Datenschutzkonzept zum Projekt Mobile WohnortnAhe Versorgung zur Steuerung der Sektor-übergreifenden Therapie bei Post-COVID-19 in THüringen (WATCH)

1. Einleitung

Das übergreifendes Projektziel von WATCH ist eine verbesserte Versorgung behandlungsbedürftiger Post-COVID-Patient*innen unter Berücksichtigung der Kostenneutralität. Hierzu wird eine fahrbare (mobile) Post-COVID-Ambulanz (Medi-Bus-Konzept der Deutschen Bahn[1]) und eine multimodale Symptom-übergreifende telemedizinische Versorgungslösung („Brain, Body, Soul“) angeboten. In Kooperation mit der Arbeitsgruppe P4 (Prof. Brokmann) des Robert-Koch-Institutes wird über die Datenspende-App® über WATCH-spezifische Fragebögen der Krankheitsverlauf dokumentiert. Während der Studienteilnahme werden über sogenannte „Wearables“ (Fitnessarmbänder) regelmäßig Daten zu Vitalparametern und zur Schlafqualität erhoben und an die Corona Datenspende-App® des RKI übertragen.

Über die Versorgungsform WATCH soll eine verbesserte körperliche Gesundheit und damit eine höhere Teilhabe am Sozial- und Arbeitsleben von Post-COVID-Patient*innen erreicht werden. Mit der Überführung des Modell-Projektes in die Regelversorgung wird eine verbesserte, kosteneffektive Versorgung von Patient*innen mit Langzeit-Sequalae nach Infektionskrankheiten im ländlichen Raum in zukünftigen Post-Pandemie-Situationen angestrebt.

2. Organisation und Verantwortlichkeiten

Die Verantwortung für die Sicherheit der Daten und für eine ordnungsgemäße Datenverarbeitung liegt beim Vorstand des Universitätsklinikums Jena und dem Konsortialführer.

Spezifische Anliegen erfordern ferner die Hinzunahme des Datenschutzbeauftragten des Universitätsklinikums Jena. Dieser muss bei folgenden Anliegen zusätzlich konsultiert werden:

- Beschwerden den Datenschutz betreffend
- Datenschutzprobleme
- Auskunftsgesuch der betroffenen Person (gemäß Art. 15 DSGVO)
- Anfragen von Datenschutz-Aufsichtsbehörden (gemäß Art. 58 DSGVO)

WATCH ist als neue Versorgungsform in einem Sektor-übergreifenden Ansatz konzipiert. Dementsprechend sind mehrere Partner an der Durchführung beteiligt. Die Konsortialführung liegt am Universitätsklinikum Jena (Prof. Dr. A. Stallmach). Zum Zweck des Projektes werden mit den externen Beteiligten Konsortialverträge geschlossen, die die Rechte und Pflichten der jeweiligen Partner klar definieren.

Externe Projektpartner sind:

- FSU Jena, Institut für Sportmedizin (PD Dr. C. Puta)
- Universität Halle/Saale, Institut für Medizinische Epidemiologie, Biometrie und Informatik (Prof. R. Mikolajczyk)

[1] https://www.deutschebahn.com/resource/blob/6864910/3db9cab4affba1e40c06ff77c370b7ce/Download-Faktenblatt-DB-Medibus-data.pdf

- Robert-Koch-Institut (Prof. D. Brockmann)
- Deutsche Stiftung für chronisch Kranke (Dr. D. Zippel-Schulz)
- Krankenkassen (AOK plus, BARMER, Techniker Krankenkasse)
- Kassenärztliche Vereinigung Thüringen (Dr. Rommel)

Die Projektpartner tragen für die Integrität der Daten gemeinsam die Verantwortung, die Hauptverantwortung liegt bei der Konsortialführung.

3. Datenschutzrechtliche Anforderungen

a.) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (i.S. Art. 5 Abs 1 lit a DSGVO)

Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

b.) Zweckbindung (i.S. Art. 5 Abs 1 lit b und Art. 9 DSGVO)

Daten dürfen ausschließlich für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (gemäß Artikel 89 Abs. 1 DSGVO) gilt nicht als unvereinbar mit den ursprünglichen Zwecken.

