

Handlungsleitfaden zur Erstellung eines Datenschutzkonzeptes für Forschungsprojekte

Leitfaden für Forschende, Stand 10/2024

Kontakt

Universität Bielefeld
Medizinische Fakultät OWL

Datenschutz- und
Informationssicherheitsmanagement der
Medizinischen Fakultät

Universitätsstraße 25
33615 Bielefeld

Datenschutz.medizin@uni-bielefeld.de

Inhalt

1. Zweck des Dokumentes	3
2. Darstellung des Forschungsvorhabens	3
3. Organisatorische Struktur	4
3.1. Verantwortlicher Verarbeiter	4
3.2. Beteiligte, Kooperationspartner, gemeinsam für die Verarbeitung Verantwortliche	4
3.3. Finanzierung durch Dritte	4
3.4. Internationale Aspekte	4
4. Studiendesign	5
4.1. Gesetzliche Rahmenbedingungen	5
4.2. Umfang der Verarbeitung von Daten bzw. Bioproben für das geplante Forschungsvorhaben	5
4.3. Beschreibung Art der Datenerhebung	6
4.4. Speicherung personenbezogener Daten	6
4.5. Ziele und Zweckbestimmung der weiteren Verarbeitung	6
4.6. Speicherbegrenzung	7
4.7. Pseudonymisierung	7
4.8. Anonymisierung und Löschung von personenbezogenen Daten und/oder Vernichtung von Bioproben	8
5. Rechtsgrundlage der Datenverarbeitung	8
6. Rechte der betroffenen Personen	9
7. Risikobestimmung, Schwellwertanalyse und Datenschutz-Folgenabschätzung	9
8. Technische und organisatorische Maßnahmen zur Sicherheit	10
9. Datenverarbeitung zur Qualitätssicherung	10
10. Anlagen	10

[Muster Datenschutzkonzept](#)

1. Zweck des Dokumentes

Diese Handreichung bietet Leitfragen für die Erstellung eines Konzepts zur Gewährleistung datenschutzrechtlicher Anforderungen in medizinischen Forschungsprojekten (Datenschutzkonzept). Ein Datenschutzkonzept konkretisiert die gesetzlichen Vorgaben und erleichtert den Nachweis über deren Einhaltung. Insbesondere Informationen für betroffene Personen wie z.B. Probanden, Verträge mit Kooperationspartnern und Anträge an Ethikkommissionen lassen sich auf Basis eines Datenschutzkonzepts einfacher erstellen.

Die Leitfragen dieser Handreichung orientieren sich an den Empfehlungen der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) AG Datenschutz.

Es sollten **zu allen nummerierten Gliederungspunkt** Angaben gemacht werden, wobei nicht jede Einzelfrage obligatorisch ist. Die Beantwortung der Leitfragen zielt auf eine nachvollziehbare Begründung, warum die Verarbeitung personenbezogener Daten im konkreten Forschungsvorhaben erforderlich und gegenüber den betroffenen Personen angemessen ist.

Nachgelagert an den Fragenkatalog ist ein Muster Datenschutzkonzept beigefügt, dass nach entsprechender Anpassung verwendet werden kann.

2. Darstellung des Forschungsvorhabens

Das Forschungsvorhaben soll beschrieben und seine Erforderlichkeit begründet werden. Der Nutzen des Vorhabens, insbesondere auch für die betroffenen Personen, soll dargestellt werden.

- Was ist das Ziel des Forschungsvorhabens? Wie soll es erreicht werden?
- Welche Fragestellungen, Anforderungen oder Herausforderungen sollen durch die Umsetzung des Vorhabens gelöst werden?
- Wie sind Behandlungs- und Forschungskontext im Rahmen des Forschungsvorhabens abgegrenzt?
- Wie weit kann mit anonymisierten oder pseudonymisierten Daten gearbeitet werden bzw. warum ist ein Personenbezug unvermeidbar?
- Wie lang ist die vorgesehene Laufzeit des Forschungsvorhabens?
- Ist eine Weiterführung des Forschungsvorhabens auch nach Ablauf der aktuellen Projektfinanzierung geregelt?
- Welche (Kooperations-) Partner sind an dem Vorhaben beteiligt?
- Wurde ein Ethikantrag gestellt?

3. Organisatorische Struktur

3.1. Verantwortlicher Verarbeiter

- Welche Organisationseinheit ist für die Forschung mit personenbezogenen Daten Verantwortlicher i.S.d. DSGVO (z. B. Universität/Institut/Klinik, andere Organisation)?
- Sind verantwortliche Entscheidungsträger, Administrator*innen sowie die jeweiligen Anwender*innen zur Vertraulichkeit verpflichtet und zum Datenschutz geschult?
- Wurde ein* Datenschutzbeauftragte*r für den / die Verantwortlichen bestellt und wie lauten die jeweiligen Kontaktdaten? Gibt es weitere Ansprechpersonen, die bei der Umsetzung des Datenschutzes unterstützen?

3.2. Beteiligte, Kooperationspartner, gemeinsam für die Verarbeitung Verantwortliche

- Welche anderen Organisationen, Partner und Institutionen sind beteiligt?
- Gibt es mehrere für die Verarbeitung Verantwortliche (vgl. Art. 26 DSGVO), falls ja, liegt eine Vereinbarung zur gemeinsamen Verantwortung vor?
- Gibt es Gründe für eine Beteiligung von Kooperationspartnern oder Dienstleistern und wenn ja, welche?
- Welche Funktionen bzw. Aufgaben übernehmen welche Partner und Stellen im Rahmen des Forschungsvorhabens?
- Wodurch wird die Zusammenarbeit im Forschungsvorhaben geregelt, z. B. Kooperations- oder Konsortialvertrag, Geschäftsordnung, Satzung?
- Werden Treuhänderdienste (Datentreuhänder, Vertrauensstelle) eingebunden und falls ja, wie?
- Gibt es vertragliche Regelungen über die Weitergabe von Bioproben?
- Welche organisatorischen Abhängigkeiten könnten Interessenkonflikte bei Durchführung des Forschungsprojekts auslösen, z.B. Auftragsforschung?

3.3. Finanzierung durch Dritte

- Wer fördert das Forschungsvorhaben und wie lange?
- Handelt es sich um ein drittmittelgefördertes Projekt?
- In welche Trägerschaft sollen personenbezogene Daten und Bioproben langfristig übergehen bzw. wie wird mit personenbezogenen Daten und/oder Bioproben nach Ablauf der Förderdauer oder des Forschungsvorhabens umgegangen?

