Platzhalter für
Logo und Titel

Datenschutz- und IT-Sicherheitskonzept für die <Titel der Studie/ des Registers> [im Rahmen des <Titel des Projekts>]

<ggf. Erläuterung im Titel verwendeter Abkürzungen>

Version <Versionsangabe> vom 04.08.2017

Herausgeber:

<Anschrift des verantwortlichen Instituts>

<Benennung des Projekt / Studien –Verantwortlichen>

Tel.: <Telefonnummer>

Fax: <Faxnummer>

E-Mail: <E-Mail>

Inhalt

1 Präambel

Die *Mustervorlage zum Verfassen eines Datenschutz- und IT-Sicherheitskonzeptes* wurde, entsprechend der Empfehlung der *87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg* für medizinische Forschungseinrichtungen und Forschungsverbünde in Konformität zum „*Leitfaden zum Datenschutz in medizinischen Forschungsprojekten der TMF (Version 2)*“ [1] verfasst.

Fokus dieser Vorlage sind epidemiologische Kohorten und Register. Die konkrete Ausprägung der Fragestellungen orientiert sich an den Hinweisen des TMF-Leitfadens für die patientenferne Forschung.

Sie finden diese Vorlage hilfreich? *Sie setzen von uns bereitgestellte Werkzeuge ein? Bitte unterstützen Sie uns und referenzieren Sie das MOSAIC-Projekt in Ihren Konzeptdokumenten und Publikationen. Zitieren Sie eine unserer Publikationen oder referenzieren Sie unser Projekt wie folgt:*

Bialke M, Bahls T, Havemann C, Piegsa J, Weitmann K, Wegner T , et al.*
MOSAIC. A modular approach to data management in epidemiological studies.
METHODS OF INFORMATION IN MEDICINE. 2015; 54(4):364-371.
http://dx.doi.org/10.3414/ME14-01-0133

2 Einleitung

Hinweis: *Ziel des einleitenden Abschnitts ist es, die Studie / das Register gleichzeitig knapp und vollständig vorzustellen.*

2.1 <Name der Studie / des Registers>

- Wird die Studie im Rahmen eines anderen Projekts durchgeführt?
- Wie ist die Studie / das Register motiviert? (Zweckbestimmung der Datenerhebung, -verarbeitung und –nutzung verdeutlichen [1])?
- Was ist das Ziel der Studie / des Registers (ausführliche Erläuterung)?
- Welchen zu erwartenden Nutzen gibt es? (Die Erforderlichkeit der Datenerhebung ausführlich darstellen.)
- Wie grenzt sich die Studie / das Register zu ähnlichen Studien / Registern ab?
- Wie ist die Studie/ das Register in Bezug auf den Behandlungs- bzw. Forschungskontext abgegrenzt?
- Wie lang ist die beantragte Laufzeit?
- Wie wird die Studie / das Register finanziert?
- Handelt es sich um ein Förderprojekt? Wenn ja, Wie soll das Projekt nach Ablauf der Förderung weitergeführt werden? [2]

Hinweis: *Die Abschnitte 2.2 und 2.3 beziehen sich vorwiegend auf die Durchführung von Studien. Bei Verwendung der Vorlage für Register ist kann der Umfang der Fragen in diesen Abschnitten auf register-relevante Aspekte reduziert werden.*

2.2 [Studienziel und Fragestellungen]

- Wie lässt sich das Studienziel in 2-3 Sätzen zusammenfassen? (knappe Erläuterung)
- Welche zentralen Studienziele ergeben sich daraus?
- Sind weitere Erläuterungen zum Verständnis der Studienziele notwendig?
- Welche wesentlichen Fragestellungen resultieren aus den Studienzielen?
- Sind weitere Erläuterungen zum Verständnis der Fragestellungen notwendig?
- Lassen sich die einzelnen Fragestellungen in weitere (Teil-) Fragen unterteilen?

2.3 [Studiendesign]

- Wie sieht das Design der Studie aus?

- Welche Besonderheiten ergeben sich aus dem Studiensetting in Bezug auf die Leitlinien der „Guten Epidemiologischen Praxis“? [3]
- Werden Proben entnommen und gesammelt?
- Wenn ja, was passiert mit diesen Proben nach Ablauf der Studie?
- Soll eine Biobank aufgebaut oder genutzt werden?
- Welche ethischen Aspekte gilt es darüber hinaus zu beachten?