Es ist ausdrücklich zu beachten, dass bei der Verarbeitung von Gesundheitsdaten zusätzlich Art. 9 DSGVO gilt (siehe Kapitel 5.3).

c.) Datenminimierung (i.S. Art. 5 Abs 1 lit c DSGVO)

Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zweck der Verarbeitung notwendige Maß beschränkt sein.

d.) Richtigkeit (i.S. Art. 5 Abs 1 lit d DSGVO)

Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

e.) Speicherbegrenzung (i.S. Art. 5 Abs 1 lit e DSGVO)

Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, verarbeitet werden.

f.) Integrität und Vertraulichkeit (i.S. Art. 5 Abs 1 lit f DSGVO)

Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter

Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

g.) Rechenschaftspflicht (i.S. Art. 5 Abs. 2 DSGVO)

Für die Einhaltung der Grundsätze zur Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DSGVO ist der Verantwortliche zuständig. Die Erfüllung muss der Verantwortliche nachweisen können.

h.) Rechtmäßigkeit der Verarbeitung

Die Datenverarbeitung im Sinne der DSGVO unterliegt besonderen Bedingungen. Ohne die Erfüllung einer dieser Voraussetzungen, gilt die Verarbeitung als nicht rechtmäßig. Eine der nachfolgenden Voraussetzungen muss mindestens vorliegen:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben [...] (gemäß Art. 6 Abs. 1 lit a DSGVO).
- die Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen [...] (gemäß Art. 6 Abs. 1 lit b DSGVO).
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt [...] (gemäß Art. 6 Abs. 1 lit c DSGVO) – bspw. die Meldung/Dokumentation über das Krebsregister.
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen [...] (gemäß Art. 6 Abs. 1 lit d DSGVO).
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde [...] (gemäß Art. 6 Abs. 1 lit e DSGVO).

Es ist ausdrücklich zu beachten, dass Im Kontext wissenschaftlicher Vorhaben / klinischen Prüfungen zusätzlich Art. 9 DSGVO gilt (siehe Kapitel 5.3).

4. Zweckbestimmung

Die beteiligten Konsortialpartner planen die gemeinsame Durchführung des Projektes WATCH mit dem Ziel die medizinische und gesundheitsökonomische Effektivität eines wohnortnahen Assessments und einer 12-wöchigen telemedizinischen Intervention bei Patienten mit post-COVID Syndrom und eingeschränkter Lebensqualität zu evaluieren. Zum Zweck der Bewertung der medizinischen Effektivität ist es notwendig, über den Projektzeitraum Patientendaten zu sammeln und zu dokumentieren. Für die gesundheitsökonomische Bewertung ist die Auswertung von Sekundärdaten der am Projekt beteiligten Krankenkassen notwendig.

5. Kreis der Betroffenen

Patient*innen mit post-COVID-Syndrom, die am Versorgungsprojekt WATCH teilnehmen

6. Verarbeitung besonderer Kategorien personenbezogener Daten (gemäß Art. 9 DSGVO)

Die Verarbeitung von Daten dieser Kategorie sind untersagt (Art. 9 Abs. 1 DSGVO). Im der klinischen Forschung machen nachfolgende Bedingungen eine Datenverarbeitung hingegen möglich:

- die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden (i.S. Art. 9 Abs. 2 lit a).
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben [...] (i.S. Art. 9 Abs. 2 lit c).
- die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 (gemäß Art. 9 DSGVO) genannten Bedingungen und Garantien erforderlich [...] (i.S. Art. 9 Abs. 2 lit h).
- die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich [...] [...] (i.S. Art. 9 Abs. 2 lit i).

Im Rahmen des Projekts WATCH werden nach Zustimmung durch die Teilnehmer im Detail folgende Daten erhoben:

Patientendaten: Alter, Geschlecht, Gewicht, Größe, Datum der Infektion, Datum der Vorstellung im post-COVID Bus, Vorerkrankungen, Begleitmedikation. Symptomatik und ggf. Behandlung der akuten Infektion, Zeiten von Arbeitsunfähigkeit seit der SARS-CoV-2 Infektion, bereits erfolgte post-COVID Diagnostik inkl. Der Befunde. Von jeder Vorstellung im Post-COVID Bus: Blutwerte, Blutdruck, Herzfrequenz, Sauerstoff-Sättigung, Körpertemperatur, 1-Minute-Sit-to-stand Test, Handkraftmessung, Resultate der Fragebögen und neuropsychologischen Tests, Elektroimpedanztomografie der Lunge, aktuell bestehende Symptomatik.