3.4. Internationale Aspekte

- Welche ausländischen Projektpartner sind beteiligt?
- Ist die Nutzung von personenbezogenen Daten und/oder Bioproben durch ausländische Interessenten vorgesehen? Falls ja, auf welcher Rechtsgrundlage sollen personenbezogene Daten und/oder Biomaterialproben in das Ausland übermittelt werden, (z. B. EU-Raum, Angemessenheitsbeschluss der Europäischen Kommission, insbesondere Standardvertragsklauseln oder geeignete Garantien)?
- Welche Vereinbarungen oder Verträge mit ausländischen Partnern wurden getroffen?

4. Studiendesign

Bei Forschung im medizinischen Kontext werden regelmäßig sensible Datenkategorien gemäß Art. 9 DSGVO verarbeitet, z.B. Gesundheitsdaten oder genetische Daten. Bitte beschreiben Sie das Vorhaben in seinem regulatorischen Rahmen und das Vorgehen entlang des gesamten Data-LifeCycle, d.h. von der ursprünglichen Erhebung bis zur Löschung.

4.1. Gesetzliche Rahmenbedingungen

- Handelt es sich um eine klinische Studie, eine interventionelle oder nicht interventionelle Studie, sowie um eine prospektive oder retrospektive Studie?
- Erfolgt die Datenerhebung im Sinne einer Querschnittstudie oder Längsschnittstudie?
- Handelt es sich um eine klinische Prüfung (CTR / MDR)?
- Unterliegt das Forschungsvorhaben anderen Spezialgesetzen (wie z. B. Krebsregistergesetze, Sozialgesetzbücher, Bundesmeldegesetz)?
- Sollen personenbezogene Daten aus anderen Quellen mit speziellen gesetzlichen Rahmenbedingungen verwendet werden (z. B. Sekundärnutzung von Routinedaten, Meldedaten, Versicherungsdaten)?
- Sind spezifische Regelungen bei Sekundärnutzung von Behandlungsdaten zu beachten (z. B. Gesundheitsdatenschutzgesetz NRW, GDNG)?
- Sollen personenbezogene Daten und/oder Bioproben aus der Behandlungsdokumentation für das Forschungsvorhaben genutzt werden oder aus dem Forschungsvorhaben in eine Behandlungsdokumentation zugeführt werden (Schweigepflichtentbindung, Übermittlungserlaubnis)?
- Ist eine direkte Rückwirkung auf die Behandlung einzelner Patienten bzw. Probanden zu erwarten oder denkbar?

4.2. Umfang der Verarbeitung von Daten bzw. Bioproben für das geplante Forschungsvorhaben

- Welche Personen sind von der geplanten Datenverarbeitung betroffen (z.B. Patient*innen, Angehörige, Beschäftigte beteiligter Institutionen, externe behandelnde Ärzt*innen ...)?
- Betrifft das Forschungsvorhaben Kinder oder vulnerable Personen (z. B. nicht einwilligungsfähige Personen, abhängig Beschäftigte)?
- Wie sind Ein- und Ausschlusskriterien für Probanden definiert?
- Welche personenbezogenen identifizierenden Daten von welchen Personen sollen verarbeitet werden (z.B. Unterscheidung von Patient*innen-Anamnese-Daten und Diagnostik-Daten; sowie bei Beschäftigtendaten z. B. Personalverwaltungsdaten)?
- Welche personenbezogenen medizinischen Daten von welchen Personen/Personengruppen sollen verarbeitet werden?
- Sollen Biomaterialien entnommen und ggf. gelagert werden?
- Sollen andere besondere Kategorien personenbezogener Daten i.S.d. Artikel 9 DSGVO verarbeitet werden und falls ja, welche?

- Sollen personenbezogene identifizierende bzw. medizinische Daten und/oder Bioproben aus anderen eigenen Forschungsvorhaben genutzt oder von anderen Einrichtungen zur Verfügung gestellt werden (z. B. Biobank)? Wenn ja, von welcher Einrichtung und auf welcher Rechtsgrundlage (z. B. Einwilligungserklärung, Zweckänderung, Datennutzungsvertrag, Material Transfer Agreement)?
- Wenn die Daten nicht bei der betroffenen Person direkt erhoben werden: Wie wird die Information der betroffenen Person gemäß Art. 14 DSGVO sichergestellt?
- Welcher Einzugsbereich und welche Fallzahlen sind für das Forschungsvorhaben vorgesehen?

4.3. Beschreibung Art der Datenerhebung

- Wie erfolgt die Erhebung personenbezogener Daten (z.B. Befragung, Probenentnahme, Auswertung vorhandener Daten, Dokumentation durch Studienpersonal etc.) konkret?
- Wer ist verantwortlich für die Information der Probanden und ggf. die Einholung der Einwilligungserklärung nach Aufklärung? Wie und wie lange werden Einwilligungserklärungen aufbewahrt?
- Wer führt die Erhebung personenbezogener Daten und/oder Bioproben durch? Sind ggf. Partner an der Erhebung personenbezogener Daten und/oder Bioproben beteiligt?
- Wie und durch wen werden die personenbezogenen Daten bei der Erhebung qualitätsgesichert (z.B. Prüfung auf Plausibilität und Vollständigkeit)?
- Wie oft werden personenbezogene Daten einer einzelnen Person erhoben (Follow-ups)?

4.4. Speicherung personenbezogener Daten

- Wie erfolgt die Speicherung personenbezogener Daten (z.B. Papierform, eCRF etc.)?
- In welchem IT-System werden personenbezogenen Daten gespeichert und wer betreibt die zugehörigen Server?
- Werden die personenbezogenen Daten vor oder bei der Speicherung anonymisiert bzw. pseudonymisiert?
- Werden Daten übermittelt? Falls ja, zu welchem Zweck, an wen/von wem werden Daten übermittelt? Wurde ggf. eine vertragliche Vereinbarung über die Übermittlung geschlossen?
- Wie erfolgt ggf. die Zusammenführung der multizentrisch erhobenen personenbezogenen Daten?
- Werden die personenbezogenen Daten versioniert oder mit Hilfe eines Audit Trail Verfahrens dokumentiert (historisiert)?
- An welchem Ort / welchen Orten werden die Bioproben wie lange gelagert?
- Wie werden die Bioproben aufbewahrt (zentrale oder verteilte Biobank)?

4.5. Ziele und Zweckbestimmung der weiteren Verarbeitung

- Welche Auswertungen sollen von wem aus welchem Grund wann vorgenommen werden?

- Warum / zu welchem Zweck sind personenbezogene (ggf. pseudonyme) Daten zwingend erforderlich? Liegt eine detaillierte Bewertung der Notwendigkeit und Verhältnismäßigkeit der geplanten Verarbeitung für das Forschungsvorhaben vor?
- Wofür sollen die personenbezogenen Daten und/oder Bioproben primär und/oder sekundär genutzt werden (z. B. für Beobachtungsstudien, Hypothesengenerierung/Data Mining, Rekrutierung für künftige klinische oder epidemiologische Studien, translationale Forschung, medizinische Qualitätskontrolle)?
- Wer soll personenbezogene Daten und/oder Bioproben nutzen dürfen?
- Ist eine Weitergabe von personenbezogenen Daten und/oder Bioproben an andere interne und/oder externe Forschungsvorhaben vorgesehen? Falls ja, wie wird das Zugangsverfahren und die Übermittlung geregelt sein?
- Welche Schritte (z. B. Re-Identifizierung /Anonymisierung) sind für die Übermittlung der personenbezogenen Daten an Dritte notwendig?
- Fallen personenbezogene Meta-Daten während der Verarbeitung und/oder in den genutzten IT-Systemen an?