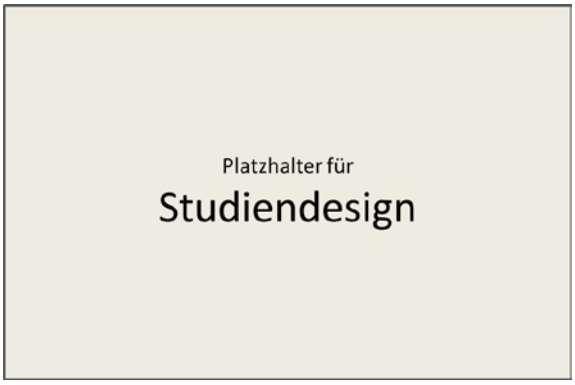

Abbildung 1: Studiendesign/Studienablauf

2.4 <Name der verantwortlichen Stelle/Einrichtung>

- Welche Forschungsschwerpunkte hat das verantwortliche Stelle / Einrichtung?
- Welche Ziele werden dabei verfolgt?
- Welche thematisch relevanten Erfahrungen konnten gesammelt werden?
- Wurden am Institut bereits ähnliche Studien / Register durchgeführt?

2.5 [Beteiligte Institutionen und Kooperationspartner]

- Wie sind die Verantwortlichkeiten innerhalb der Studie / des Registers geregelt? (Stichworte: informationelle Gewaltenteilung [1], Weisungsfreiheit und Unabhängigkeit)
- Welche Kooperationspartner gibt es?
- Welche weiteren Institutionen und Partner sind an der Studie / dem Register beteiligt?
- Welche Dienstleister sind an der Studie / dem Register beteiligt?
- Welche Gründe gibt es für deren Beteiligung und welche Funktionen übernehmen sie im Rahmen der Studie / des Registers?
- Wie kann man das Zusammenspiel der einzelnen Partner tabellarisch oder grafisch veranschaulichen?

Abbildung 2: Organigramm

- Welche Rechtsform haben die Kooperationspartner? Wer verkörpert die zuständige juristische Person (rechtliche Verantwortlichkeit)? [2]
- Welche Datenschutzbeauftragten sind für die Vorabprüfung des Datenschutzkonzepts zuständig? Nach Möglichkeit sollten diese frühzeitig eingebunden werden.

3 Rechtsgrundlagen

***Hinweis**: In diesem Abschnitt sollen die angewendeten gesetzlichen Grundlagen zur Datenerhebung, Einwilligung und Pseudonymisierung/Anonymisierung von Daten im Rahmen einer Studie oder eines Registers dargestellt werden. Einstiegspunkt sollten die zusammenfassend im Datenschutzleitfaden der TMF [1] beschriebenen gesetzlichen Aspekte des Datenschutzes sein.*

Grundsätzlich geltende, gesetzliche Rahmenbedingungen sind bereits am Beispiel des Landesdatenschutzgesetzes Mecklenburg-Vorpommern aufgeführt. ***Die entsprechenden Paragraphen der im Einzelfall geltenden Landesdatenschutzgesetze sind zu ergänzen.*** *Ein umfassendes Rechtsgutachten zur Sekundärnutzung medizinischer Behandlungsdaten wird von der TMF [4] bereitgestellt.*

Geheimnisschutz nach § 203 StGB

Im direkten Behandlungszusammenhang unterliegen medizinische Daten dem Schutz durch die ärztliche Schweigepflicht. Gemäß § 203 StGB betrifft diese das Behandlungsteam (Ärzte, Apotheker, Pflegekräfte, medizinische Fachangestellte). Sobald die medizinischen Daten den Behandlungskontext verlassen, verlieren die medizinischen Daten diesen Schutz durch die Schweigepflicht.

Bundesdatenschutzgesetz

Ob eine Einrichtung aus datenschutzrechtlicher Sicht dem Bundesdatenschutzgesetz (BDSG) oder dem entsprechenden Landesgesetz unterliegt, wird anhand der jeweiligen Rechtsform entschieden. ([4], S. 145)

Bei nicht-öffentlichen Stellen, Stellen des Bundes und Privatunternehmen unterliegt die Erhebung und Verarbeitung personenbezogener Daten dem BDSG. [4]:

- Es gelten die Grundsätze der Datenvermeidung und Datensparsamkeit (§3a BDSG).
- Eine Zulässigkeit ist durch entsprechende Rechtsvorschrift oder Einwilligung des Betroffenen gegeben. (§4 BDSG)
- Angemessene technische und organisatorische Maßnahmen setzen Datenschutz durch.

Landesdatenschutzgesetz

- Wie ist die Verarbeitung personenbezogener Daten gesetzlich geregelt? (vgl. LDSG-MV §7-23)
- Ist eine Anonymisierung der Daten gesetzlich erforderlich oder eine hilfsweise Pseudonymisierung möglich? (vgl. LDSG-MV §5)
- Ist die Einwilligung des Probanden gesetzlich erforderlich und auf welche Weise ist diese per Gesetz einzuholen? (vgl. LDSG-MV §8)
- In welchem Rahmen ist die Nutzung der Daten gesetzlich geregelt? (LDSG-MV §8)
- Wie ist per Gesetz mit unkorrekten Daten zu verfahren? (LDSG-MV §10)
- Wer trägt die laut Gesetz Verantwortung für die Übermittlung der Daten? (LDSG-MV §14-16)
- Welche Rechte zum Widerruf eines Betroffenen sind umzusetzen? (LDSG-MV 24-25)
- Wie hoch ist per Gesetz die zulässige Dauer der Datenspeicherung bzw. Archivierung von Proben?
- Ist eine die Übermittlung der Daten an Dritte mit Einwilligung des Betroffenen per Gesetz zulässig?
- Welche haftungsrechtlichen Aspekte ergeben sich aus der Erhebung gegenüber dem Betroffenen?