Während der Studienteilnahme werden über sogenannte „Wearables“ (Fitnessarmbänder) regelmäßig Daten zu Vitalparametern und zur Schlafqualität erhoben und an die Corona Datenspende-App® des RKI übertragen. In der Corona Datenspende-

App® werden regelmäßig nach einzelnen Übungen und nach definierten Zeitpunkten Fragebögen angeboten.

Von den Krankenkassen werden unter Verwendung von Pseudonymen zudem folgende Daten abgefragt: Von den Krankenkassen getragene medizinische und pflegerische Leistungen, die im Zeitraum eines Jahres vor Infektionsbeginn bis ein Jahr nach Maßnahmenende in Anspruch genommen wurden. Hierunter fallen verschreibungspflichtige Medikamente, verordnete Heilmittel und Krankenpflege, ärztliche Leistungen, Krankenhausaufenthalte, gemeldete Arbeitsunfähigkeitstage und sonstige erstattungsfähige Leistungen.

7. Umsetzung der Betroffenenrechte

Im Rahmen des wissenschaftlichen Vorhabens sind die Rechte der Betroffenen besonders zu wahren. Teilnehmende Patient*innen erhalten in Bezug auf Ihre Daten folgende Rechte:

1.) Recht auf Auskunft:

Betroffene Personen haben das Recht auf Auskunft über die sie betreffenden personenbezogenen Daten, die im Rahmen der klinischen Studie erhoben, verarbeitet oder ggf. an Dritte übermittelt werden (Aushändigen einer kostenfreien Kopie) (Artikel 15 DSGVO, §§34 und 57 BDSG-neu).

2.) Recht auf Berichtigung:

Betroffene Personen haben das Recht, sie betreffende unrichtige personenbezogene Daten berichtigen zu lassen (Artikel 16 und 19 DSGVO, § 58 BDSG-neu).

3.) Recht auf Löschung:

Betroffene Personen haben das Recht auf Löschung Sie betreffender personenbezogener Daten, Der Verantwortliche ist verpflichtet, die Löschung unter Berücksichtigung der Existenz einer der nachfolgenden Bedingungen, unverzüglich vorzunehmen:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung. (Anmerkung: Im Rahmen eines wissenschaftlichen Vorhabens / einer klinischen Prüfung dürfen die bis zum Widerruf bereits verarbeiteten Daten für Studienzwecke weiterverwendet werden (gemäß Art. 7 Abs. 3 DSGVO).
- Die betroffene Person erhebt Widerspruch gegen die Verarbeitung und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die personenbezogenen Daten der betroffenen Person wurden unrechtmäßig erhoben.

4.) Recht auf Einschränkung der Verarbeitung:

Unter Voraussetzung einer der nachfolgenden Bedingungen hat die betroffene Person das Recht, die Einschränkung der Verarbeitung seiner betreffenden personenbezogenen Daten zu verlangen:

a.) Die Richtigkeit der Verarbeitung personenbezogenen Daten wird von der betroffenen Person bestritten.
   - Der Verarbeitung personenbezogener Daten ist unrechtmäßig, die betroffene Person lehnt jedoch die Löschung seiner betroffenen Daten ab und fordert die Einschränkung der Nutzung seiner personenbezogenen Daten
   - Die personenbezogenen Daten werden für den ursprünglichen Verarbeitungszweck nicht länger benötigt, die betroffene benötigt diese jedoch hinsichtlich der Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen.
   - Die betroffene Person hat Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten eingelegt und es ist noch unklar, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen

b.) Wurden personenbezogene Daten in ihrer Verarbeitung eingeschränkt, dürfen diese einzig unter der Voraussetzung einer der nachfolgenden Bedingungen erneut verarbeitet werden:
   - Einwilligung der betroffenen Person
   - Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
   - Schutz der Rechte einer anderen natürlichen oder juristischen Person

5.) Recht auf Datenübertragbarkeit:

- Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und bei Bedarf mit einem anderen Verantwortlichen zu teilen.
- Unter Voraussetzung der technischen Möglichkeiten hat die betroffene Person das Recht eine Übermittlung der personenbezogenen Daten von einem Verantwortlichen zu einem anderen Verantwortlichen zu erwirken.

