Dokumentation führen können.

Durch die Nutzung ihrer Daten entstehen den Patienten keine Nachteile, da bereits vorliegende Behandlungsdaten weiterverwendet werden. Ein mögliches Risiko besteht durch die Verletzung der Persönlichkeitsrechte der Patienten durch das Bekanntwerden von Patientenidentitäten. Dieses Risiko ist durch die Einhaltung der datenschutzrechtlichen Bestimmungen adressiert und kann damit ausgeschlossen werden.

Basis der vorliegend beschriebenen Tätigkeiten ist die Durchführung von Wissenschaft und Forschung, deren Förderung als Zweck des Universitätsklinikums Jena in §2 Abs. 2 der UKJ-Grundsatzung verankert ist. Die standortübergreifende Verknüpfung von Daten, Informationen und Wissen aus Krankenversorgung und biomedizinischer Forschung adressiert dabei eine gesellschaftliche Verantwortung wissenschaftlicher Tätigkeit auf dem Gebiet der Medizinischen Informatik, bei der aktive Partizipation der Patienten, Schutz der Daten der Bürger, Verbesserung der Patientenversorgung und Erhöhung der Patientensicherheit wichtige Faktoren für die Akzeptanz von Datennutzungsprojekten sind. Im Bereich ELSI (Ethical, Legal, and Social Implications) sind dabei ethische, soziale und rechtliche Fragestellungen einzelner Projekte konkret zu beleuchten.

4 Organisation und Verantwortlichkeiten

4.1 Beteiligte Einrichtungen

Geschäftsbereich IT des UKJ (GB IT)
Die Leitung des Geschäftsbereichs IT ist im Zuge des Projekts SMITH für die Etablierung des Datenintegrationszentrums und dessen Verfahren gemeinsam mit dem IMSID (s.u.) verantwortlich. Der Betrieb der und die Bereitstellung von Daten aus den Primärdokumentationssystemen obliegt den Abteilungen Medizinische Applikationen, Medizinische Spezialsysteme und Administrative Applikationen des GB IT. Die Bereitstellung von Rechner- und Netzwerk-Infrastruktur erfolgt durch die Abteilung Infrastruktur-Management.

Datenintegrationszentrum Jena (DIZ)
Alle Verarbeitungsprozesse von medizinischen und Forschungsdaten zum Zwecke der Nutzung in standorteigenen oder standortübergreifenden Forschungsprojekten sowie die Rückführung interoperabler, integrierter und qualitätsgesicherter Daten und Ergebnisse in die Krankenversorgung werden am DIZ Jena durchgeführt.

Integrierte Biobank Jena (IBBJ)
Die mögliche Nutzung von Bioproben im Kontext von Forschungsprojekten wird über die Einbindung der IBBJ in die Patienteneinwilligungs- und Datennutzungsverfahren sichergestellt.

Zentrum für Klinische Studien Jena (ZKS)
Beschäftigte der IT Unit des ZKS übernehmen die Aufgaben einer Datentreuhandstelle zur Trennung von Krankenversorgungs- und Forschungsdaten. Darüber hinaus kann im Rahmen von klinischen Forschungsprojekten die Beteiligung und Unterstützung des ZKS erfolgen; hierbei ist projektspezifisch zu prüfen, ob die Treuhandstellenfunktionalität jeweils gewährleistet werden kann.

Institut für Medizinische Statistik, Informatik und Datenwissenschaften (IMSID)
Die Leitung des IMSID ist im Zuge des Projekts SMITH für die Etablierung des Datenintegrationszentrums und dessen Verfahren gemeinsam mit dem GB IT (s.o.) verantwortlich. Darüber hinaus können statistisch-methodische Beratungen zu Analyseverfahren in Datennutzungsprojekten sowie konkrete Umsetzungen der Datenanalysen von durch das DIZ bereitgestellten Daten durch Beschäftigte des IMSID durchgeführt werden.

4.2 Verantwortlichkeiten

Für den Prozess der Nutzung von Daten aus Krankenversorgung und Forschung im Rahmen weiterer Forschungsprojekte sind durch die jeweils unterschiedlichen Abläufe und geltenden regulatorischen Vorgaben verschiedene Verantwortungsbereiche zu unterscheiden.

Tabelle 1: Verantwortlichkeiten

Verantwortlichkeit	Datenart	
	IDAT, PID Clinical Domain	**MDAT Clinical Domain**
verantwortliche Stelle	DIZ	DIZ
Datenlieferant	GB IT	GB IT
Vertrauensstelle	Treuhandstelle	
	SIC Research Domain	**MDAT Research Domain**
verantwortliche Stelle	DIZ	DIZ
Datenlieferant	Treuhandstelle	DIZ
Vertrauensstelle	Treuhandstelle	
	PID Trust Unit	**SIC, PSIC Trust Unit**
verantwortliche Stelle	Treuhandstelle	Treuhandstelle
Datenlieferant	DIZ	Treuhandstelle
Dateneinsicht	Treuhandstelle	
	PSIC Datennutzungsprojekt	**MDAT Datennutzungsprojekt**
verantwortliche Stelle	Projektleitung	Projektleitung
Datenlieferant	DIZ	DIZ
Datenauswertungen	Projektleitung, DIZ, IMSID	

Die grundsätzliche Verantwortlichkeit für die Verarbeitung von personenbezogenen Daten (IDAT, PID, MDAT, vgl. Abschnitt 5.1) im Rahmen der Krankenversorgung (Schutzzone „Clinical Domain“, vgl. Abschnitt 6.1) und der Bereitstellung der Daten in pseudonymisierter Form (SIC, MDAT, vgl. Abschnitt 5.1) für noch nicht durchgeführte Forschungsprojekte (Schutzzone „Research Domain“, vgl. Abschnitt 6.1) obliegt der DIZ-Leitung. Im Rahmen von operativen Tätigkeiten tragen die für die Verarbeitung verantwortlichen Beschäftigten unter Berücksichtigung der für den jeweiligen Bereich erstellten Verfahrensanweisungen ebenfalls Verantwortung. Verantwortlich für die Verarbeitung personenbezogener Daten (PSIC, MDAT, vgl. Abschnitt 5) in konkreten Forschungsvorhaben ist, wie in der Datenschutz-Richtlinie des UKJ [2] geregelt, die jeweilige Projektleitung.

Am DIZ Jena ist ein DIZ-Datenschutz-Koordinator benannt, der mit dem DIZ-IT-Sicherheitskoordinator in enger Abstimmung steht und mit der DIZ-Qualitätsmanagement-Beauftragten zusammenarbeitet. Im Fokus der Tätigkeit stehen hierbei die Überwachung der Einhaltung sämtlicher Datenschutzvorschriften und Verordnungen in diesem Kontext sowie der technischen und organisatorischen Maßnahmen (TOMs) der Verantwortlichen oder der Auftragsverarbeitenden für den Schutz personenbezogener Daten, einschließlich der Zuweisung von DIZ-internen Zuständigkeiten sowie der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten am DIZ Beschäftigten. In den Aufgabenbereich fallen ebenso die Umsetzung UKJ-interner Prozesse. Hierzu erfolgen eine regelmäßige Unterrichtung und Beratung des DIZ-Datenschutz-Koordinators durch UKJ-Datenschutzbeauftragte.