Landeskrankenhausgesetz

- Welche zusätzlichen Forderungen an den Patientendatenschutz regelt das anzuwendende Landeskrankenhausgesetz? (vgl. [4])

4 Organisation und Aufgabenteilung

Hinweis: *Der Abschnitt „Organisation und Aufgabenteilung“ umfasst Erläuterungen zur Arbeitsteilung der an der Studie / dem Register beteiligten Partner. Es sollen Verantwortlichkeiten und Arbeitsfunktionen deutlich gemacht werden. Zudem ist es erforderlich zu erhebenden Daten klar zu spezifizieren.*

4.1 Aufgabenteilung bei der Datenverarbeitung

- Wie sind die Verantwortungsbereiche definiert? [2] (Welche Partner und Stellen sind auf welche Weise beteiligt?)
- Handelt es sich um eine Auftragsdatenverarbeitung oder eine Funktionsübertragung? [1]
- Wer ist die für die Daten bzw. Proben „verantwortliche Stelle“ (Daten verarbeitende Stelle, Verantwortung für die erhobenen Daten)
- Wem gehören die entnommenen Proben (Klärung der Eigentumsfrage [2])?
- Wie wird die Eigentumsübertragung bei Proben (z.B. durch Einwilligungen) geregelt?
- Inwiefern ist eine informationelle Gewaltenteilung erforderlich? Welche Konsequenzen ergeben sich daraus? (Technische Trennung, unterschiedliche Fachbereiche, Einrichtung einer rechtlich unabhängigen Treuhandstelle) [1] [2]
- Wie sieht der geplante Datenfluss in seiner Gesamtheit aus?

4.2 Spezifikation der Daten

- Wie werden die unter Kapitel 3 erwähnten Punkte zum Datenschutz konkret realisiert?
- Welche Personen/Personengruppen sind von der Datenerhebung betroffen (Patienten und Probanden, Angehörige, Mitarbeiter beteiligter Institutionen, Mitarbeiter nicht beteiligter Institutionen wie z.B. behandelnde Ärzte, …)?
- Wie sind Ein- und Ausschlusskriterien für Patienten und Probanden definiert?
- Welche personenbezogene Daten werden erhoben?
- Welche medizinische Daten werden erhoben?
- Welche Datenkategorien, -formate und -typen resultieren aus der Erhebung?
- Gibt es heterogene, homogene und/oder unstrukturierte Datentypen?
- Werden Biomaterialien entnommen und gelagert?
- Welche Rechtsgrundlage findet bei der Datenerhebung (gesetzliche Grundlage, freiwillige informierte Einwilligung, Datenverarbeitung im Auftrag, …) jeweils Anwendung?
- An welchem Ort werden die Daten / Proben wie lange gespeichert / gelagert?
- Gibt es Regelfristen zur Löschung der Daten / Vernichtung der Proben?

- Wie wird mit den Daten und ggf. Bioproben nach Ende der Förderungsdauer verfahren? Wer zeichnet dafür verantwortlich? [2]

5 Beschreibung der datenbezogenen Prozesse

***Hinweis**: Der nachfolgende Abschnitt erläutert die datenbetreffenden Prozesse. Ziel ist es, das geplante Vorgehen aus organisatorischer Sicht detailliert darzustellen, so dass Missverständnisse und Implikationen vorab vermieden werden können. Die nachfolgende Tabelle soll eine Übersicht sämtlicher Arbeitsabläufe bieten. Eine ausführliche Erläuterung der einzelnen Workflows sollte für mehr Anschaulichkeit um eine geeignete Grafik ergänzt werden. (siehe Abb. 3)*

Arbeitsablauf	Erläuterung
Einholung Einwilligung	…
Erhebung von Daten bzw. Proben	…
Rekrutierung von Teilnehmern	…
Übermittlung von Daten bzw. Proben	…
Speicherung bzw. Lagerung von Daten bzw. Proben	…
Bereitstellung von Daten bzw. Proben	…
Durchführung von Follow-Ups	…
Widerruf von Einwilligungen	…

Tabelle 1 Beispielhafte Übersicht von Arbeitsabläufen

5.1 Einwilligungen und Widerrufe

***Hinweis:** An dieser Stelle werden die Verfahren zum Umgang mit Einwilligungen und Widerrufen und daraus resultierende Prozesse dargestellt. Die Festlegung der Inhalte der Einwilligungen und deren Abstimmung mit der zuständigen Ethikkommission ist nicht Teil dieses Abschnitts. (Unterstützung gibt es dennoch unter: http://www.tmf-ev.de/Produkte/PEWWizard.aspx)*

- Ist es notwendig, für die Erhebung der Daten eine Einwilligung einzuholen?
- Wie wird mit Nichteinwilligungsfähigkeit, beispielsweise bei Kindern, verfahren?
- Inwiefern ist eine separate Entbindung von der Schweigepflicht erforderlich?
- Wer zeichnet für die Inhalte der Einwilligungen verantwortlich?