6.) Widerspruchsrecht:

Die betroffene Person jederzeit hat das Recht, die Verarbeitung seiner personenbezogenen Daten zu widersprechen. Der Verantwortliche muss die Verarbeitung unverzüglich einstellen, sofern nicht eine der nachfolgenden Bedingungen dem entgegensteht:

- Nachweis zwingend schutzwürdiger Gründe
- Interessen, Rechte und Freiheiten der betroffenen Person überwiegen
- Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Zur Umsetzung dieser Rechte erhalten die betroffenen Personen mit der Aufklärung Kontaktadressen (email, Post, Telefon, Fax) im Studienzentrum, bei denen sie sich melden können, um die vorgenannten Rechte in Anspruch zu nehmen. Des weiteren erhalten die Patienten die Kontaktdaten der zuständigen Datenschutzbeauftragten am Universitätsklinikum Jena, im Freistaat Thüringen sowie in der Bundesrepublik Deutschland ausgehändigt.

Nach Art. 89 DSGVO können von den o.g. Rechten gemäß der Artikel 15, 16, 18 und 21 Ausnahmen vorgesehen werden, wenn personenbezogene Daten zu wissenschaftlichen Zwecken verarbeitet werden und diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.

So sieht Art. 17 Abs. 3 c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit sowie Art. 17 Abs. 3 d) DSGVO für wissenschaftliche Forschung eine Ausnahme von dem Recht auf Löschung vor, wenn die Verwirklichung die Ziele der Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt.

8. Beschreibung der Datenverarbeitung unter Berücksichtigung der datenschutzrechtlichen Anforderungen zur Datenminimierung /Speicherbegrenzung

DATENSPENDE APP: Die Informationen werden an den Backend-Server der Corona-Datenspende des RKI geleitet. Der Backend-Server wird in der Open Telecom Cloud (OTC) gehostet. Die Server der OTC befinden sich in Deutschland und sind hinsichtlich Qualitätsmanagement und Sicherheit extern auditiert und zertifiziert (Antrag Robert Koch-Institut Corona Datenspende). Gemeinsam mit der Arbeitsgruppe P4 des Robert Koch-Instituts werden die Daten anonymisiert gruppenaggregiert analysiert und für 14-tägige Beiträge auf dem Corona Datenspende Blog vorbereitet. Zum Zweck der gemeinsamen Datenverarbeitung wird mit dem RKI ein Joint Controllership Agreement geschlossen, in dem Verantwortungen, Aufgaben und Details der Datenverarbeitung geregelt werden.

DATEN AUS PATIENTENVORSTELLUNG: Alle im Rahmen der Patientenvorstellung gewonnen Daten werden durch einen Mitarbeiter des Studienzentrums in die Studiendatenbank eingegeben. Dabei werden nur pseudonymisierte Daten gespeichert. Die Daten werden auf Servern des Instituts für medizinische Statistik, Informatik und Dokumentation des Universitätsklinikums Jena gespeichert und entsprechend der dort vorhandenen SOPs und Qualitätsmanagement Prozesse behandelt.

KRANKENKASSENDATEN: Daten der Krankenkasse werden an eine Treuhandstelle, die unabhängig von den anderen Partnern ist, übertragen, durch diese pseudonymisiert und mit den anderen Daten verknüpft. Die Datentreuhandstelle übernimmt dabei auch keine weiteren Aufgaben in dem Projekt.

Zur Auswertung und Evaluation erhalten die beteiligten Partner nur pseudonymisierte Datensätze, die keinen Rückschluss auf einzelne Personen erlauben.

9. Verzeichnis der Verarbeitungstätigkeiten

Die Verarbeitungstätigkeiten werden entsprechend Art. 30 DSGVO im Verzeichnis der Verarbeitungstätigkeiten dokumentiert. (Vorgangsnummer: DS718819)

10. Sicherheit der Verarbeitung nach Art. 32 DSGVO

Entsprechend den datenschutzrechtlichen Bestimmungen sind Maßnahmen zu treffen, die gewährleisten, dass

- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
- personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),

- personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können(Authentizität),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

a.) Maßnahmen zur Sicherung der Vertraulichkeit

Es muss gewährleistet werden, das unbefugte Personen keinen Zugang zu den entsprechenden Daten erhalten.