4.3 Kreis betroffener Personen

Patienten des UKJ
Von der Verarbeitung ihrer Daten für die hier beschriebenen Zwecke sind prinzipiell alle am UKJ behandelten Personen betroffen. Dieser Betroffenenkreis wird durch zwei Faktoren eingeschränkt:

1. Die weitere **Verarbeitung** ihrer Daten in pseudonymisierter Form und die Bereitstellung dieser auch für multizentrische Forschungsprojekte unterliegt grundsätzlich der Einwilligungspflicht der betroffenen Patienten. Diese Einwilligung kann projektunabhängig durch die breite Patienteneinwilligung der MII („Broad Consent“) [7] erfolgen oder durch eine studienspezifische Einwilligung, oder es existiert eine weitere gesetzliche Grundlage für die Verwendung in einem konkreten Datennutzungsprojekt. Andernfalls erfolgt die Verarbeitung ausschließlich für die Krankenversorgung.
2. Die tatsächliche **Nutzung** der Daten in konkreten Forschungsprojekten (standortintern oder standortübergreifend) kann nur auf der Basis einer jeweils konkret anzugebenden gesetzlichen Grundlage erfolgen. Eine wie unter 1. beschrieben eingeholte Form der Patienteneinwilligung ist dabei eine mögliche Rechtsgrundlage. Ohne Rechtsgrundlage erfolgt die Verarbeitung ausschließlich für die Krankenversorgung.

Beschäftigte des UKJ
Durch die Verarbeitung medizinischer Daten, die im Rahmen der Dokumentation auch Angaben zu durchführendem, dokumentierendem oder verantwortlichem Personal im Kontext von Forschungs- und Versorgungsprozessen enthalten können, sind von der Verarbeitung auch Beschäftigte des UKJ betroffen. Die Verarbeitung dieser Daten erfolgt grundsätzlich im Rahmen der Krankenversorgung (Schutzzone „Clinical Domain“, vgl. Abschnitt 6.1). Insoweit personenbezogene Daten nach §27 Abs. 4 ThürKHG zu anonymisieren sind, sobald dies nach dem Forschungszweck möglich ist, werden Beschäftigtendaten im Zuge der pseudonymisierten Datenbereitstellung für standortübergreifende Projekte und je nach Projekterfordernissen auch bei der Nutzung in standortbezogenen Forschungsprojekten anonymisiert. Ausnahmen hiervon können

weitere Informationspflichten und Genehmigungen erforderlich machen, z.B. die Zustimmung des UKJ-Personalrats.

Weitere Personenkreise
Im Zuge der Nutzung von Krankenversorgungsdaten in Forschungsprojekten kann die Verarbeitung personenbezogener Daten weiterer Personenkreise erforderlich sein:

- Daten von Kooperationspartnern in einem multizentrischen Forschungsprojekt
- Daten von Personen, die projektspezifische Prozesse extern überwachen (Studienmonitore, Auditoren)
- Daten von Auftragsverarbeitenden

Die Verarbeitungsprozesse der Daten dieser Personenkreise sind für das jeweilige Datennutzungsprojekt zu konkretisieren.

5 Zu verarbeitende Daten

5.1 Datenkategorien

Für die Nutzung in Forschungsprojekten werden grundsätzlich personenbezogene Daten verarbeitet. Vorrangig handelt es sich um Gesundheitsdaten. Diese werden aus der Dokumentation im Rahmen der Krankenversorgung oder aus zusätzlichen Erhebungen im Zuge eines Forschungsprojekts gewonnen und für das jeweilige Projekt bereitgestellt. Für diese Daten bzw. Datenkategorien sind individuelle Schutzbedarfe zu definieren, welche im Folgenden dargestellt sind (entnommen aus [3, Abschnitt 5.4]):

Identifizierende Daten (IDAT)
Bei den IDAT handelt es sich um die primär identifizierenden Merkmale des Patienten wie Name, Geburtsdatum, Adresse usw. Hierbei handelt es sich nicht um Gesundheitsdaten; allerdings ist zu berücksichtigen, dass zusammen mit dem Wissen der Herkunft der Daten (Behandlungskontext, Forschungskontext) eine höhere Schutzstufe entstehen kann. Ebenso werden ggf. identifizierende Daten von Beschäftigten verarbeitet.

Patient Identifier (PID)
Die PID ist der quellenspezifische eindeutige Identifikator des Patienten. Er stammt aus dem Primärdokumentationssystem des UKJ (Krankenhausinformationssystem SAP IS-H) und wird nur in den entsprechenden Schutzzonen (Behandlungskontext, standortinterner Studienkontext) verwendet. Die PID ist in den Quellsystemen mit den jeweiligen IDAT des Patienten verknüpft.

Master Patient Index ID (MPI-ID)
Die MPI-ID ist die eindeutige ID innerhalb der Schutzzone Clinical Domain (vgl. Abschnitt 6.1). Wenn verschiedene PIDs aus verschiedenen Quellen (Behandlungskontext und Studienkontext) an die Clinical Domain übermittelt werden, werden alle PIDs unter einer MPI-ID gespeichert.

Subject Identifier Code (SIC)
Patienten des UKJ wird bei der Datenübertragung von der Clinical Domain in die Research Domain (vgl. Abschnitt 6.1) des Datenintegrationszentrums ein eindeutiger Subject Identifier Code (SIC) als Primärpseudonym zugewiesen. Sämtliche medizinische Daten in der Research Domain werden unter der SIC abgespeichert.

Project Subject Identifier Code (PSIC)
Für eine Weitergabe oder Auswertung in Datenanalyseprojekten wird die SIC in einem zweiten Schritt auf einen zufällig erzeugten Project Identifier Code (PSIC) als Sekundärpseudonym eindeutig abgebildet. Aus der PSIC kann nicht auf die Identität des Patienten rückgeschlossen werden.

Medizinische Daten (MDAT)

Bei MDAT handelt es sich um alle im Rahmen der Behandlung oder in Forschungsprojekten erfassten Daten. Sie umfassen auch alle daraus abgeleiteten Daten (Analyseergebnisse etc.). Die konkrete Art der verwendeten MDAT unterscheidet sich je nach Fragestellung des spezifischen Forschungsprojekts und ist stets einem entsprechenden Studienprotokoll zu entnehmen. Eine Basis für alle Datennutzungsprojekte bildet der sogenannte Kerndatensatz der Medizininformatik-Initiative, dessen Datenelemente für konkrete Projekte erschlossen und bereitstellbar sein müssen [9].

Tabelle 2: Datenkategorien und Vorkommen

Zone	IDAT	MPI-ID	PID	SIC	PSIC	MDAT
DIZ Clinical Domain	×	×	×			×
DIZ Research Domain				×		×
Trust Unit		×	×	×	×	
Data Sharing					×	×

5.2 Umgang mit identifizierenden Daten

Für die Bereitstellung für biomedizinische Forschungsprojekte werden medizinische Daten grundsätzlich organisatorisch getrennt von den Identifikationsdaten der Patienten verarbeitet und persistiert. Jede am Verarbeitungsprozess beteiligte Stelle verfügt grundsätzlich nur über diejenigen Daten, die sie zur Erfüllung ihrer Zielsetzung benötigt.