4.6. Speicherbegrenzung

- Werden nicht mehr benötigte identifizierende Daten gelöscht, wenn diese nicht mehr zwingend erforderlich sind? Nach welcher Frist und welcher Löschroutine?
- Lässt sich der Data-LifeCycle nachvollziehbar darstellen?

4.7. Pseudonymisierung

- Werden Probanden jeweils eindeutige Kennungen in Form von Pseudonymen zugeordnet? Wenn ja, welche Methodik und welche technischen Verfahren liegen dieser Zuordnung zugrunde?
- Unter welchen Bedingungen erfolgt eine Re-Identifikation?
- Wer hat Zugriff auf Zuordnungsschlüssel? Ist sichergestellt, dass die Anwender/Nutzer der pseudonymisierten Daten keinen Zugriff auf den Zuordnungsschlüssel erhalten und dass ein Abgleich der pseudonymisierten Daten mit den Daten der Echtumgebung ausgeschlossen ist?
- Wie wird gewährleistet, dass die Einhaltung der Bedingungen für eine Re-Identifikation in jedem Einzelfall durch den oder die Verantwortlichen geprüft und das Ergebnis dokumentiert wird?
- Falls verschiedene Pseudonyme verwendet werden: Wie erfolgt die Zuordnung?
- Ist der Einsatz von Record-Linkage-Verfahren geplant?
- Ist sichergestellt, dass die Zuordnungsschlüssel nach Beendigung des Verfahrens vernichtet werden?
- Ist gewährleistet, dass das Pseudonymisierungsverfahren alle identifizierenden Daten erfasst, ggf. auch Freitextfelder, Kommentarfelder, Anlagen usw.?
- Unter welchen Bedingungen könnte aus den pseudonymisierten Daten die Identität der betroffenen Personen auch ohne den Zuordnungsschlüssel ermittelt werden? Wie hoch ist der Aufwand?

4.8. Anonymisierung und Löschung von personenbezogenen Daten und/oder Vernichtung von Bioproben

- Welche Aufbewahrungsfristen existieren für welche Daten(arten) und/ oder gibt es Regelfristen zur Löschung der personenbezogenen Daten?
- Ist eine Anonymisierung der Daten für die Aufbewahrung möglich?
- Ist ein Anonymisieren der personenbezogenen Daten durch die Einwilligungserklärung abgedeckt oder liegt eine gesetzliche Erlaubnis hierfür vor (ggf. bitte benennen)?
- Existiert ein Anonymisierungskonzept und ist die Methodik der Anonymisierung dokumentiert? Erfolgt die Anonymisierung automatisiert und falls ja, wie und durch wen?
- Der Aufwand bei der Erlangung der originalen Information aus einem anonymisierten Datenbestand muss für jedermann unverhältnismäßig hoch sein. Ist dies gewährleistet?
- Gibt es Regelfristen zur Vernichtung der Bioproben?
- Werden Vergleichsproben zu Bioproben archiviert, die für wissenschaftliche Publikationen verwendet wurden? Wenn ja, wo und wie?
- Werden personenbezogene Daten nach dem Tod von Probanden gelöscht oder anonymisiert?
- Wie werden personenbezogene Daten archiviert, die für wissenschaftliche Publikationen verwendet wurden?

5. Rechtsgrundlage der Datenverarbeitung

- Wird die betroffene Person hinreichend aufgeklärt?
- Besteht Gelegenheit zu Rückfragen?
- Wird ein Mustertext genutzt und falls ja, welcher?
- Sofern die Verarbeitung nicht auf eine Einwilligung gestützt wird: Auf welche gesetzliche Erlaubnis soll die geplante Verarbeitung gestützt werden?
- Wird ein Mustertext für die Aufklärung verwendet und falls ja, welcher?
- Gibt es Anforderungen von Patientenorganisationen oder Ethikkommissionen hinsichtlich der Aufklärung von Probanden und an die Einwilligungserklärung und wie werden diese ggf. erfüllt?
- Ist eine separate Entbindung von einer gesetzlichen Schweigepflicht erforderlich?
- Sind alle geplanten Datenverarbeitungen beschrieben?
- Welche zusätzlichen Maßnahmen zur Transparenz werden für das Forschungsvorhaben eingerichtet (z. B. Öffentlichkeitsarbeit, Webpräsenz, Publikationsregeln)?
- Wie breit ist die Einwilligungserklärung formuliert? Handelt es sich um eine breiter angelegte Einwilligungserklärung, bei der ggf. nachinformiert wird, oder wird eine detaillierte, zweckgebundene Einwilligungserklärung eingesetzt?
- Ist die Kontaktierung von Probanden durch die Einwilligungserklärung abgedeckt (z. B. bei Zufallsfunden oder Follow-Ups)?

6. Rechte der betroffenen Personen

- Wer ist Ansprechpartner der Probanden zur Wahrnehmung ihrer Betroffenenrechte? Wie und wo werden die Kontaktdaten zum Ansprechpartner für Betroffenenrechte veröffentlicht bzw. mitgeteilt?
- Wie erfolgt die Identitätsfeststellung einer anfragenden Person?
- Wie können betroffenen Personen ihrer Einwilligungserklärung widerrufen (Mail, Telefon, persönlich, Komplettwiderruf, Teilwiderruf)?
- Wie sind die Ablaufprozesse gestaltet, wenn betroffene Personen ihr Recht auf Widerruf eine Einwilligung, Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben, Auskunft, Berichtigung oder Löschung ausübt?
- Welche Auswirkungen haben der Widerruf einer Einwilligungserklärung oder Erklärungen zum Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben, (z.B. Löschung, Vernichtung, Sperrung, Anonymisierung, Nutzungseinschränkung)?
- Wie können betroffene Personen ihr Recht auf Löschung von personenbezogenen Daten und/oder Vernichtung von Bioproben wahrnehmen, die sie selbst betreffen? Wie können betroffene Personen Auskunft und ggf. eine Kopie der über sie verarbeiteten personenbezogenen Daten und/oder Bioproben erhalten?
- Wie können betroffene Personen ihr Recht auf Einschränkung der Verarbeitung personenbezogener Daten und/oder Bioproben wahrnehmen?
- Wie erfolgt die Einschränkung der Verarbeitung personenbezogener Daten und/oder Bioprobe im Einzelnen? Liegen begründete Ausnahmen von der Verpflichtung zu Einschränkung der Verarbeitung vor?
- Wie wird die betroffene Person über die Aufhebung der Einschränkung der Verarbeitung personenbezogener Daten und/oder Bioproben unterrichtet?