- Wie breit ist die Einwilligung formuliert: handelt es sich um eine allgemeine Einwilligung oder wird eine detailliierte, zweckbezogene Einwilligung benötigt? [2]
- Wird in der Einwilligungserklärung auf die Pseudonymisierung der erhobenen Daten hingewiesen?
- Wer klärt den Betroffenen vor Ort über seine Rechte auf und steht für Fragen bereit?
- Wann liegt eine gültige Einwilligung des Betroffenen vor?
- Wird die Einwilligung in Papierform oder in elektronischer Form eingeholt?
- Wird die notwendige Einwilligung in elektronischer Form unterzeichnet und ist dies überhaupt zulässig?
- Wer ist für die Aufbewahrung der Einwilligungen zuständig?
- Wo werden die Einwilligungen aufbewahrt?
- Wie lange werden die Einwilligungen aufbewahrt?
- Wie lange ist eine Einwilligung gültig?
- Wer ist für die Verwaltung der Einwilligungen zuständig?
- Wie läuft der Widerruf einer Einwilligung ab?
- Welche Möglichkeiten für einen Widerruf gibt es (Mail, Tel, Fax, Persönlich, Komplettwiderruf, Teilwiderruf)
- Wer erhält den Widerruf?
- Wo wird der Widerruf gelagert?
- Auf welche Weise wird ein Widerruf durchgesetzt?
- Wie sind im Fall eines Widerrufs die Zuständigkeiten definiert?
- Auf welche Weise erfolgt die Rückmeldung nach einem Widerruf?
- Welche Auswirkungen hat ein Widerruf auf die Daten bzw. Proben der betroffenen Person (Löschung, Vernichtung, Sperrung, Anonymisierung, Nutzungseinschränkung)?
- Wer ist für die Anonymisierung bzw. Löschung der Daten bzw. Vernichtung der Proben zuständig?
- Welche Fristen sind dabei einzuhalten?
- Wie wird ein Widerruf protokolliert / dokumentiert?
- Welche Schritte sind nach einem erfolgreichen Widerruf notwendig? (z.B. Bestätigung an den Widerrufenden)
- Kann ein Widerruf widerrufen werden? Was geschieht ggf. in einem solchen Fall?

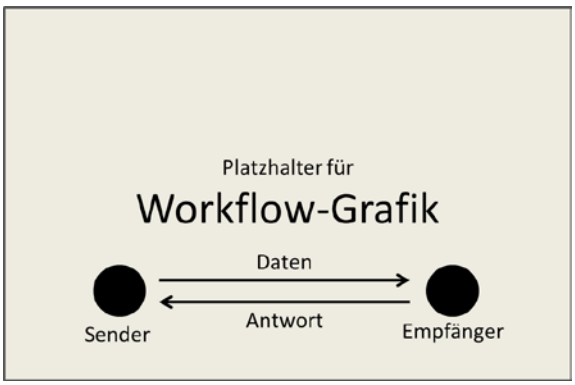

Abbildung 3: Grafische Darstellung des Workflows

5.2 Verarbeitung der Daten

5.2.1 Erhebung

- Welche technischen und organisatorischen Voraussetzungen sind für eine erfolgreiche Datenerhebung vorab erforderlich?
- Wie läuft die Datenerhebung ab?
- Wer führt die Datenerhebung durch?
- Welche Partner sind an der Datenerhebung beteiligt?
- Wie werden die Daten qualitätsgesichert (z.B. Prüfung auf Plausibilität und Vollständigkeit)?
- Wie groß ist das geschätzte Datenvolumen?
- Wie oft werden Daten einer einzelnen Person erhoben? (Follow-Ups?)
- Wird jedem Probanden/ Patienten eine eindeutige Kennung zugeordnet? Wenn ja, welche technischen Verfahre liegen dieser Zuordnung zugrunde?

5.2.2 Übermittlung im Rahmen der Datenerhebung

- Welche Übermittlungsprozesse sind vorgesehen?
- Ist eine Übermittlung der Daten zulässig?
- Wie werden die Daten übermittelt?
- Welche Daten werden übermittelt?
- Welche Form haben die übermittelten Daten? (Protokolle, Standards, …)
- Welche Partner / Institutionen sind an der Übermittlung beteiligt?
- Welche externen Systeme kommen zum Einsatz?
- Wie häufig werden Daten übermittelt?