Pseudonymisierung

Unter dem Begriff Pseudonymisierung versteht man die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Voraussetzung ist jedoch, dass diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen. Pseudonyme müssen zusammen mit den identifizierenden Eigenschaften einer Person in einer separaten Teilnehmeridentifikationsliste geführt und in einem getrennten und abgesicherten Systemen aufbewahrt werden (bestenfalls verschlüsselt). Die Dokumentation von personenbezogenen Daten zu erfolgten Therapien (den sog. Quelldaten) findet in der Patientenakte unter dem realen Namen des Teilnehmers statt. Die im Ethikantrag aufgeführten bzw. vom Prüfplan geforderten Informationen müssen pseudonymisiert in ein studienspezifisches CRF überführt werden. Dieses kann sowohl papierbasiert als auch elektronisch sein. Bei einer elektronischen Verarbeitung muss darauf geachtet werden, das einzig pseudonymisierte Daten exportiert werden. Bildhafte Befunde (Lungenimpendanztomografie) sowie entnommene Biomaterialien müssen ebenfalls pseudonymisiert abgespeichert werden und dürfen einzig in dieser Form Verwendung finden.

Zutrittskontrolle

Die Zutrittskontrolle soll gewährleisten, das Unbefugten der Zutritt zu Datenverarbeitungsanlagen bzw. Räumen, in denen personenbezogene Daten verarbeitet werden, verwehrt wird.

Der Zutritt zu den Räumlichkeiten (Büros zur Aufbewahrung von Unterlagen in Papier sowie Laborräume zur Lagerung von Biomaterialien) ist nur autorisierten Personen möglich. Dies wird durch eine kontrollierte Transponder (Thoska-Karte)- bzw. Schlüsselvergabe sichergestellt. Sowohl Thoska als auch Schlüssel dürfen NICHT an nicht-autorisierte Personen weitergegeben werden. Zimmertüren sind von der letzten Person, die einen Raum verlässt, abzuschließen. Beim Ausscheiden eines Mitarbeiters hat dieser sowohl die Thoska als auch empfangene Schlüssel unverzüglich zurückzugeben. Die Vergabe von Thoska-Rechten und Schlüssel ist zu dokumentieren.

Zugangskontrolle und Zugriffskontrolle

Die Zugangskontrolle soll sicherstellen, dass einzig die dazu berechtigten Personen Zugang zu den Datenverarbeitungssystemen erhalten. Mit Hilfe der Zugriffskontrolle muss gewährleistet werden, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen einzig auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Auf Papier dokumentierte personenbezogene Daten (bspw. Einwilligungserklärungen, Patienten- und Probandenakten) müssen in verschließbaren Schränken aufbewahrt werden. Die Schränke sind stets verschlossen zu halten.
Daten, welche systembasiert verarbeitet werden auf einem Datenbankserver gespeichert. Der Datenbankserver befindet sich im Universitätsklinikum Jena. Der Systemzugriff erfolgt über einen persönlichen Benutzeraccount. Kooperationspartner erhalten ggf. nach schriftlicher Genehmigung durch den Studienleiter Systemzugriff. Die Zugriffslaufzeit ist dabei auf die Projektdauer beschränkt. Geeignete Garantien und Vereinbarungen zur ordnungsgemäßen Nutzung von personenbezogenen Daten sind vertraglich festzuhalten und schriftlich zu bestätigen.
Die Dateneingabe muss im gesicherten Netz des Universitätsklinikums Jena erfolgen und ist durch ein Berechtigungskonzept geregelt. Für die Dateneingabe ist der persönliche Benutzeraccount zu verwenden. Eine Dateneingabe unter Verwendung eines fremden Benutzeraccounts ist nicht zulässig und strengstens untersagt. Über den Benutzeraccount sind die entsprechen Berechtigungen innerhalb des Studienprojektes geregelt. Nach einer längeren Inaktivität wird der Benutzer automatisch ausgeloggt. Ein standardisiertes Passwortverfahren soll die Zusammensetzung einzelner Komponenten regeln.
Elektronische Daten dürfen einzig innerhalb der in der Verantwortung des GB IT stehenden Serverinfrastruktur gespeichert werden. Dabei muss der verfügbare Ordner der Studie verwendet werden. Der Zugang ist nur autorisierten Mitarbeitern der Studie möglich. Die Berechtigung wird im Auftrag und nach Bestätigung des Studienleiters durch den GB IT freigegeben. Die Freigabe von Berechtigungen wird dokumentiert. Der Zugang auf die Server-Infrastruktur erfolgt passwortgeschützt unter Verwendung des persönlichen Novel-Logins. Nach Beendigung der Arbeit muss ein Logout durch den Benutzer erfolgen, um einen Zugriff Unbefugter zu vermeiden. Elektronisch geführte Teilnehmer-identifikationslisten sind durch ein Passwort zu sichern. Autorisierte Mitarbeiter des Studienteams erhalten im Rahmen einer persönlichen Einweisung das Passwort der Teilnehmeridentifikationsliste mitgeteilt. Die Mitteilung des Passwortes muss dokumentiert werden. Es muss regelmäßig auf den ordnungsgemäßen Umgang mit der Datei sowie mit deren Passwort hingewiesen.
Ein Speichern von personenbezogenen Daten auf privaten Endgeräten und/oder über Cloud Computing ist nicht zulässig.