7. Risikobestimmung, Schwellwertanalyse und Datenschutz-Folgenabschätzung

- Wurden etwaige Risiken für die Rechte und Freiheiten der betroffenen Personen aufgrund der Form der geplanten Datenerarbeitung im Forschungsvorhaben festgestellt (Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe)?
- Konnten geeignete und nachweisbar wirksame organisatorische und/oder technische Maßnahmen identifiziert werden, die die identifizierten hohen Risiken für die Rechte und Freiheiten der betroffenen Personen ausreichend eindämmen? Falls nein: Wurde gemäß Art. 35 DSGVO eine Datenschutz-Folgenabschätzung durchgeführt?
- Wurden ggf. die Standpunkte der betroffenen Personen oder ihrer Vertreter eingeholt?
- Wurden geeignete Prozesse eingerichtet, um Änderungen der mit der Verarbeitung personenbezogener Daten und/oder Bioproben verbundenen Risiken zu überwachen bzw. auf Ihre Wirksamkeit zu überprüfen?

8. Technische und organisatorische Maßnahmen zur Sicherheit

- Liegt ein Sicherheitskonzept betreffend die genutzten Datenverwaltungssysteme vor? Ggf. als erforderlich erkannte Ergänzungen beschreiben.
- Wurde ein projektspezifisches Rollen- und Berechtigungskonzept erstellt? Wird dessen Einhaltung protokolliert und stichprobenartig überprüft?
- Besteht ein ausreichendes Back-up / Recovery-Konzept?

9. Datenverarbeitung zur Qualitätssicherung

- Gibt es ein Monitoring-Verfahren? Welche Daten sieht der Monitor und welche Bearbeitungsrechte (z.B. Sperren, Löschen) hat er (z.B. gemäß Monitoring Manual)?
- Welche Datenqualitätssicherungsverfahren werden für das Forschungsvorhaben vorgesehen? In welcher Form werden qualitätssichernde Maßnahmen in den einzelnen Arbeitsmaßnahmen integriert und wirksam nachgehalten?
- Gibt es ein internes Auditverfahren und wie sieht es aus (Beschreibung)? Wer kontrolliert die Einhaltung der technischen und organisatorischen Sicherheitsmaßnahmen?

10. Anlagen

Einige zur Darstellung der Einhaltung des Datenschutzes bzw. zur Erfüllung datenschutzrechtlicher Anforderungen werden ggf. in externen Dokumenten dargestellt. Bitte benennen Sie hier alle Dokumente, aus denen sich ggf. ergänzend zu diesem Datenschutzkonzept datenschutzrechtliche Anforderungen ergeben.

Beispielsweise:

- Datenflussdiagramm
- Berechtigungskonzepte für zentrale Datenverwaltungssysteme
- Dokumente zur Patienteninformation, Aufklärung, Einwilligung
- Antrag an die Ethikkommission / Ethik-Votum
- Verträge (insb. Kooperationsvertrag, Prüfzentrumsvertrag, Material Transfer Agreement, Gemeinsame Verantwortung, Auftragsverarbeitungsvertrag)
- Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO beteiligter Stellen

Datenschutzkonzept für Studien außerhalb von
Arzneimittelgesetz (AMG) oder Medizinproduktegesetz (MPG):

xx-Studie

Version 1.0, 13.09.2024, Draft

Abkürzungsverzeichnis

CDMS	Clinical Data Management System
CV	Curriculum Vitae
DMZ	Demilitarized Zone
DSGVO	Datenschutz-Grundverordnung
eCRF	Electronic Case Report Form
EU	Europäische Union
DSGVO	Datenschutz-Grundverordnung der Europäischen Union
GCP	Good Clinical Practice
https	Hypertext Transfer Protocol Secure
ICH	International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use
ISF	Investigator Site File, auch Prüfarztordner
Patienten-ID	Patienten-Identifizierungscode
QM	Qualitätsmanagement
SOP	Standard Operation Procedure
TMF	Trial Master File
TOMs	Technisch-organisatorische (datenschutzrechtliche) Maßnahmen

Inhalt und Zweck der Studie/Datenverarbeitung

In der Studie werden personenbezogene medizinische Daten (Studiendaten, Gesundheitsdaten und Bilddaten) von Patient*innen zum Zweck Beschreibung Studieninhalt erfasst, verarbeitet, analysiert, gespeichert und archiviert.

Die Studie ist eine multizentrische nationale klinische Studie. Diese wird federführend durch die Einrichtung unter Leitung von Studienleitung durchgeführt.

Die Studie soll in ca. Anzahl deutschen Zentren durchgeführt werden. Sponsor ist Einrichtung. Der Sponsor überträgt seine Pflichten im Innenverhältnis an die Studienleitung: Name. Der Sponsor bevollmächtigt die Studienleitung im Rahmen der vertragsgegenständlichen Studie zur Vertretung des Sponsors im Außenverhältnis mit Ausnahme von Vertragsvorbereitung und Vertragsvollmacht. In einer Vereinbarung über die Studie wird die Kooperation zwischen Einrichtungen schriftlich festgelegt.

Bei der Studienplanung und -durchführung wird die Studienleitung durch Einrichtung unterstützt. Die an Einrichtung delegierten Aufgaben sind in einer Dienstleistungsvereinbarung über ein Forschungsvorhaben in Kooperation zwischen Einrichtungen festgelegt, dazu gibt es eine entsprechende Task Allocation List, die als Bestandteil an die Dienstleistungsvereinbarung gekoppelt ist.

Die Studie wird durch Fördermittelgeber als Projektträger finanziert.

Neben medizinischen Patient*innendaten werden Daten von Mitarbeiter*innen in den Studienzentren (Studienpersonal), an Einrichtung und weiteren zentralen Leistungserbringern (Projektteam) zur Erfüllung der gesetzlichen Anforderungen (ICH E6 (R2) - GCP (Good Clinical Practice) Guideline, GCP-Verordnung, Datenschutz-Grundverordnung (DSGVO) und das Landesdatenschutzgesetz der betroffenen Bundesländer, sowie weiteren Datenschutzbestimmung, wie dem Kirchlichen Datenschutz-Gesetz (KDG) verarbeitet: z. B. Kontaktdaten, Lebensläufe (CVs) und Trainingszertifikate. Zur Organisation der Studie werden Daten wie z. B. Namen, dienstliche Telefonnummern, dienstliche E-Mail-Adressen in entsprechenden Kontaktlisten gesammelt.