5.2.3 Speicherung und Integration

- Welche Schritte sind vor der Speicherung der Daten durchzuführen?
- Wie erfolgt die Datenspeicherung?
- Welche Daten werden im Detail gespeichert?
- An welchem Ort werden die Daten gespeichert?
- Wie werden die Daten gespeichert (Zentral, Dezentral, Papier-basiert, Datei-basiert, Datenbank, Datawarehouse, …)?
- Werden die Daten vor der Speicherung (domänenspezifisch) anonymisiert/ pseudonymisiert?
- Wie erfolgt ggf. die Zusammenführung der multizentrischen Daten?
- Wie erfolgt ggf. die Zusammenführung heterogener Daten?

5.2.4 Pseudonymisierung

- Warum ist eine Pseudonymisierung erforderlich? [1]
- Welche Daten werden pseudonymisiert?
- Wie sieht das Pseudonymisierungsverfahren konkret aus? (Verwendetes Werkzeug, eingesetzte Algorithmen)
- Wer ist für die Pseudonymisierung der Daten verantwortlich?
- In welchen Fällen ist eine De-Pseudonymisierung der Daten erforderlich?
- Ist die Pseudonymisierung zeitlich befristet? [2] Wenn ja, warum ist eine Befristung notwendig?

5.2.5 Bereitstellung/Weitergabe der Daten (Use & Access)

- Welche Regelungen sollen für die Nutzung von Daten gelten? [1]
- Wie wird die Einhaltung dieser Regelungen kontrolliert?
- In welcher Form werden die Daten für eine spätere Nutzung bereitgestellt?
- Welche Schritte sind für die Bereitstellung der Daten notwendig?
- Gibt es vertragliche Vereinbarungen zwischen der bereitstellender Einrichtung und dem Datenempfänger, die die weitere Weitergabe der Daten, eine Dauerspeicherung und Versuche zur Re-Identifikation verhindern sollen? [2]
- Wer ist für die Bereitstellung der Daten zuständig?
- Wer entscheidet im Einzelfall über die Zulässigkeit der Datenherausgabe?
- Wie läuft der Prozess der Bereitstellung ab?
- Gibt es ein standardisiertes Antragsverfahren?

- Werden für die Datenherausgabe spezifische Pseudonyme erzeugt oder erfolgt die Bereitstellung der Daten in anonymisierter Form? [2]
- Ist eine Rückmeldung von Analyseergebnissen erforderlich?

5.2.6 Auswertung der Daten

- Wer ist für die Auswertung der Daten verantwortlich?
- Auf welche Weise werden die Daten ausgewertet?
- Werden die Daten zur Auswertung pseudonymisiert bzw. anonymisiert?

5.2.7 Anonymisierung / Löschung

- Wann ist eine Anonymisierung/Löschung der Daten erforderlich? (vgl. Abschnitt 5.1)
- Warum wird das gewählte Verfahren (Anonymisierung oder Löschung) bevorzugt genutzt?
- Wie wird das Verfahren konkret umgesetzt?
- Wer ist für die korrekte Durchführung des Verfahrens zuständig?
- Ist nach Durchführung des Verfahrens eine Erfolgsmeldung an den Teilnehmer erforderlich?

5.3 Qualitätssicherung

- In welcher Form werden qualitätssichernde Maßnahmen in den einzelnen Arbeitsmaßnahmen integriert?
- Welche gesonderter Anforderungen an den Datenschutz ergeben sich daraus in Bezug auf die Re-Identifikation von Probanden / Patienten, die Rückmeldung an Probanden / Patienten und die Datenerhebung?

6 Feststellung des Schutzbedarfs [und Risikoanalyse]

***Hinweis**: Ziel des nachfolgenden Abschnitts ist es, Prozesse, Anwendungen und Systeme hinsichtlich Struktur und Schutzbedarf zu betrachten. Es gilt Bedrohungen zu identifizieren und daraus resultierende Risiken aufzuzeigen. Jedes Projekt muss sich mit dem erforderlichen Schutzbedarf und der Bedrohungsanalyse auseinandersetzen. Es ist empfehlenswert auf Besonderheiten des Projekts hinzuweisen. Der Schutzbedarf von Studien-/Registerdaten ist grundsätzlich sehr hoch [1]. Eine Risikoanalyse ist obligatorisch.*

Kapitel 7 präsentiert im Anschluss technische und organisatorische Maßnahmen, um die ermittelten Risiken zu minimieren.

Hilfestellung zu den einzelnen Punkten bietet der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (siehe** [5]**).