<u>Trennungskontrolle</u>
Unter die Trennungskontrolle fallen alle Maßnahmen, die gewährleisten, das Daten getrennt voneinander verarbeitet werden können. Erreicht wird das in der Regel durch eine logische und physikalische Trennung der Daten.
Die identifizierenden Daten der Teilnehmer (Name, Geburtsdatum und Kontaktdaten), anhand dessen ein eindeutiger Bezug zur betroffenen Person hergestellt werden könnte, müssen getrennt von den Studiendaten in einer Teilnehmeridentifikationsliste aufbewahrt werden. Rückschlüsse auf einzelne Teilnehmer einzig mit Hilfe der Teilnehmer-

identifikationsliste möglich. Sie darf einzig autorisierten Mitarbeitern des Studienteams zugänglich sein. Dieser Umstand gilt sowohl während als auch nach Abschluss des wissenschaftlichen Vorhabens/klinischen Prüfung. Im Fall schwerwiegender Begleitumstände während des Vorhabens, muss eine Re-Pseudonymisierung möglich sein.
I
m Falle einer systembasierten Datenverarbeitung muss sichergestellt werden, dass die Anwendung zwei Umgebungen unterscheidet. Eine Entwicklungsumgebung, zur Erstellung, Modifikation und Löschung von Formularen/eCRFs. Daneben muss eine Produktionsumgebung bestehen, in welcher letztlich die realen Daten verarbeitet werden. In der Produktionsumgebung ist eine Modifikation und Löschung der Formulare/eCRFs nicht möglich. Ferner muss ein Berechtigungskonzept die jeweiligen Nutzerrechte bzgl. der Datenverarbeitung im System bzw. Studienprojekt entsprechend regeln.

b.) Maßnahmen zur Sicherung der Integrität

Es muss gewährleistet werden, dass die Daten während der Verarbeitung nicht von Unbefugten modifiziert werden können.

Weitergabekontrolle

Bei der Weitergabekontrolle handelt es sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Daten dürfen sowohl intern einzig in anonymisierter bzw. pseudonymisierter Form weitergegeben werden. Klarnamen und identifizierende Merkmale sind zu vermeiden. Es muss darauf geachtet werden, dass eine Datenverarbeitung stets über eine verschlüsselte Verbindung (bspw. https) oder unter Einsatz eines VPN-Zugriffs erfolgt. Darüber hinaus sollte die Weitergabe relevante Inhalte per E-Mail unter Einsatz von Verschlüsselungs- und Signaturmechanismen erfolgen.
Auf Grund der Komplexität im Hinblick auf eine externe Weitergabe sei an dieser Stelle auf Kapitel 3 der DSGVO verwiesen. Im Zweifel ist der Datenschutzbeauftragte zu konsultieren.