Im Rahmen der Bereitstellung von strukturierten Daten für beliebige standortübergreifende Forschungsprojekte werden Daten, die eine direkte Identifikation des Patienten ermöglichen, generell nach einem beschriebenen Verfahren pseudonymisiert. Nichtstrukturierte Daten, deren Format eine Pseudonymisierung unterstützt (z.B. DICOM) werden ebenfalls pseudonymisiert. Nichtstrukturierte Datenformate, die in sich „potenziell“ identifizierende Merkmale tragen (z.B. Arztbriefe, Genomdaten, etc.) werden nicht übermittelt. Für die Pseudonymisierung von Volltextdokumenten werden entsprechende Verfahren zur Deidentifikation genutzt.

5.3 Datenformate

Bei MPI-ID, PID, SIC und PSIC handelt es sich um Identifikatoren, für deren Format Nummern oder Codes aus alphanumerischen Zeichen verwendet werden.

IDAT und MDAT werden aus den Primärdokumentationssystemen des UKJ über standardisierte Schnittstellen (z.B. HL7v2-Nachrichtenformat) oder z.B. durch Abfrage aus Datenpersistenzschichten zur weiteren Verarbeitung extrahiert. Am Datenintegrations-zentrum erfolgt eine Integration und Transformation der heterogenen Primärdaten in das

interoperable Format HL7 FHIR. Die Daten werden dabei auch durch die Annotation mit Codes aus deutschen und internationalen Terminologien (z.B. ICD, LOINC, SNOMED CT etc.) weiter angereichert. Technische Vorgaben für diese Tätigkeiten sind dem Kerndatensatz der Medizininformatik-Initiative [9] zu entnehmen.

6 Datenverarbeitende Prozesse

6.1 IT-Architektur zur Versorgungs- und Forschungsdatennutzung

Um Daten aus Krankenversorgung und klinischer Forschung für die Nutzung in weiteren, ggf. zukünftigen Forschungsprojekten bereitzustellen, werden am Datenintegrationszentrum geeignete IT-Verfahren etabliert, mittels welcher die entsprechend geltenden Vorgaben zum Datenschutz umgesetzt werden können. Hierfür sind die IT-Verfahren in verschiedene Schutzzonen unterteilt. Als Schutzzonen gelten organisatorisch abgeschlossene Bereiche mit jeweils eigenen Verantwortlichkeiten (vgl. Abschnitt 4.1).

Die Schutzzonen sind für alle Datenintegrationszentren des SMITH-Konsortiums identisch definiert und im SMITH-Datenschutzkonzept [3] im Detail beschrieben.

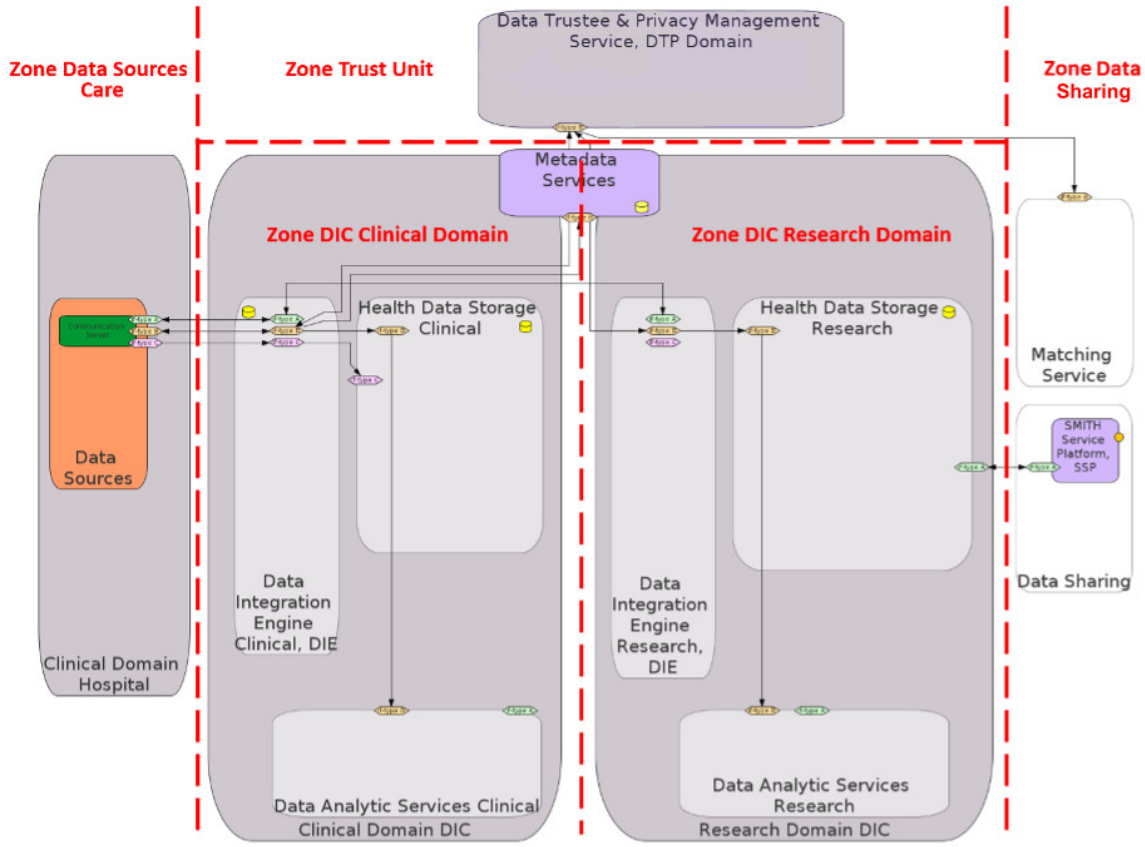

Abbildung 1: Schutzzonen der Datenverarbeitung

Die Zuordnung der konkreten IT-Verfahren im UKJ zu den jeweiligen Schutzzonen ist in der IT-Architekturbeschreibung des Datenintegrationszentrums erläutert.

Die Verfahren im Rahmen der Kommunikation und Archivierung für die Krankenversorgung sowie im Rahmen der Bereitstellung von Forschungsdaten sind als IT-Verfahren des

Datenintegrationszentrums zur Verarbeitung personenbezogener Daten im Verzeichnis der Verarbeitungstätigkeiten des Universitätsklinikums Jena nach Art. 30 DS-GVO dokumentiert.