6.1 [Strukturanalyse]

- Wie wird bei der Analyse vorgegangen (z.B. BSI IT-Grundschutzkataloge [6])?
- Welche Prozesse, Anwendungen und Informationen sind von besonderer Relevanz? (kurzer, beschreibender Systemüberblick)
- Welche Kommunikationswege, IT- und DV-Systeme (grafische Darstellung), Anwendungen, Räume und Personen spielen dabei eine Rolle? (tabellarischer Überblick)
- Welche Daten mit besonderem Schutzbedarf werden im Detail gespeichert (tabellarische Übersicht)?
- Welche Abhängigkeiten ergeben sich daraus?
- Lässt sich die Komplexität der Abhängigkeiten durch Bildung von Gruppen auf geeignete Weise reduzieren?

6.2 Ermittlung des Schutzbedarfs

- Ergibt sich für die Daten, Systeme und Abläufe ein gesonderter Schutzbedarf nach Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz?[1]
- Welche Schadensszenarien sind für die jeweiligen Grundwerte (realistisch) vorstellbar? [5]
- Welche Folgen ergeben sich im Schadensfall (Schadenshöhe und Schadenswahrscheinlichkeit) (Sicherheit des Grundwerts kann nicht gewährleistet werden)?
- Welcher Schutzbedarf ergibt sich daraus für den jeweiligen Grundwert, gemessen an den Schutzkategorien (normal, hoch, sehr hoch)? (vgl. BSI IT-Grundschutzkatalog)

[1] Grundwerte nach §21 LDSG-MVs

Grundwert	Schutzbedarf	Begründung
Vertraulichkeit	Hoch	Schadensszenario und Folgen für die Studie/ das Register
Verfügbarkeit	Normal	…
Integrität	…	…
Authentizität	…	…
Revisionsfähigkeit	…	…
Transparenz	…	…

Tabelle 2 Schutzbedarfsfeststellung gemäß §21 LDSG-MV

6.3 [Bedrohungsanalyse]

Hinweis: *Der Begriff Bedrohung bezeichnet die potentielle Gefahr, die durch eine Schwachstelle ausgelöst wird. Gemäß [5] wird im Rahmen der Bedrohungsanalyse eine vollständige Aufzählung aller möglichen Bedrohungen erstellt, die die nachfolgenden Fragen beantworten.*

- Welche Objekte werden bedroht?
- Welchen Bedrohungen sind die Objekte ausgesetzt?

Bedrohtes Objekt	Darstellung der Bedrohung	Bedrohtes Schutzziel
Laptop mit gespeicherten Daten	Diebstahl	Vertraulichkeit, Verfügbarkeit
…	…	…

Tabelle 3 Beispielhaftes Ergebnis der Bedrohungsanalyse [5]

6.4 [Risikoanalyse]

Hinweis: *Der Begriff Risiko bezeichnet die Wahrscheinlichkeit, dass tatsächlich ein Schaden entsteht. Für Grundwerte mit hohem bzw. sehr hohem Schutzbedarf (vgl. Tabelle 2) ist eine gesonderte Risikoanalyse anhand konkreter Beispiele erforderlich. Eine formale Analyse muss Aufschluss über wesentliche Risiken und zu treffende Gegenmaßnahmen geben.*

Risiko	Gegenmaßnahme
Bekanntwerden der gespeicherten personenbezogenen Daten nach Diebstahl	Verschlüsselung des Systems
Bekanntwerden der Pseudonymisierungsfunktion	Spezieller Pseudonymisierungsalgorithmus und Mehrfachpseudonymisierung
…	…

Tabelle 4 Beispielhafte Gegenüberstellung von Risiken und Gegenmaßnahmen

7 Technische und organisatorische Maßnahmen

Hinweis: *Der nachfolgende Abschnitt erläutert technische und organisatorische Maßnahmen, die zur Gewährleistung des in Kapitel 0 ermittelten Schutzbedarfs realisiert werden.*

- Welche Gefahren gilt es bei der Erhebung, Übertragung, Verarbeitung, Speicherung und Bereitstellung der Daten zu beachten?
- Welche technischen, personellen, organisatorischen und räumlichen Maßnahmen werden unternommen, um den Gefahrenfall zu vermeiden?
- Welche technischen, personellen, organisatorischen und räumlichen Maßnahmen werden unternommen, um das verbliebene Gefahrenpotential zu verringern?
- Welche technischen, personellen, organisatorischen und räumlichen Maßnahmen werden im Gefahrenfall unternommen?
- Wie werden die Datenschutzanforderungen aus Kapitel 3 realisiert?
- Wie wird der Schutzbedarf aus Kapitel 6 umgesetzt?

7.1 Organisation und Personal

7.1.1 [Räumliche Maßnahmen]

- Welche räumlichen Maßnahmen sind aus Datenschutzsicht erforderlich?
- Wie werden die Räumlichkeiten geschützt?

- Wer hat Zugang zu den Räumlichkeiten?
- Wer vergibt Zugangsberechtigungen?

7.1.2 [Personelle Maßnahmen]

- Welche personellen Maßnahmen sind aus Datenschutzsicht erforderlich?
- Wie ordnen sich diese Maßnahmen in die betrieblichen Hierarchien ein?
- Sind gesonderte Schulungen für diese Maßnahmen notwendig?