In allen Prüfzentren werden Daten nach prüfzentrums-spezifischer Verordnung erhoben. Aus diesem Grund sind die Prüfzentren verantwortlich für die Einhaltung der jeweiligen Verordnungen und Gesetzeslagen.

Sobald Daten jeglicher Art an Dritte übermittelt werden, werden diese Daten nach DSGVO und diesem Datenschutzkonzept verarbeitet.

Rechtsgrundlagen für die Datenverarbeitung

Rechtsgrundlagen für die Verarbeitung von Daten der Studienteilnehmenden

Rechtsgrundlage für die Datenerhebung ist Art. 6 (1a) in Verbindung mit Art. 9 (2a) der EU-Datenschutz-Grundverordnung (DSGVO) und somit eine freiwillige, informierte Einwilligung der Patient*innen. Die datenschutzrechtliche Einwilligung ist mit der Einwilligung zur Teilnahme an der Studie verknüpft, d. h. ohne eine datenschutzrechtliche Einwilligung kann der Betroffenen nicht an der Studie teilnehmen. Genaueres s. [Anlage](#).

Rechtsgrundlagen für die Verarbeitung von Daten der Studienmitarbeitenden

Rechtsgrundlagen für die Verarbeitung von Daten der Studienmitarbeitenden sowie von Daten des Projektteams bestehen:

- im öffentlichen Interesse an der Forschung nach Artikel 6 Abs. 1 lit. e DSGVO in Verbindung mit **Gesundheitsdatennutzungsgesetz**
- aufgrund berufsethischer Erwägungen bzw. zur Erfüllung guter wissenschaftlicher Praxis. In der Berufsordnung der **Landesärztekammer** und in der Muster-Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (der **Bundesärztekammer**) steht, dass Ärzte bei Forschung am Menschen die in der Deklaration von Helsinki niedergeschriebenen Grundsätze für die medizinische Forschung beachten. In der Deklaration von Helsinki steht wiederum, dass Forschungsvorhaben, an welchen Versuchspersonen beteiligt sind in einer öffentlich zugänglichen Datenbank zu registrieren sind.
- aufgrund **Landeshochschulgesetz Nordrhein-Westfalen** zum Zwecke der des Nachweises der Verwendung von Förder- und Drittmittel gegenüber **Fördermittelgeber**.

Genauerer hierzu im studienspezifischen Mitarbeiterinformationsblatt (siehe **Anlage** des Studienzentrenvertrages). Diese Mitarbeiter*inneninformation wird durch den (lokalen) Studienleitung an die an der Studie beteiligten Mitarbeiter*innen seines Zentrums gegeben.

Rechtsgrundlagen für die Verarbeitung von Studienmitarbeiterdaten bei Kooperationspartnern

Rechtsgrundlage für die Verarbeitung von Daten des **Studienpersonals externer Zentren** sind die Zentrumsverträge, die zwischen **Einrichtung** und externen Studienzentren geschlossen werden. Dort verpflichtet sich das externe Zentrum bzw. der Studienarzt/Studienärztin, die Mitglieder seiner Studiengruppe entsprechend zu informieren und eine rechtskonforme Datenweitergabe an **Einrichtung** sicherzustellen.

Verantwortlicher für die Datenverarbeitung

Datenschutzrechtlich verantwortlich gem. Art. 26 DSGVO ist **Einrichtung** gemeinsam mit dem/der jeweils verantwortlichen Studienarzt/Studienärztin an den teilnehmenden Zentren.

Die Aufgaben und Verantwortlichkeiten zwischen der **Einrichtung** und einem teilnehmenden Zentrum sind in einem datenschutzrechtlichen **Zusatzvertrag** zwischen **Einrichtung** und teilnehmenden Zentrum oder einer entsprechenden verbindlichen datenschutzrechtlichen **Anlage** zu einem **Hauptvertrag** (Zentrumsvertrag) festgelegt.

Genauerer siehe studienspezifisches Zusatzvertragstemplate bzw. studienspezifischer Anhang zum Hauptvertrag (kurz: „Studienzentrumsvertrag“, siehe **Anlage**). Der Zusatzvertrag oder der Anlage zum Hauptvertrag hat wiederum einen TOM-Anhang welcher die technischen und organisatorischen Maßnahmen (kurz TOM) der **Einrichtung** und des teilnehmenden Zentrums tabellenartig auflistet.

An den teilnehmenden Zentren wird jeweils ein lokal datenschutzrechtlich Verantwortlicher ermittelt. Dieser wird auch in der lokal angepassten Patienteninformation benannt.

Betroffener Personenkreis

Studienpatient*innen: Die Rekrutierung erfolgt in den teilnehmenden Zentren im Rahmen der Patient*innenbehandlung aufgrund der Daten in den Patient*innenakten und in Übereinstimmung mit den Ein-/Ausschlusskriterien der **Studie**. Studiendaten werden erst nach schriftlicher Einwilligung des Patienten als Studiendaten erfasst und in die zentrale Studiendatenbank weitergeleitet.

Studienpersonal: Alle Beteiligten in den teilnehmenden Zentren: ärztliche und nicht-ärztliche Mitglieder des Studienteams, etc.

Projektteam: Mitarbeiter*innen der zentralen Studienkoordination an **Einrichtung**, sowie Mitarbeiter*innen der **Einrichtung**.

externer Projektmitarbeiter: Mitarbeiter des **Projektpartners**.

Festlegung der Art der personenbezogenen Daten und Proben

Erhobene Daten der Studienpatienten

Behandlungsdaten (source data)

Daten der Studienpatient*innen werden an den Studienzentren erhoben und verbleiben dort in der Patient*innenakte. Zu diesen „Quelldaten“ („source data“) gehören:

Erhobene Daten	Studienpatient*innen
Name, Vorname	<input checked="" type="checkbox"/>
Studienspezifische Patienten-ID (Vergabe s. Kapitel 0)	<input checked="" type="checkbox"/>
Daten zur Person: Alter, Geschlecht	<input checked="" type="checkbox"/>
Anamnesedaten (Ein- Ausschlusskriterien)	<input checked="" type="checkbox"/>
Berichte von vorherigen studienrelevanten Untersuchungen	<input checked="" type="checkbox"/>

Studiendaten (CRF study data)

Alle studienrelevanten Daten (**Studiendaten**, CRF study data, Daten aus den Patient*innenfragebögen) sind im Prüfplan der Studie definiert. Sie werden in pseudonymisierter Form an den Sponsor weitergeleitet (s. **Kapitel 0**). Alle Daten, die an den Sponsor weitergeleitet werden, müssen als Quelldaten in der Patientenakte am Studienzentrum vorliegen.