6.2 Typen von IT-Verfahren

Clinical Domain

- *Data Integration Engine:*
  IT-Verfahren, die der Datenkommunikation und -transformation dienen
- *Health Data Storage:*
  IT-Verfahren, die der Datenpersistenz dienen
- *Data Analytic Services:*
  IT-Verfahren, mittels denen Datenanalysen und -auswertungen durchgeführt werden können (hier insbesondere für die klinische Routine)
- *Access Control and Auditing Services:*
  IT-Verfahren zur Zugangskontrolle und -protokollierung
- *Patient Identification Services:*
  IT-Verfahren zur eindeutigen Zuordnung von MDAT zu Patienten mittels IDAT
- *User/Clinician Registry:*
  IT-Verfahren zur Identifikation und Authentifikation von Nutzenden

Research Domain

- *Data Integration Engine:*
  IT-Verfahren, die der Datenkommunikation und -transformation dienen
- *Health Data Storage:*
  IT-Verfahren, die der Datenpersistenz dienen
- *Data Analytic Services:*
  IT-Verfahren, mittels denen Datenanalysen und -auswertungen durchgeführt werden können (hier insbesondere standortübergreifende Auswertungen)
- *Access Control and Auditing Services:*
  IT-Verfahren zur Zugangskontrolle und -protokollierung

Trust Unit

- *Consentmanagement:*
  IT-Verfahren zur Erfassung, Verwaltung und Abfrage von Patienteneinwilligungen
- *Pseudonymmanagement:*
  IT-Verfahren zur Erzeugung, Verwaltung und Abfrage von Pseudonymen (SIC, PSIC, vgl. Abschnitt 5.1)

Data Sharing

- *Data and Metadata Transfer Management Service:*
  IT-Verfahren, die zur Datenaufbereitung und -bereitstellung für konkrete multizentrische Forschungsprojekte z.B. über die SMITH-Service-Plattform dienen

- *SMITH-Service-Plattform:*
  externes IT-Verfahren zur Erstellung von Datennutzungsanträgen, Durchführung von Fallzahlanfragen und zur Übermittlung von Forschungsdaten in einem bewilligten und vertraglich geregelten Datennutzungsprojekt

6.3 Verarbeitung der Daten in der Schutzzone „Clinical Domain“

Rechtsgrundlage
Die Datenintegration in der Schutzzone Clinical Domain ist Teil der herstellerneutralen Archivierungsstrategie (Vendor-Neutral Archive, VNA) am UKJ. In der Clinical Domain und den betreffenden IT-Verfahren werden IDAT und MDAT verarbeitet [vgl. 2, Abschnitt 4.2]. Alle verarbeiteten Daten wurden im Rahmen der Behandlung des Patienten erfasst und unterliegen den entsprechenden rechtlichen Bedingungen der Krankenversorgung.

Verarbeitungszweck
Kern der Verarbeitungstätigkeit ist die Integration von unterschiedlich strukturierten Daten aus unterschiedlichen Quellen und die Transformation aller Datenformate auf Basis des internationalen Interoperabilitätsstandards HL7 FHIR, inklusive semantischer Annotation mit einheitlichen Terminologien. Zwecke dieser Datenintegration sind die herstellerneutrale Datenarchivierung und die standortunabhängige Verarbeit- und Auswertbarkeit im Rahmen von Forschungsfragestellungen.

Verarbeitungsweisen
Die Datenextraktion erfolgt je nach geforderter Datenart aus verschiedenen Quellsystemen. Patientenstammdaten, Verlegungsdaten, Falldaten, Diagnosen und Prozeduren werden über SAP IS-H bereitgestellt; Laborbefunde über nexus swisslab; Biosignale, Diagnosen, Prozeduren, Verläufe und Medikationen über COPRA sowie ID MEDICS, Dokumente (PMD, PDF, Word) über Cerner i.s.h.med und weitere Daten über sonstige im zeitlichen Verlauf erschlossene Primärsysteme (Stand 2021).

Datenextraktion und Datentransformation erfolgen in IT-Verfahren des Typs „Data Integration Engine“. Die transformierten Daten werden in IT-Verfahren des Typs „Health Data Storage“ in der Clinical Domain persistiert. Insofern der Health Data Storage der Clinical Domain Bestandteil eines Archivs von Krankenversorgungsdaten ist, richten sich die Dauern der Speicherung von Daten in diesem Bereich nach den vorgegebenen Archivierungsfristen. Nähere Angaben hierzu vgl. →DIZ-Archivierungskonzept.

Um medizinische Daten aus verschiedenen Quellen eindeutig den richtigen Patienten zuordnen zu können, erfolgt eine Verarbeitung von PID und ggf. Nutzung von MPI-ID (vgl. Abschnitt 5.1) in IT-Verfahren des Typs „Patient Identification Services“.

Forschungsprojekte nach §27 Abs. 4 ThürKHG, die durch Krankenhausärzte des UKJ mit Daten von Patienten des UKJ durchgeführt werden dürfen und keine explizite Einwilligung benötigen, können Datennutzungen innerhalb der Schutzzone Clinical Domain erfordern.

Datenanalysen und -auswertungen für solche Projekte, insbesondere auch innerhalb der klinischen Routine, werden in IT-Verfahren des Typs „Data Analytic Services“ durchgeführt.

Die Zugriffe von Nutzern und Administratoren insbesondere auf Komponenten von IT-Verfahren, in denen personenbezogene Daten verarbeitet werden, bedürfen einer Registrierung und werden entsprechend technisch überprüft und dokumentiert. Die Registrierung erfolgt über IT-Verfahren des Typs „User / Clinician Registry“ und unter der Verarbeitung personenbezogener Daten der Nutzer (insbesondere Login). Die Zugriffskontrolle und -dokumentation erfolgt mittels IT-Verfahren des Typs „Access Control and Auditing Services“.

Verantwortlichkeiten
Verantwortlich für die Datenextraktion, Datentransformation, Datenpersistenz und Datenanalyse sind Beschäftigte des DIZ in entsprechend definierten Rollen (Schnittstellenadministration, Daten- und Metadatenmanagement und Software-entwicklung; vgl. →DIZ-Aufgabenbeschreibungen). Die Verantwortlichkeit für Nutzeridentifikation, Zugriffskontrolle und Audit-Logging liegt bei Beschäftigten des DIZ in der Rolle Administration IT-Sicherheits- und Treuhanddienste. Detaillierte Informationen zur Umsetzung sind in der technischen Dokumentation der genutzten IT-Verfahren näher ausgeführt.

6.4 Verarbeitung der Daten in der Schutzzone „Research Domain“

Rechtsgrundlage
Erfolgt durch den Patienten eine Einwilligung zur Verarbeitung seiner Daten für bestimmte oder jegliche Forschungsprojekte (vgl. Abschnitt 6.6), konkret zur Erhebung, Verarbeitung, Speicherung und wissenschaftlichen Nutzung, oder gibt es eine projektbezogene gesetzliche Grundlage dafür, so ist eine weitere Verarbeitung dieser Daten außerhalb des Krankenversorgungskontexts in der Schutzzone Research Domain möglich. Gleichfalls kann einwilligungsbasiert oder aufgrund einer projektbezogenen gesetzlichen Grundlage die Ergänzung oder Erfassung weiterer Daten über Record Linkage oder Electronic-Data-Capture-Verfahren (EDC) möglich sein.