7.1.3 [Rollen und Rechte – Konzept]

- Für welche Bereiche ist das Rechte-Rollenkonzept gültig?
- Welche Rollen gibt es? Welche Rechte haben sie jeweils? (ggf. tabellarische Übersicht ergänzen)
- Wer ist für die Zuweisung der Rollen und Rechte zuständig?
- Wie wird eine Authentifizierung umgesetzt?

7.1.4 Internes Kontrollsystem

- Wer kontrolliert die Einhaltung der Sicherheitsmaßnahmen?
- Was wird je nach Maßnahme konkret geprüft? (tabellarische Übersicht?)
- Werden Sicherheitsüberprüfungen anlassbezogen oder regelmäßig (wie oft konkret?) durchgeführt?
- Werden Überprüfungen stichprobenartig oder vollständig durchgeführt?
- Wo werden Verfahren und Prozesse dokumentiert?

7.2 Infrastruktur

7.2.1 [Datenübertragung]

- Wie wird die Übertragung der Daten gesichert?
- Welches Verschlüsselungsverfahren wird bei der Datenübertragung eingesetzt.
- Gibt es redundante Systeme zur Übertragung im Falle eines Systemausfalls?
- Welche Probleme können bei der Datenübermittlung auftreten?
- Welche personellen, organisatorischen und technischen Maßnahmen werden getroffen um diese Probleme zu vermeiden / beheben?

7.2.2 Datenspeicherung

- Wo werden die Daten gespeichert?
- Wer speichert diese Daten?

- Wie lange werden die Daten gespeichert?
- In welcher Form werden die Daten gespeichert? (Format, Datenbank, Data Warehouse, Verschlüsselung)
- Werden die Daten versioniert?
- Werden die Daten historisiert?

7.2.3 Datenschutz

- Wie erfolgt technisch die Trennung von personenidentifizierenden und medizinischen Daten?
- Wie wird das Identitätsmanagement von Patienten und Probanden technisch realisiert?
- Kommen Werkzeuge zur Pseudonymisierung der erhobenen Daten zum Einsatz? Wenn ja, welche genau und welche Vorteile ergeben sich daraus?
- Wird eine Software zur Verwaltung der Einwilligungen und Widerrufen eingesetzt? Wenn ja, welche genau und welche Vorteile ergeben sich daraus?

7.2.4 Datensicherheit

- Werden die Daten verschlüsselt? Wenn ja, wer hat die Zugangsdaten? Wer hat eine Kopie der Zugangsdaten? Wo werden die Zugangsdaten für den Ernstfall hinterlegt? Wer ist für die Verschlüsselung verantwortlich? Wie wird im Detail verschlüsselt? Wie beeinflusst die Verschlüsselung die automatische Datensicherung?
- Wie sind Zugriff und Zutritt geregelt?
- Wie werden die Daten vor unerlaubtem Zugriff geschützt?
- Wie werden die Daten vor versehentlicher / vorsätzlicher Änderung / Löschung geschützt?
- Wird eine Datensicherung durchgeführt? Wenn ja, wie oft? Was wird gesichert? Wie wird gesichert? Wo wird gesichert? Wer führt die Sicherung durch? Wo werden die Sicherungen hinterlegt? Wer hat Zugriff auf die Sicherungen? Wann werden die Sicherungen gelöscht?

7.3 IT-Systeme

7.3.1 Ausfallschutz

- Welche Systeme dürfen nicht ausfallen?
- Welche Auswirkungen kann ein Ausfall der Systeme auf den Studienbetrieb haben?
- Welche Ursachen kann ein Systemausfall haben?
- Welche Maßnahmen können dagegen getroffen werden?
- Welche Auswirkungen haben die jeweiligen Maßnahmen?
- Gibt es weitere Maßnahmen um die Verfügbarkeit der Studiensysteme zu gewährleisten?

Ursachen	Maßnahmen
Ursache 1	Maßnahme 1
	Maßnahme 2
Ursache 2	Maßnahme 1
	Maßnahme 2

Tabelle 5: Maßnahmen zum Ausfallschutz

7.4 Netze

7.4.1 [Netzwerkschutz]

- Wie ist der Schutz des Netzwerkes auf physischer, logischer und Anwendungsebene geregelt? (z.B. räumliche Trennung von Serverinfrastrukturen, Firewalls, Routing, IP-Filter, Authentifizierung)
- Wer hat Zugriff auf das Studiennetzwerk?
- Wie wird das Studien- oder Registernetzwerk gegen unberechtigte Zugriffe geschützt?
- Welche Voraussetzungen müssen zum Aufbau einer Netzwerkverbindung in das Studiennetzwerk erfüllt sein?