Erhobene Daten des Studienpersonals, Projektteams und weiterer Beteiligter

Erhobene Daten	Studienpersonal	Projektteam	externer Projektmitarbeiter*innen
dienstliche Kontaktdaten	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Daten über die Beteiligung/Funktion an Studie	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Angaben zum beruflichen Lebenslauf	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Aufzeichnungen über die Ausbildung/Qualifikation/Schulungen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Informationen zur tariflichen Eingruppierung und Vertragslaufzeit	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Datenerhebung, Datenweitergaben und Speicherorte/Speicherung

Datenerhebung

Im Studienzentrum werden die studienpezifisch relevanten Daten der **Studienpatient*innen** durch schriftlich autorisiertes Studienpersonal aus den **Source-Data** in einem electronic Case Report Form (eCRF) in pseudonymisierter Form (s. **Kapitel 0**) dokumentiert. Verwendet wird das **System** zur Erfassung, Verwaltung und Verifizierung von Patient*innendaten via eCRFs in klinischen Prüfungen (Beschreibung des Systems s. **Kapitel 0**). Mit dem **System** werden die Daten vom teilnehmenden Zentrum zur **Einrichtung** transferiert.

Die Daten der Fragebögen (ausgefüllt von **Studienpatient*innen**) zu den studienrelevanten **Parametern** werden von den Patient*innen auf Papierbögen eingetragen, die mit der Patienten-ID und dem Datum des Ausfüllens gekennzeichnet sind. Diese Daten werden von Mitarbeiter*innen

des Prüfzentrums in die **System-Studiendatenbank** eingegeben.

Die Daten des **Studienpersonals** werden von den Zentren an **den Sponsor / an die vom Sponsor beauftragte Einrichtung** gesendet.

Daten für die Anlage eines Accounts für die Nutzung der Datenbank (Name, Information zur Rolle im System, E-Mail-Adresse) werden an die **Einrichtung** versendet, dort überprüft und verarbeitet. Anschließend werden die erforderlichen Zugangsdaten versendet. Nachweise der Autorisierung des Studienpersonals (z. B. Delegation Log, Studien-Trainingslog, eCRF-Trainingsliste) sind gleichzeitig auch im Prüfarztordner (Investigator Site File (ISF)) am Zentrum abgelegt.

Die Daten des **Projektteams** und weiterer **externer Beteiligter** werden vom Projektteam der **Einrichtung** gesammelt.

Alle Daten können durch Clinical Research Associates (CRAs) geprüft werden.

Datenweitergaben von Studiendaten (eCRF study data)

Die Rechtsgrundlagen, auch für Weitergaben nach diesem **Kapitel 0** sind in **Kapitel 0** beschrieben.

Datenweitergabe innerhalb des Studienzentrums

Die Datenweitergabe von Studienpatient*innen an das Studienpersonal zur Eingabe in den eCRF wird in **Kapitel 0** näher beschrieben.

Studienzentren an Sponsor

Zur Datenerhebung und Dokumentation im eCRF s. **Kapitel 0**.

Zum Zweck der Bereitstellung von pseudonymisierten Studiendaten für den Sponsor werden die Studiendaten in das eCRF des **Systems** eingegeben. Zur biostatistischen Analyse werden die Daten aus **System** exportiert und als SAS-Tabellen auf dem Studienserver der **Einrichtung** zur Verfügung gestellt.

Sponsor an den Projektträger/Förderer

Die Studie wird durch das **Fördermittelgeber** gefördert. **Turnus** erhält der **Fördermittelgeber** einen Statusbericht, der aggregierte Daten zum Rekrutierungsverlauf enthält.

Beschreibung Board und Komitee

Welche Einrichtungen sind noch beteiligt, erhalten Daten?

Sponsor an den Projektträger

Im Antrag auf Förderung werden Namen sowie die Tarifeinstufungen von Inhabern geförderter Personalstellen an den **Förderer** weitergeleitet. Dieses geschieht aufgrund gesetzlicher Vorgaben und mit dem Einverständnis der entsprechenden Personen. Im Rahmen der geforderten **turnus** Berichterstattung kann es ggf. in Einzelfällen zum Transfer von Namen von Inhabern geförderter Personalstellen kommen, Patienten-IDs werden in diesen Berichten nicht weitergegeben.

Weitergaben von Daten der Studienmitarbeitenden

Zu den Rechtsgrundlagen der Weitergaben von Daten der Studienmitarbeitenden (s. **Anlage**).

Sponsor an Ethikkommissionen

Einrichtung schickt im Auftrag des Sponsors CVs von Studienärzt*innen an die zuständigen

Ethikkommissionen. Außerdem werden die Namen von Studienärzt*innen und Beauftragten des Sponsors an die Ethikkommissionen gemeldet. Liste der für die Studienzentren zuständigen Ethikkommissionen: [siehe](#).

Speicherorte

Die Speicherorte ergeben sich aus den beschriebenen Erfassungen und Weitergaben aus den [Kapiteln 0 bis 0](#).

Weitere Erläuterungen zu einzelnen Speicherorten

Die Studiendaten werden innerhalb des Systems der Einrichtung pseudonymisiert gespeichert. Die dazugehörige Studiendatenbank befindet sich auf einem System, dessen Administration durch das Einrichtung stattfindet.

Studienspezifisch relevante Quelldaten wie z.B. Patientenfragebögen werden in den regulären Patient*innenakten aus der klinischen Behandlung abgelegt (s. [Kapitel 0](#)).

Die Dokumente mit Daten des Studienpersonals und des Projektteams werden in Papierform im ISF am Studienzentrum und im Trial Master File (TMF) bei Einrichtung abgelegt, sowie digital auf Servern der Einrichtung gespeichert.

Berichte werden sowohl im ISF am Zentrum als auch im TMF in Einrichtung abgelegt.

Datenanalyse

Analyse von Studiendaten

Die Auswertung der pseudonymisierten Studiendaten erfolgt durch den Bereich an Einrichtung. Hierzu wird zunächst ein statistischer Analyseplan erstellt, auf dessen Basis die Analysen programmiert und validiert werden. Für die Datenanalyse werden die Studiendaten durch das Datenmanagement aus System exportiert und der Biometrie als SAS-Tabellen auf dem Studienserver der Einrichtung zur Verfügung gestellt. Auf der Basis der Daten werden die Studienergebnisse sowohl in pseudonymisierter oder anonymisierter als auch in aggregierter Form (Diagramme, Graphiken, Tabellen, Listings etc.) dargestellt.

Außerdem werden die Studienergebnisse in wissenschaftlichen Zeitschriften, bei wissenschaftlichen Kongressen/Konferenzen/Tagungen und im öffentlich einsehbaren Deutschen Register Klinische Studien unter der -Identifikationsnummer Nummer veröffentlicht. Die Veröffentlichung erfolgt ausschließlich in anonymisierter und aggregierter Form.