Verarbeitungszweck
Die Verarbeitungstätigkeit in der Research Domain zielt auf die Bereitstellung von medizinischen Daten im interoperablen Format, das in der Clinical Domain erzeugt wurde, für ggf. noch nicht bekannte, künftige Forschungsprojekte ab. Zweck der Verarbeitung ist daher eine einrichtungsunabhängig gleichartige Verfügbarkeit pseudonymisierter Daten für die Forschung.

Verarbeitungsweisen
Für Datenbereitstellungen im Rahmen multizentrischer Forschungsprojekte und für nicht-patientennahe Forschung werden Daten patientenbezogen in die Schutzzone Research

Domain überführt [vgl. 2, Abschnitt 4.2]. Die Überführung erfolgt mittels IT-Verfahren des Typs „Data Integration Engine“.

Eine Überführung ist nur möglich, wenn dazu eine geeignete Einwilligung des Patienten oder projektspezifisch eine andere geeignete Rechtsgrundlage vorliegt und die Pseudonymisierung (insbesondere Ersetzen der MPI-IDs durch SICs) der Daten durchgeführt wurde. Die Prüfung der Einwilligung erfolgt im IT-Verfahren des Typs „Consentmanagement“ und die Erzeugung von Pseudonymen (SIC, vgl. Abschnitt 5.1) im IT-Verfahren des Typs „Pseudonymmanagement“.

Die Pseudonymisierung erfolgt nach einem in SMITH entwickelten, für alle SMITH-Kooperationspartner identischen Vorgehen, dessen Details für das UKJ in einer Verfahrensanweisung beschrieben sind (→VA Pseudonymisierung). Dabei werden identifizierende Daten entfernt oder geeignet vergröbert und die PID durch einen neuen Identifikator, die SIC, ersetzt.

Mittels SIC pseudonymisierte MDAT von einwilligenden Patienten werden in der Research Domain in IT-Verfahren des Typs „Health Data Storage“ persistiert. Eine konkrete Nutzung der Daten erfolgt immer nur auf vorab definierten Teilmengen dieser Daten, die von IT-Verfahren des Typs „Data and Metadata Transfer Management Service“ (vgl. Abschnitt 6.5) erzeugt werden können. Nutzungen sind Fallzahlanfragen, Datenanalysen oder Datenbereitstellungen im Kontext von (geplanten oder durchgeführten) Forschungsprojekten.

Auswertungen auf definierten Teilmengen der Daten in der Research Domain werden mittels IT-Verfahren des Typs „Data Analytic Services“ durchgeführt.

Wie in der Clinical Domain werden Zugriffe auf die IT-Verfahren mittels weiterer Verfahren vom Typ „Access Control and Auditing Services“ protokolliert.

Verantwortlichkeiten
Verantwortlich für die Datenüberführung in die Clinical Domain, die Datenpersistenz und die Erzeugung bzw. Nutzung von Teilmengen dieser Daten in konkreten Projekten sind Beschäftigte des DIZ in entsprechend definierten Rollen (Schnittstellenadministration, Daten- und Metadatenmanagement; vgl. →DIZ-Aufgabenbeschreibungen). Die Verantwortlichkeit für Zugriffskontrolle und Audit-Logging liegt bei Beschäftigten des DIZ in der Rolle Administration IT-Sicherheits- und Treuhanddienste. Detaillierte Informationen zur Umsetzung sind in der technischen Dokumentation der genutzten IT-Verfahren näher ausgeführt.

6.5 Verarbeitung der Daten in der Schutzzone „Trust Unit“

Rechtsgrundlage
Erfolgt durch den Patienten eine Einwilligung zur Verarbeitung seiner Daten für bestimmte oder jegliche Forschungsprojekte (vgl. Abschnitt 6.6), konkret zur Erhebung, Verarbeitung,

Speicherung und wissenschaftlichen Nutzung, oder gibt es eine projektbezogene gesetzliche Grundlage dafür, so ist eine weitere Verarbeitung dieser Daten außerhalb des Krankenversorgungskontexts in der Schutzzone Research Domain möglich. Um eine Pseudonymisierung der Daten in der Research Domain zu erreichen, bei der Beschäftigte des Datenintegrationszentrums keine Zusammenführung eindeutiger Identifikatoren (Fallnummern, Pseudonyme etc.) von Patienten durchführen [vgl. 3, Abschnitt 3.3], ist die Verwaltung von Zuordnungen zwischen solchen Identifikatoren durch eine vom Datenintegrationszentrum organisatorisch unabhängig agierende Treuhandstelle vorgesehen.

Verarbeitungsweisen
Durch die Treuhandstelle besteht die Möglichkeit, Einwilligungsinformationen und Pseudonymlisten konkreter Patienten einzusehen. Diese Einsicht ist erforderlich bei Auskunftsersuchen, Einwilligungswiderrufen, Rekontaktierungen oder anderen Umsetzungen von Betroffenenrechten (vgl. Abschnitt 6.7). Die Prüfung der Einwilligung erfolgt durch Zugriff auf IT-Verfahren des Typs „Consentmanagement“ und die Zuordnung von Pseudonymen durch Zugriff auf IT-Verfahren des Typs „Pseudonymmanagement“. Die konkreten Prozesse sind in entsprechenden Verfahrensanweisungen beschrieben (→VA Auskunftsersuchen, →VA Einwilligungswiderruf, →VA Re-Kontaktierung).

Verantwortlichkeiten
Die Verwaltung von Einwilligungen und Pseudonymlisten wird durch Beschäftigte der Treuhandstelle verantwortet. Entsprechende Abläufe sind den Verfahrensanweisungen der Treuhandstelle zu entnehmen.

6.6 Verarbeitung der Daten außerhalb des UKJ, „Data Sharing“

Rechtsgrundlage
Die Bereitstellung von Daten für eine Nutzung außerhalb des UKJ oder der Erhalt von Daten für eine Auswertung am UKJ in multizentrischen Forschungsprojekten erfordert neben entsprechenden Einwilligungen der betroffenen Patienten bzw. projektspezifisch einer anderen Rechtsgrundlage auch vertragliche Vereinbarungen zur Datennutzung. Diese Vereinbarungen richten sich nach der Form der Datenbereitstellung (Datenlieferung, Datenzugriff oder Nutzung von verteilten Analyseverfahren).

Verarbeitungszweck
Die Datenbereitstellung für konkrete Forschungsprojekte erfolgt nur projektspezifisch. Verarbeitungszweck der Verfahren in der Schutzzone „Data Sharing“ ist daher die Bereitstellung von Daten für ein konkretes Datennutzungsprojekt.

Verarbeitungsweisen
Für Datenbereitstellungen im Rahmen multizentrischer Forschungsprojekte und für nicht-patientennahe Forschung werden Daten patientenbezogen auf Basis getätigter Einwilligungen oder projektspezifisch auf Basis einer anderen Rechtsgrundlage für ein

konkretes Forschungsprojekt aufbereitet. Zu den Aufbereitungsverfahren gehören Einwilligungsprüfung bzw. Prüfung der Rechtsgrundlage, projektspezifische Datenqualitätsprüfung und erneute Pseudonymisierung der Daten mittels projektspezifischer Identifikatoren (PSIC) oder die Erzeugung von Daten ohne Patientenbezug z.B. durch Aggregation.