Eingabekontrolle

Unter Eingabekontrollen sind Maßnahmen zu verstehen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrollen (sog. Audit Trail) können auf unterschiedlichen Ebenen (bspw. Betriebssystem, Datenbank, Anwendung) stattfinden.
Die verarbeiteten Daten müssen regelmäßig auf Plausibilität und Vollständigkeit überprüft und gegebenenfalls korrigiert und/oder ergänzt werden. Im Rahmen eines geplanten Monitorings müssen die Quelldaten aus der Patienten- bzw. Probandenakte mit den Eintragungen im CRF abgeglichen werden. Bei festgestellten Mängeln muss eine Korrektur erfolgen, welche ebenfalls zu dokumentieren ist. Dies gilt sowohl für die papierbasierte als auch die elektronische Form der Datenverarbeitung.
Im Rahmen einer systembasierten Datenverarbeitung können die entsprechenden Nutzerrechte hinsichtlich der Eingabe, der Änderung und der Löschung von Daten bzw. Dateneingaben geregelt werden.

c.) Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Hierbei handelt es sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Eine zyklische Datensicherung muss über ein Backup-Konzept geregelt sein. Die daraus resultierenden Sicherungen müssen getrennt und außerhalb des Serverraumes aufbewahrt werden. Daneben muss sichergestellt werden, dass die Sicherungsmedien eine korrekte Wiederherstellung der Daten erlauben. Es müssen regelmäßige Tests und Protokollierungen stattfinden, um den korrekt funktionierende Wiederherstellungs-vorgang zu bestätigen bzw. nachweisen zu können. Dieser Prozess muss in einem Recoverykonzept geregelt sein.

Personenbezogene Daten müssen so lange aufbewahrt werden, wie dies im Rahmen der Studie gesetzlich vorgeschrieben ist und/oder nach den Empfehlungen zur Sicherung guter wissenschaftlicher Praxis notwendig erscheint. Nicht mehr benötigte Daten müssen durch sicheres Überschreiben / endgültiges Löschen der Datensätze und Entfernen etwaiger Sicherheitskopien gelöscht werden. Vorhandene und nicht mehr benötigte Proben komplett vernichtet werden.

Ist eine Löschung nicht vorgesehen und/oder nicht möglich, müssen die vorhandenen Studiendaten anonymisiert werden. Bei einer Anonymisierung werden die personenbezogenen Daten derart verändert, dass ein Rückschluss auf die Betroffenen wesentlich erschwert wird bzw. Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Vorgänge zur Löschung, Vernichtung oder Anonymisierung müssen dokumentiert werden.

Maßnahmen zur Sicherung der Authentizität

Studiendaten müssen sich ihrem Ursprung anhand von Quelldaten in der Patienten- bzw. Probandenakte zuordnen lassen.

Maßnahmen zur Sicherung der Revisionsfähigkeit und Transparenz

Eintragungen, Änderungen und Streichungen müssen im Rahmen der papierbasierten Verarbeitung mit einem persönlichen Namenskürzel sowie dem aktuellen Datum versehen werden. Bei einer elektronischen Verarbeitung muss dies der Audit Trail gewährleisten.

11. Feststellung des Schutzbedarfs

Im Rahmen der Dokumentation im Verzeichnis der Verarbeitungstätigkeiten wird eine Schwellwertanalyse durchgeführt und eine Datenschutz-Folgenabschätzung entsprechend Art 35 DSGVO durchgeführt werden.

Für die Corona-Datenspende-App wurde durch das RKI bereits eine Datenschutzfolge-Abschätzung durchgeführt, diese ist in der Anlage beigefügt.

12. Durchführung der Datenschutzfolgeabschätzung nach Art. 35 DSGVO

Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde (Thüringer Landesdatenschutzbeauftragter), wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung der personenbezogenen Daten ein hohes

Risiko zur Folge für den Betroffenen hat, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft (Art. 36 DSGVO)

Für die Corona-Datenspende App ist eine Datenschutz-Folgeabschätzung durch das RKI bereits erfolgt.

13. Meldung von Datenschutzverletzungen nach Art. 33 und 34 DSGVO

Die Meldung von Datenschutzverletzungen erfolgt gemäß des QM-Standards des UKJ und wird an alle Beteiligten und Betroffenen unmittelbar nach Bekanntwerden kommuniziert.

14. Datenübermittlung Drittland nach Art. 45 ff. DSGVO

Es erfolgt keine Datenübermittlung in ein Drittland

15. Weitere Garantien für den Betroffenen

Das Projekt wird vor Beginn der zuständigen Ethikkommission der Friedrich-Schiller-Universität Jena vorlegt. Das Datenschutzkonzept wird mit der zuständigen Datenschutzbeauftragten Frau Tödter und dem Beauftragten für die IT-Sicherheit Herrn Sparbrod abgestimmt.