Datenarchivierung

Am Studienende werden in System sämtliche Benutzerzugänge gesperrt und die Studie vom Produktiv-Status („Production“) in den Archiv-Status („Analysis“ bzw. „Completed“) überführt. Der Studienverzeichnisbaum auf dem Studienserver mit den exportierten Rohdaten und den daraus erstellten Analysedaten wird nach Löschen der Zugangsrechte in ein Archivverzeichnis verschoben. Nach dem Ende der regulatorisch vorgegebenen Archivierungspflicht werden die Daten gelöscht.

ISF und TMF werden nach Beendigung der Studie nach den aktuellen gesetzlichen Vorgaben archiviert. Im ISF wird im Studienzentrum vor Ort archiviert, der TMF in Einrichtung.

Pseudonymisierungsverfahren

Wie im Prüfplan beschrieben, wird ein Pseudonym (Forschungspseudonym) bei der Registrierung eines*r Patient*in vergeben. Dieses Pseudonym besteht aus einer eindeutigen Zentrumsnummer und einer pro Zentrum fortlaufenden Patient*innenummer. Die Eindeutigkeit wird durch eine Registrierung im eCRF gewährleistet. Eine Doppelvergabe einer Patienten-ID ist dadurch ausgeschlossen. Es werden keine Initialen oder sonstigen identifizierenden Daten für die Erstellung

des Pseudonyms verwendet.

Betroffenenrechte

Art der Rechte

Die Betroffenen haben gem. DSGVO (Kapitel III, Art. 12-23) Recht auf:

- **Auskunft** (Art. 15 DSGVO) über ihre im Rahmen der Studie verarbeiteten personenbezogenen Daten
- **Berichtigung** (Art. 16 DSGVO) ihrer personenbezogenen Daten, wenn diese unvollständig oder falsch sein sollten.
- **Einschränkung der Verarbeitung** (=Sperrung, Art. 18 DSGVO), z. B. wenn Sie die Richtigkeit der betreffenden Daten beanstanden, für die Dauer der Überprüfung dieser Beanstandung
- **Widerruf** (Art. 7 Abs. 3 DSGVO) ihrer Einwilligung zur Verarbeitung ihrer personenbezogenen Daten (der Widerruf für Studienteilnehmer ist in der Studie jedoch beschränkt; siehe Recht auf Löschung)
- **Löschung** (Art. 17 DSGVO) ihrer personenbezogenen Daten. Es gibt jedoch Ausnahmen von diesem Recht: Ein Recht auf Datenlöschung besteht nicht, wenn durch dessen Inanspruchnahme die wissenschaftlich korrekte Durchführung des Forschungsvorhabens unmöglich gemacht oder ernsthaft beeinträchtigt würde.

Genauerer siehe [Anlage](#).

Umsetzung von Betroffenenrechten:

Der/die Betroffene (d. h. der/die Studienpatient*in) wird beim ärztlichen Aufklärungsgespräch gebeten, sich mit Anfragen zur Wahrnehmung seiner Betroffenenrechte vorzugsweise an das Studienzentrum zu wenden (siehe [Anlage](#)). Ggf. kann auch der Sponsor (Studienleitung) oder die Einrichtung von dem/der Patienten/in kontaktiert werden. Mit einer Beschwerde bezüglich des Datenschutzes kann sich der/die Patient*in an die zuständigen Aufsichtsbehörden wenden. Alle Kontaktdaten (Postanschrift, Telefon, E-Mail) sind in der Patienteninformation genannt.

Die Person bei Einrichtung, die das Begehren erhält, dokumentiert das Begehren im Ort, und informiert Funktion/Einrichtung. Funktion/Einrichtung klärt zusammen mit dem gesamten Projektteam der Einrichtung, dem Datenschutzbeauftragten das weitere Vorgehen im Einzelfall. Je nach Inhalt und Umfang der Anfrage wird auch der Leitung der klinischen Prüfung einbezogen.

Im Allgemeinen gilt Folgendes:

- Um einen Überblick über die auf die Begehren folgenden Prozesse zu haben, werden diese im Ort getrackt.
- Zur Dokumentation der Aktionen werden Aktennotizen erstellt, von den beteiligten Akteuren der Einrichtung, ggf. auch vom Studienleiter unterschrieben und im TMF abgelegt.
- Das Studienzentrum informiert den*die Patient*in abschließend über die ergriffenen Maßnahmen.

Richtlinien für Maßnahmen bei Betroffenenbegehren

Auskunftsbegehren

Alle etwaigen Auskünfte erteilt das Studienzentrum nur nach Rücksprache mit der Studienleitung/Sponsor/Einrichtung. Über Daten aus Audittrails wird generell keine Auskunft erteilt.

Berichtigungsbegehren

Eine Berichtigung der gespeicherten Daten im eCRF erfolgt durch die Einrichtung, oder durch das

Prüfzentrum nach Rücksprache mit der **Einrichtung**.

Einschränkung der Verarbeitung (=Sperrung)

Die Sperrung der gespeicherten Daten veranlasst **Einrichtung/Funktion**. Eine Sperrung kann wieder aufgehoben werden, wenn die betroffene Person die Sperrung zurück nimmt oder, wenn von **Einrichtung** festgestellt wird, dass das Sperrbegehren unbegründet ist und die betroffene Person zuvor über die Aufhebung der Sperrung informiert wurde. In welcher Form Daten gesperrter Patient*innen ausgewertet, oder ob diese Patient*innendaten aus der Auswertung ausgeschlossen werden, muss im Einzelfall geklärt werden.

Widerruf

Die Einwilligung zur Erhebung und Verarbeitung der personenbezogenen Daten ist widerruflich. Widerruft ein*e Patient*in seine*ihre Einwilligung zur Datenverarbeitung, werden die notwendigen Prozesse von **Einrichtung/Funktion** der Einrichtung nach Rücksprache mit dem Studienzentrum organisiert. Die Rechtmäßigkeit der bis zu einem solchen Widerruf erfolgten Datenverarbeitung wird davon nicht berührt.

Löschung

Eine Löschung der gespeicherten Daten erfolgt nach Widerruf der Einwilligung zur Datenspeicherung (bzw. nach Widerruf der Teilnahme an der Studie), sofern die Daten der betroffenen Person noch nicht anonymisiert sind. **Einrichtung** führt eine Prüfung durch, ob ein Löschantrag besteht. Sollen personenbezogene Daten gelöscht werden, informieren sich die Beteiligten (Studienzentrum, **Einrichtung**, Studienleiter) zuvor gegenseitig und sprechen sich ab. Falls eine Löschung erfolgt, wird diese dokumentiert.

Anlaufstelle bei Fragen

Patient*innen können sich mit Fragen zum Datenschutz an die in der Patienteninformation benannten Verantwortlichen für die Datenverarbeitung in der Studie (die benannte lokale Studienleitung, die Studienleitung oder die benannten Datenschutzbeauftragten) richten (s. **Anlage**).