Grundsätzlich ist für die Bereitstellung der Interoperabilitätsstandard HL7 FHIR vorgesehen, profiliert durch die Implementierungsleitfäden des MII-Kerndatensatzes [9]. Projektspezifisch ist jedoch auch die Erzeugung und Bereitstellung weiterer Formate möglich.

Die beschriebenen Prozesse werden durch IT-Verfahren vom Typ „Data and Metadata Transfer Management Service“ unterstützt, die in der Schutzzone Research Domain betrieben werden. Daten ohne Patientenbezug können vorab auch durch IT-Verfahren des Typs „Data Analytic Services“ erzeugt werden, z.B. durch verteilte Analyseverfahren, die aggregierte Daten erzeugen.

Die Schutzzone „Data Sharing“ wird erst erreicht, wenn Daten außerhalb des UKJ verarbeitet werden. Dies kann über einen Datenupload oder über die Ermöglichung von Datenzugriffen erfolgen. Das zentrale IT-Verfahren zur Unterstützung solcher Abläufe ist die „SMITH-Service-Plattform“.

Verantwortlichkeiten
Für die Datenaufbereitung und -bereitstellung sowie die Anbindung an die SMITH-Service-Plattform sind Beschäftigte des DIZ in der Rolle Daten- und Metadatenmanagement verantwortlich. Detaillierte Informationen zur Umsetzung sind in der technischen Dokumentation der genutzten IT-Verfahren näher ausgeführt.

6.7 Umgang mit Einwilligungen und Widerrufen, Betroffenenrechte

Patienteneinwilligung
Die rechtliche Grundlage der Verarbeitung personenbezogener Daten mit Einwilligung spielt für die Nutzung dieser Daten in Forschungsprojekten eine tragende Rolle, [vgl. auch 2, Abschnitt 2.7.4].

Die Arbeitsgruppe Consent der Medizininformatik-Initiative hat bundeseinheitliche Regelungen, Prozesse und Formulierungen erarbeitet, die eine projekt- und einrichtungsübergreifende Nutzung von Patientendaten für Forschungszwecke ermöglichen soll. Der erarbeitete und mit der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) sowie mit allen zuständigen Ethikkommissionen für die Universitätsklinika in Deutschland abgestimmte „Broad Consent“ [7] erlaubt eine möglichst breite aber dennoch datenschutzrechtlich und ethisch geregelte Verwendung der personenbezogenen Daten der Patienten.

Auf Basis dieses Mustertexts ist eine UKJ-spezifische Erklärung zur Einwilligung in die Nutzung von Patientendaten, Krankenkassendaten und Biomaterialien (Gewebe und Körperflüssigkeiten) für medizinische Forschungszwecke erstellt worden.

Einwilligungen dieser Art werden am UKJ erfasst und in einem vom DIZ bereitgestellten IT-Verfahren zum Consentmanagement (vgl. Abschnitt 6.2) verwaltet. Näheres zu diesen Prozessen regeln entsprechende Verfahrensanweisungen (→VA Patienteneinwilligung, →VA Einwilligungsverwaltung).

Nur auf Basis einer Einwilligung eines Patienten oder projektspezifisch auf Basis einer anderen gesetzlichen Grundlage in die Erhebung, Verarbeitung, Speicherung und wissenschaftliche Nutzung seiner Daten werden diese Daten innerhalb der Schutzzone Research Domain pseudonymisiert für künftige Forschungsprojekte bereitgestellt (vgl. Abschnitt 6.4).

Widerruf der Einwilligung
Patienten haben jederzeit das Recht, jegliche Formen einer getätigten Einwilligung zur Nutzung ihrer Daten zu widerrufen.

Der Widerruf einer Patienteneinwilligung vom Typ „Broad Consent“ wie oben beschrieben oder von Teilen dieser wird wie eine erneut ausgefüllte Version dieser Einwilligung behandelt. Nicht näher spezifizierte Widerrufe resultieren in einer Einwilligung, in der alle Fragen mit „nein“ beantwortet werden.

Im Falle eines Widerrufs der Erhebung, Verarbeitung, Speicherung und wissenschaftlichen Nutzung der Daten eines Patienten dürfen diese nicht mehr bzw. nur auf Basis anderer, projektspezifisch festzulegender Rechtsgrundlagen in pseudonymisierter Form in der Schutzzone Research Domain für Forschungsprojekte bereitgestellt werden. Diese Daten werden dann durch DIZ-Beschäftigte mit der Rolle Administration Forschungsprojektdaten gelöscht. Im Falle von derzeit durchgeführten Forschungsprojekten mit pseudonymisierter Datennutzung sind Projektverantwortliche über den Widerruf der Datennutzung zu informieren, so dass dieser im jeweiligen Projekt umgesetzt und die Daten gelöscht werden.

Nähere Angaben zur Umsetzung des Widerrufs enthält die entsprechende Verfahrensanweisung hierzu (→VA Einwilligungswiderruf, →VA Datenlöschung).

Betroffenenrechte
Die Rechte der von den hier beschriebenen Datenverarbeitungsverfahren Betroffenen (vgl. Abschnitt 4.3) werden in den folgenden Artikeln der DSGVO spezifiziert:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung („Recht auf Vergessenwerden“, Art. 17 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Zu den weiteren Rechten des Betroffenen zählen das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie das Widerspruchsrecht gegen die Verarbeitung (Art.21 DSGVO).

Betroffenenrechte am DIZ Jena sind grundsätzlich in der Richtlinie für die Umsetzung der Datenschutzanforderungen am UKJ [2] geregelt. Entsprechende Anfragen werden gemäß Abschnitt 4.1.4.2 von UKJ-Datenschutzbeauftragten verifiziert und gemeinsam mit der fachlichen Struktureinheit, welche entsprechende personenbezogene Daten verarbeitet, inhaltlich bewertet und bearbeitet.

Im Falle des Einbezugs von hier dargestellten IT-Verfahren erfolgt diese Zusammenarbeit mit der DIZ-Datenschutzkoordination (vgl. Abschnitt 4.2). Für Auskunftsrechte werden Informationen über DIZ-Beschäftigte mit der Rolle Daten- und Metadatenmanagement sowie über die Treuhandstelle eingeholt (Vorhandensein von Daten in IT-Verfahren der Clinical Domain, der Research Domain in pseudonymisierter Form, Nutzung der Daten in Forschungsprojekten). Berichtigungen von Daten werden über die Korrektur der Daten in IT-Verfahren der Krankenversorgung durchgeführt und von dort über die IT-Verfahren der Forschungsdatennutzung weiterverarbeitet. Datenlöschungen werden identisch zum Eingang eines Widerrufs durch DIZ-Beschäftigte mit der Rolle Administration Forschungsprojektdaten bearbeitet. Für das Recht auf Datenübertragbarkeit erfolgt über DIZ-Beschäftigte mit der Rolle Daten- und Metadatenmanagement sowie über die Treuhandstelle eine manuelle Zusammenstellung der verarbeiteten Daten.

Nähere Angaben zum Umgang mit Anfragen in Bezug auf Betroffenenrechte regelt eine entsprechende Verfahrensanweisung (→VA Auskunftsersuchen, →VA Datenlöschung).