7.5 Anwendungen

7.5.1 [Audit Trail]

- Inwiefern werden Zugriffe sowohl auf die Forschungsdaten als auch auf die datenspeichernden Systeme protokolliert?
- Was wird jeweils konkret erfasst?
- Wer hat Zugriff auf diese Protokolle?
- Wer ist für die Konfiguration der Audit Trail-Mechanismen zuständig?
- Wird zu diesem Zweck eine spezifische Software eingesetzt? Wenn ja, welche genau und aus welchem Grund?
- Wie lange werden diese Protokolldateien gespeichert? Gemäß Empfehlung des **BSI IT-Grundschutzkatalogs** (M 2.110 Datenschutzaspekte bei der Protokollierung) sollen Protokolldateien nach Erfüllung des Zwecks (z.B. zum Nachvollziehen von Unregelmäßigkeiten), spätestens jedoch nach einem Jahr gelöscht werden.

8 Vergleich mit dem TMF-Datenschutzleitfaden

***Hinweis**: Ziel des nachfolgenden Abschnitts ist es, das bisher entstandene Datenschutzkonzept kritisch zu betrachten. Um eine Abstimmung der Inhalte mit der TMF AG Datenschutz zu vereinfachen, wird empfohlen bewusste Abweichungen zum Forschungsmodul des Datenschutzleitfadens der TMF [1] zu begründen. [8] Bei ungewollten Abweichungen ist das bisherige Datenschutzkonzept an passender Stelle zu ergänzen. Nachfolgend eine kleine Auswahl möglicher Punkte.*

- Welche organisatorischen Fragen bleiben ungeklärt? (Rechtsform, langfristige Verantwortlichkeit, Nachfolgeregelungen) [8]
- Gibt es offene technische Fragen?
- Wurde von technischen Empfehlungen des Leitfadens abgewichen? Wenn ja, aus welchem Grund?
- Ist ein Datentreuhänder erforderlich? Wie wird die dafür notwendige Unabhängigkeit im Detail realisiert?

9 Abkürzungsverzeichnis

BDSG – Bundesdatenschutzgesetz

BGB – Bürgerliches Gesetzbuch

BSI – Bundesamt für Sicherheit in der Informationstechnik

BVerfGE – Bundesverfassungsgericht

GG – Grundgesetz

LDSG – Landesdatenschutzgesetz

LDSG-MV – Landesdatenschutzgesetz Mecklenburg Vorpommern

LKHG – Landeskrankenhausgesetz

LKHG MV – Landeskrankenhausgesetz Mecklenburg Vorpommern

StGB – Strafgesetzbuch

10 Glossar

Anonymisierung - Veränderung personenbezogener Daten derart, dass die 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. (§3 BDSG)

Einwilligung– Vereinbarung zwischen Patient und datenerhebender Stelle betreffs Erhebung und Verarbeitung personenbezogener Daten.

Ermächtigung– Erlaubnisgewährung gegenüber Dritten, ein üblicherweise nicht zustehendes Recht im eigenen Namen auszuüben.

Pseudonymisierung - Ersetzung des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. (§3 BDSG)

Widerruf - Zu jeder Zeit mögliche Zurücknahme eines Einwilligung.

11 Literaturverzeichnis

[1] K. Pommerening, J. Drepper, K. Helbing und T. Ganslandt, „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten. Generische Lösungen der TMF 2.0," MWV, Berlin, 2014.

[2] J. Drepper, „tmf-ev.de," 23 05 2014. [Online]. Available: http://www.tmf-ev.de/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=24476&PortalId=0. [Zugriff am 20 06 2014].

[3] B. Kurth, H. Hense und W. Hoffmann, „gesundheitsforschung-bmbf.de," 2004. [Online]. Available: http://www.gesundheitsforschung-bmbf.de/_media/Empfehlungen_GEP.pdf. [Zugriff am 07 10 2013].

[4] U. K. Schneider, Sekundärnutzung klinischer Daten - Rechtliche Rahmenbedingungen (TMF-Schriftenreihe Band 12), Berlin: MWV, 2015.

[5] T. Hillegeist, Rechtliche Probleme der elektronischen Langzeitarchivierung wissenschaftlicher Primärdaten, Göttingen: Universitätsverlag Göttingen, 2012.

[6] S. Wirth, „datenschutz-hamburg.de," 2012. [Online]. Available: http://www.datenschutz-hamburg.de/uploads/media/Hinweise_zur_Risikoanalyse_und_Vorabkontrolle.pdf. [Zugriff am 20 9 2013].

[7] Bundesamt für Sicherheit in der Informationstechnik, „bsi.bund.de,“ 2013. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html. [Zugriff am 20 9 2013].

[8] K. Pommerening, „Wie soll eine Anleitung zur Erstellung eines Datenschutzkonzepts anhand des Datenschutzleitfadens der TMF aussehen?,“ in *Vortragsfolien zur TMF-Sitzungswoche vom 16. September 2014*, Berlin, 2014.

12 [Anlagen]

I.1 <Anlage 1>

III.2 <Anlage 2>