Beschwerdestellen

Bei Beschwerden im Zusammenhang mit dem Datenschutz (Art. 77, DSGVO) können sich die Betroffenen im Rahmen der **Studie** an die **Einrichtung (Sitz des Sponsors)** zuständige Aufsichtsbehörde wenden oder an die jeweilige Aufsichtsbehörde des Studienzentrums (s. **Anlage**).

Technische Ausgestaltung

Die Patient*innenregistrierung und die Zuteilung der Patienten-ID veranlasst das Studienzentrum über **System**. Im Prüfzentrum werden auch die studienspezifisch relevanten Daten der Studienpatienten durch schriftlich autorisiertes Studienpersonal, (festgehalten auf einem Delegation-Log) in den eCRF eingeben.

Qualitätssicherung, Monitoring

Das Monitoring und damit die Qualitätskontrolle im Prüfzentrum erfolgt durch **Einrichtung** auf der Grundlage der folgenden Standard Operation Procedures (SOPs) der **Einrichtung**:

- **ABC**

Durch das Monitoring auf der Grundlage von ICH-GCP E6 (R2) werden auch die datenschutzrechtlich relevanten Aspekte der Studie überwacht. Dazu wird das Studienpersonal in der Initiierungsvisite vor Beginn der Patientenrekrutierung geschult in Bezug auf:

- die Bestimmungen der Datenschutzgesetze
- die Pflicht zur Aufklärung der Patienten über deren Datenschutzrechte
- die Weiterleitung von Daten des Studienpersonals

wird während der Studie im Rahmen von on-site Visits überprüft, dass:

- die Studie unter Einhaltung der gesetzlichen Bestimmungen zum Datenschutz durchgeführt wird,
- Einwilligungserklärungen der Patienten vorliegen,
- neues Studienpersonal entsprechend geschult und die Schulung dokumentiert ist.

Der Umfang dieser Maßnahmen und die Frequenz der Visiten werden an die jeweiligen Prüfzentren nach Bedarf angepasst.

Monitore und Auditor*innen im Auftrag des Sponsors sowie die zuständigen Überwachungsbehörden können am Prüfzentrum Einsicht in personenbezogene Daten nehmen soweit dies für die Überprüfung der ordnungsgemäßen Durchführung der Studie notwendig ist. Die Patienten werden darüber in der Patienteninformation informiert und willigen entsprechend ein.

Technisch-organisatorische Maßnahmen (TOMs)

Allgemeine Maßnahmen:

Studiendokumente werden in den Studienzentren im Prüfarztordner (ISF) und beim Sponsor/Studienleiter/Einrichtung im TMF in abschließbaren Schränken gelagert, die Räume dürfen nur mit Zugangsberechtigung betreten werden.

Der Zugang zu Studiendaten im eCRF ist nur mit persönlichem Login-Passwort möglich. Im Audit-Trail werden Datenmanipulationen jeglicher Form und wer diese vornimmt dokumentiert. Es wird weiterhin dokumentiert wer Eingaben oder Änderungen vornimmt, wer Queries stellt oder beantwortet etc. Es wird dokumentiert wer welchen Zugang, zu welchen Daten und mit welchen Rechten in welchem Zeitraum hat.

- Pseudonymisierung von Studiendaten:

Originale Quelldaten, also Patient*innendaten, werden im eCRF ausschließlich pseudonymisiert erfasst, das heißt mit einer eindeutigen, einmalig vergebenen Nummer, bestehend aus einer Zentrumsnummer und einer pro Zentrum fortlaufenden Zahl. Nur das Studienpersonal des jeweiligen Zentrums führt die Liste, mit deren Hilfe Pseudonym und Studienpatient/in zugeordnet werden können. Diese Liste wird im Prüferordner (ISF) abgelegt.

Gewährleistung der Vertraulichkeit des eCRF :

Der Zugang zu den Daten des eCRF ist durch ein umfangreiches Rechte- und Rollenkonzept von System eingeschränkt.

Gewährleistung der Integrität von System:

System ist ein GCP-konformes Klinisches Datenmanagement System, abgekürzt auch CDMS (Clinical Data Management System). Sämtliche Änderungen am System oder an der Datenbank unterliegen dem Change Management-Prozess der Einrichtung. Ein dokumentierter Test jeder Änderung wird zunächst am Testsystem durchgeführt, bevor das Produktivsystem mit den laufenden Studien aktualisiert wird. Die Studiendatenbank wird von Funktion der Einrichtung aufgesetzt und wird während der Erstellung regelmäßig vom Entwickelnden getestet. Vor Freigabe unterläuft die Studiendatenbank einer umfangreiche Validierung durch eine

unabhängige Person.

Gewährleistung von Verfügbarkeit und Belastbarkeit von System:

Die Übertragung von pseudonymisierten Patient*innendaten zum System erfolgt verschlüsselt über https (Hypertext Transfer Protocol Secure). Entwickelt wurde System von Einrichtung. Für die Verwendung bei Einrichtung wird das System gehostet bei Einrichtung. Es besteht aus einem Applikations- und einem Datenbankserver. Der Applikationsserver befindet sich in der DMZ (Demilitarized Zone), der Datenbankserver befindet sich im internen Netz. Ein direkter Zugriff auf den Datenbankserver von extern ist somit nicht möglich. Betrieben wird der Applikationsserver und der Datenbankserver von Einrichtung. Die Betriebssysteme beider Server werden regelmäßig aktualisiert. Die Applikationsserversoftware wird bei Bedarf aktualisiert.

Die virtuellen Maschinen des Systems werden Anzahl Tage tagessichert. Für System besteht eine maximale erlaubte Downtime von Anzahl Stunden.

Für System existiert ein virtuelles Testsystem. Das Testsystem wird dazu benutzt, Softwareupdates zuerst darin einzuspielen, um ggf. auftretende Probleme frühzeitig und ungefährlich für das Produktivsystem erkennen zu können. Softwareupdates auf dem Produktivsystem werden erst dann installiert, wenn sich die Installation auf dem Testsystem als unproblematisch herausgestellt hat. Vor einem Softwareupdate haben die Administratoren zusätzlich die Möglichkeit sogenannte „snapshots“ zu erstellen, um bei auftretenden Problemen sehr einfach auf den Stand von vor dem Softwareupdate gehen zu können.

Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

Der Datenschutz bei Einrichtung ist Teil eines Qualitätsmanagementsystems und unterliegt somit den allgemeinen QM-Verfahren für regelmäßige Überprüfung, Bewertung und Evaluation.

Verzeichnis der Verarbeitungstätigkeiten (DSGVO, Art. 30)

Für die Studie wird durch den datenschutzrechtlich Verantwortlichen das Verzeichnis der Verarbeitungstätigkeiten eingetragen und gepflegt.

Dokumentenfreigabe

Ort, Datum
[TT.MM.JJJJ]

Studienleitung

Unterschrift

Ort, Datum
[TT.MM.JJJJ]

Datenschutz

Unterschrift

Anlagen