7 Feststellung des Schutzbedarfs und Risikoanalyse

7.1 Allgemeines

Die Erstellung von Datenschutzfolgeabschätzungen für die vorliegend beschriebenen Verarbeitungsverfahren ergibt sich aus der Klassifikation als umfangreiche Verarbeitungsvorgänge von Gesundheitsdaten und aus entsprechenden Vorgaben aus dem übergreifend gültigen SMITH-Datenschutzkonzept [3, Abschnitt 4.1].

Die Datenschutzfolgeabschätzungen sind als Anlagen zum vorliegenden Datenschutzkonzept erarbeitet, welche nach den Vorgaben der UKJ- Richtlinie Datenschutz [vgl. 2, Abschnitt 4.1.2] und der entsprechenden Verfahrensanweisung des UKJ für die Datenschutzfolgeabschätzung erarbeitet wurden.

Hierbei werden grundsätzlich die Einteilung der Datenkategorien (vgl. Abschnitt 5.1) in vorgegebene Schutzstufen sowie die Schutzbedarfsfeststellungen im Rahmen der Risikobewertungen für einzelne datenverarbeitende Abläufe aus dem SMITH-Datenschutzkonzept [3, Abschnitte 4.1 und 5.4] übernommen, sofern in den jeweiligen Datenschutzfolgeabschätzungen keine abweichenden Angaben gemacht werden.

7.2 Datenschutzfolgeabschätzung für die Schutzzone „Clinical Domain“

siehe →Datenschutzfolgeabschätzung Clinical Domain

7.3 Datenschutzfolgeabschätzung für die Schutzzone „Research Domain“

siehe →Datenschutzfolgeabschätzung Research Domain

7.4 Datenschutzfolgeabschätzung für die Schutzzone „Trust Unit“

siehe →Datenschutzfolgeabschätzung Trust Unit

7.5 Datenschutzfolgeabschätzung für die Schutzzone „Data Sharing“

siehe →Datenschutzfolgeabschätzung Data Sharing

8 Technische und organisatorische Maßnahmen

8.1 Allgemeines

Für die datenverarbeitenden Prozesse im Kontext der Nutzung von Forschungs- und Krankenversorgungsdaten in biomedizinischen Forschungsprojekten („Datennutzungsprojekten“), wie in Abschnitt 6 beschrieben, werden die im Folgenden dargestellten technisch-organisatorischen Maßnahmen getroffen, um die jeweiligen gesetzlichen Vorschriften am UKJ umzusetzen. Die Maßnahmen folgen den Vorgaben aus der UKJ-Richtlinie Datenschutz [vgl. 2, Abschnitt 4.1.7.2] und werden ergänzt durch weitere Maßnahmen, die in Richtlinien und Verfahrensanweisungen des GB IT z.B. zur Zutrittskontrolle zu Rechenzentren beschrieben werden, sowie durch die allgemeinen Vorgaben des SMITH-Datenschutzkonzepts [vgl. 3, Abschnitt 5.5].

8.2 Kontrolle von Zugängen und Zugriffen

Der Zugang zu den datenverarbeitenden Systemen ist bis auf die Komponenten, welche zum Zweck des Data Sharing außerhalb des UKJ etabliert werden, ausschließlich aus dem Kliniksnetz möglich. Die für das Data Sharing relevanten Komponenten werden in einer DMZ etabliert und der Zugang nur von konkret benannten externen Servern aus ermöglicht. Generell ist das der Zugang über die SMITH-Service-Plattform und deren Server. Es besteht die Möglichkeit, projektspezifisch weitere Zugänge zu ermöglichen (z.B. Zugang für einen Projektpartner eines anderen Universitätsklinikums im Kontext eines bestimmten Datennutzungsprojekts).

Zugriffe auf die datenverarbeitenden Verfahren der Typen in Abschnitt 6.1 sind nur für die zur Nutzung dieser Systeme Berechtigten möglich. Dies wird durch Authentifikation über das IT-Verfahren „User/Clinician Registry“ oder durch Nutzername-/Passwort-Vergaben für konkrete IT-Systeme umgesetzt. Die Zugriffe werden durch IT-Verfahren des Typs „*Access Control and Auditing Services*” protokolliert und überwacht. Nähere Angaben hierzu finden sich im →DIZ-IT-Sicherheitskonzept sowie in den IT-Servicebeschreibungen der konkret für die IT-Verfahren eingesetzten Produkte.

Die getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten wird durch das Konzept der Schutzzonen umgesetzt, vgl. Abschnitte 5.1 und 6.1. Die jeweiligen IT-Verfahren der Schutzzonen werden mit unterschiedlicher organisatorischer Zuordnung und unter Trennung der Verantwortlichkeiten betrieben. Beschäftigte, welche aufgrund ihrer Funktion Zugriff sowohl auf Identifikationsdaten als auch wissenschaftliche Daten haben (z.B. Softwareadministratoren, Datenmanager), werden per Arbeitsanweisung auf ihre besondere Verantwortung im Umgang mit den ihnen zugänglichen Daten hingewiesen und ihnen untersagt, eindeutige Identifikatoren (PID, SIC, PSIC) und weitere Daten von Patienten zusammenzuführen und außerhalb der dafür vorgesehenen Speicherorte aufzubewahren.

8.3 Regelungen zur Datenverarbeitung

Personenbezogene Daten sind nach den im Abschnitt 3.1 benannten gesetzlichen Vorgaben zu pseudonymisieren oder zu anonymisieren. Diesem Zweck dient das Verfahren der Datenverarbeitung in der Research Domain, vgl. Abschnitt 6.4 und [3, Abschnitt 4.6.1]. Die konkrete Umsetzung ist in der zugehörigen Verfahrensanweisung beschrieben (→VA Pseudonymisierung).

Projektspezifisch ist die Erzeugung weitergehend anonymisierter Daten für den standortübergreifenden Austausch möglich, z.B. durch Erzeugung aggregierter Daten ohne Personenbeziehbarkeit. Projektspezifische Pseudonymisierungs- oder Anonymisierungsverfahren sind gesondert zu beschreiben.

Die für Krankenversorgung und biomedizinische Forschung gespeicherten Daten (vgl. Abschnitt 5.1) unterliegen verschiedenen Aufbewahrungs- bzw. Löschfristen und sind zum Teil bei der Umsetzung des Betroffenenrechts auf Datenlöschung (vgl. Abschnitt 6.7) einzubeziehen. Hierfür sind organisatorische und technische Prozesse zur Datenlöschung in den jeweiligen datenverarbeitenden IT-Verfahren definiert. Nähere Angaben sind in der korrespondierenden Verfahrensanweisung (→VA Datenlöschung) sowie in den IT-Servicebeschreibungen der konkret für die IT-Verfahren eingesetzten Produkte hinterlegt. Für projektspezifisch etablierte IT-Verfahren sind eigene Angaben zur Datenlöschung zu ergänzen.

8.4 Datenschutzrechtliche Vereinbarungen

Die Verarbeitung personenbezogener Daten aus Krankenversorgung und Forschung wird durch verschiedene Formen von Vereinbarungen ermöglicht bzw. beeinflusst.

Die wichtigste Vereinbarung ist die Patienteneinwilligung vom Typ „Broad Consent“ (vgl. Abschnitt 6.7). Der konkrete Einwilligungstext ist durch die MII vorgegeben. Der Einwilligung ist eine Patienteninformation mit den relevanten Datenschutzinformationen beigefügt (Informationen zum Zweck der Nutzung von Daten und Biomaterialien, Rekontaktierungsmöglichkeit, Gültigkeitszeitraum, Widerrufsrecht und weitere Betroffenenrechte sowie Kontaktinformationen zum Datenintegrationszentrum, Datenschutzbeauftragten und Landesdatenschutzbehörde).

Auf Basis der unterzeichneten projektunabhängigen Patienteneinwilligung ist derzeit keine Übermittlung personenbezogener Daten an Drittstaaten außerhalb der EU vorgesehen. In Datennutzungsprojekten mit Übermittlung an Drittstaaten ist für dieses Projekt nach dem vorgegebenen Verfahren aus der UKJ-Richtlinie Datenschutz [vgl. 2, Abschnitt 4.1.6] vorzugehen.

Alle weiteren für die Umsetzung gesetzlicher Vorgaben notwendigen Vereinbarungen sind für ein jeweiliges Datennutzungsprojekt zu prüfen. Hierzu zählen insbesondere (vgl. auch Abschnitt 3.1):

- →Datennutzungsvertrag nach vorgegebenem Muster
- Projektkooperationsvertrag
- projektspezifisches Datenschutzkonzept, ggf. Datenschutzfolgeabschätzung
- Einträge in das Verzeichnis der Verarbeitungstätigkeiten für projektspezifische Verarbeitungsverfahren personenbezogener Daten
- Vertraulichkeits- und Verschwiegenheitsvereinbarungen mit externen Projektmitarbeitern
- Vereinbarungen zur Auftragsverarbeitung mit Dienstleistern für IT-Verfahren
- Vereinbarungen zur Gemeinsamen Verantwortung

Die Prüfung der Erforderlichkeit dieser Vereinbarungen wird durch ein vorgegebenes Verfahren im Arbeitsbereich Projektverwaltung des Datenintegrationszentrums unterstützt (→VA Projektvertragswesen).

8.5 Umsetzung von Informationspflichten

Im Rahmen eines Auskunftsersuchens sind Anfragenden Informationen über die Verarbeitung ihrer Daten (Zwecke, Kategorien, Empfänger, Speicherdauer) zur Verfügung zu stellen (vgl. Abschnitt 6.7). Hierfür erfolgt bezüglich einer Nutzung personenbezogener Daten für die biomedizinische Forschung eine Zuarbeit zum in der UKJ-Richtlinie Datenschutz beschriebenen Verfahren des Umgangs mit Anfragen betroffener Personen [vgl. 2, Abschnitt 4.1.4.2]. Die Zuarbeit erfolgt nach einem Textmuster als Anlage für das allgemeine Anschreiben zur Umsetzung der Auskunftsrechte. Dieses enthält

- Informationen über die Datenverarbeitung im Datenintegrationszentrum
- patientenfreundliche Beschreibung von Datennutzungsprojekten inklusive Weblinks
- Ansprechpartner für die benannten datenverarbeitenden Prozesse (DIZ-Leitung, Projektleitungen)

Die konkrete Umsetzung ist in einer entsprechenden Verfahrensanweisung geregelt (→VA Auskunftsersuchen). Für konkrete Datennutzungsprojekte sind entsprechende Angaben passgerecht zu erarbeiten und vorzuhalten.

Anhang

Quellen

[1] BMBF (Hrsg.): Medizininformatik: https://www.bmbf.de/de/medizininformatik-3342.html, abgerufen am 2.4.2021

[2] Universitätsklinikum Jena – Der Vorstand (Hrsg.): Richtlinie zur Umsetzung der gesetzlichen Datenschutzanforderungen am UKJ. 7.4.2021 (unveröff.)

[3] SMITH-Konsortium (Hrsg.): Datenschutzkonzept SMITH-Konsortium. Version 2.1, 10.3.2021 (unveröff.)

[4] K. Pommerening, Klaus; Drepper, Johannes; Helbing, K; Ganslandt, Thomas: Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF 2.0. Berlin: MWV, 2015 [Schriftenreihe der TMF; Bd. 11]. Aufzufinden auch unter https://mwv-open.de/site/books/10.32745/9783954662951/download/3140/, abgerufen am 2.4.2021

[5] Unabhängige Treuhandstelle der Universitätsmedizin Greifswald: Vorlage zum Verfassen eines Datenschutzkonzeptes für (multizentrische) Studien und Register. https://www.ths-greifswald.de/wp-content/uploads/2019/07/Musterdokument_Datenschutzkonzept_v1.6.pdf, abgerufen am 2.4.2021

[6] GMDS-Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG), ZTG Zentrum für Telematik und Telemedizin GmbH (Hrsg.): Leitfaden für die Erstellung von Datenschutzkonzepten im Gesundheitswesen. https://gesundheitsdatenschutz.org/html/datenschutzkonzept.php, abgerufen am 2.4.2021

[7] Medizininformatik-Initiative (Hrsg.): Mustertext zur Patienteneinwilligung. https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung, abgerufen am 2.4.2021

[8] Medizininformatik-Initiative (Hrsg.): Übergreifende Nutzungsordnung zum Austausch von Patientendaten, Biomaterialien, Analysemethoden und -routinen im Rahmen der Medizininformatik-Initiative. https://www.medizininformatik-initiative.de/de/nutzungsordnung, abgerufen am 3.4.2021

[9] Medizininformatik-Initiative (Hrsg.): Der Kerndatensatz der Medizininformatik-Initiative. https://www.medizininformatik-initiative.de/de/der-kerndatensatz-der-medizininformatik-initiative, abgerufen am 2.4.2021

Querverweise

- Datenschutzkonzept SMITH-Konsortium
- UKJ-Richtlinie zur Umsetzung der gesetzlichen Datenschutzanforderungen
- Einträge von DIZ-IT-Verfahren im UKJ-Verzeichnis der Verarbeitungstätigkeiten
- DIZ-Datenschutzfolgeabschätzung Clinical Domain
- DIZ-Datenschutzfolgeabschätzung Research Domain
- DIZ-Datenschutzfolgeabschätzung Trust Unit
- DIZ-Datenschutzfolgeabschätzung Data Sharing
- DIZ-Geschäftsordnung
- DIZ-Nutzungsordnung
- DIZ-Datennutzungsvertrag
- DIZ-IT-Sicherheitskonzept
- DIZ-Aufgabenbeschreibungen
- DIZ-Archivierungskonzept
- DIZ-VA Patienteneinwilligung
- DIZ-VA Einwilligungsverwaltung
- DIZ-VA Pseudonymisierung
- DIZ-VA Einwilligungswiderruf
- DIZ-VA Auskunftsersuchen
- DIZ-VA Re-Kontaktierung
- DIZ-VA Datenlöschung