Datenschutz- und IT-Sicherheitskonzept für die unabhängige Treuhandstelle der Nationalen Kohorte

Autoren: C. Havemann, K. Fitzer, S. Ostrzinski, R. Wolff, M. Bialke, T. Bahls, W. Hoffmann

Institut für Community Medicine
Universitätsmedizin Greifswald K. d. ö. R.
Ellernholzstr. 1-2
17487 Greifswald

Kontakt: wolfgang.hoffmann@uni-greifswald.de

Version 1.0 vom 25. Februar 2014

Inhalt

Vorbemerkungen

Dieses Dokument ist eine Ergänzung und Konkretisierung des Datenschutzkonzeptes der Nationalen Kohorten bezüglich des Datenschutzes und der Informationssicherheit in der unabhängigen Treuhandstelle der Nationalen Kohorte. Dieses Dokument besteht aus zwei Teilen, einem projektunabhängigen und einem projektspezifischen. Im projektunabhängigen Teil werden diejenigen rechtlichen Rahmenbedingungen, Prozesse, Verfahren und Systeme beschrieben, die für die Tätigkeit einer Treuhandstelle in der Rolle des Datentreuhänders allgemein zutreffend sind. Im zweiten, projektspezifischen Teil werden diese, bezogen auf die spezifischen Anforderungen, Strukturen, Festlegungen und Anwendungsfälle in der Nationalen Kohorte, konkretisiert.

A. Projektunabhängiger Teil

1 Prozesse der unabhängigen Treuhandstelle

Die Treuhandstelle stellt im Wesentlichen ein technisch und organisatorisch unabhängiges System dar, bestehend aus einem Treuhänder, einer definierten Menge von Prozessen bzw. Abläufen und dafür benötigten autarken technischen Diensten. Sie übernimmt die Aufgaben des „Datentreuhänders" bzw. der „Vertrauensstelle", wie sie u.a. in den generischen Konzepten zum Datenschutz der TMF dargestellt werden [1].

Zu den typischen Aufgaben der unabhängigen Treuhandstelle zählen:

- die Zuordnung von personenidentifizierenden Daten und entsprechenden Kennungen für Quell- und Sekundärsysteme
- die Verwaltung von Einwilligungen, Ermächtigungen und Widerrufen
- die Pseudonymisierung bzw. De-Pseudonymisierung von Daten
- Mitwirkung bei
  - ⇨ Registerabrufen
  - ⇨ Sekundärdatenabgleich und –zusammenführung
  - ⇨ Durchführung von Follow-Ups (z.B.: Vitalstatus)
  - ⇨ Re-Kontaktierung, sowie Mitteilung von Zufallsbefunden
  - ⇨ Umsetzung von Widerrufen bzw. deren prozessualen Folgen
  - ⇨ Transferstellen-Prozess zur Daten- und Materialübergabe

Intern werden die Prozesse der Treuhandstelle durch festgelegte SOPs abgesichert. Nachfolgend werden zentrale Verantwortlichkeiten der Treuhandstelle, die zur erfolgreichen Erfüllung der übertragenden Funktionen wesentlich sind, näher betrachtet.

1.1 Eindeutige Identifizierung

Medizinische Einrichtungen verwenden typischerweise lokal eindeutige Kennungen (sog. Local Identifier), um medizinische Daten einer Person eindeutig zuzuordnen. Diese Kennungen haben jedoch nur innerhalb der jeweiligen Domäne (z.B. Klinik) Gültigkeit. Datensätze identifizierender Daten zur selben Person können in verschiedenen Quellen aufgrund von Schreibfehlern oder zwischenzeitlichen Änderungen voneinander abweichen, so dass es bei der Zusammenführung von Daten zu Zuordnungsfehlern kommen kann. Werden Daten verschiedener Personen fälschlicherweise einer einzigen Person zugeordnet, entsteht ein **Homonymfehler**. Im umgekehrten Fall spricht man von einem **Synonymfehler**. Ersterer ist fatal und im Nachgang nur mit sehr hohem Aufwand korrigierbar, letzterer ist technisch unter Zuhilfenahme weiterer Daten auflösbar.

Um Forschungsdaten aus mehreren Projekten und Studien einer einzigen Person zuordnen zu können, ist eine projektweite Kennung erforderlich, der sowohl die personenidentifizierenden Daten, als auch die einzelnen lokalen Kennungen zugeordnet sind. Dies muss fehlertolerant und nachvollziehbar erfolgen.

Aufgabe der Treuhandstelle ist es, Identitätsdaten unter Vermeidung von Homonymfehlern sicher vorhandenen Datensätzen zuzuordnen, neue Datensätze unter Vermeidung von Synonymfehlern anzulegen, potentielle Dubletten zu erkennen, mögliche unsichere Zuordnungen zu klären und in sichere Zuordnungen zu überführen sowie vorhandene Identitätsdaten zu aktualisieren.

Ergebnis der Zuordnung ist ein eindeutiger Master Person Index Identifier (MPI-ID), die gemäß den Konzepten der TMF (vgl. [2]) ein Pseudonym erster Stufe darstellt.

1.2 Pseudonymisierung

Nach §40 Abs. 2 BDSG sind personenbezogene Daten, die zu wissenschaftlichen Zwecken verarbeitet werden, frühestmöglich zu anonymisieren. Merkmale, mit denen Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können, sind bis dahin gesondert zu speichern. Gemäß § 34 Abs. 1 DSG M-V kann alternativ eine Pseudonymisierung der Daten erfolgen, sollten einer Anonymisierung wissenschaftliche Gründe entgegenstehen.

Die Pseudonymisierung besteht im Wesentlichen aus der *„Ersetzung des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren".* (§3 BDSG, [3]). Konkret wird der MPI-ID eine eindeutige Pseudo-Nummer (Pseudonym, PSN) zugeordnet.

Im Rahmen der Treuhandstelle wird eine Pseudonymisierung der medizinischen Daten durchgeführt, um:

- eine eindeutige Zusammenführung medizinischer Daten einer Person / eines Patienten / eines Probanden im Studienverlauf zu ermöglichen,
- die prospektive Nachverfolgung von Probanden im Rahmen von Follow-Ups zu realisieren,
- wiederholt den Kontakt zu Teilnehmern aufnehmen zu können,
- Qualitätssicherung gemeinsam mit den datenerhebenden Einrichtungen zu ermöglichen,
- und Sekundärdaten-Analysen zu ermöglichen.

Die angeführten Punkte machen im Rahmen von Projekten, Registerabrufen und Studien eine Umkehrbarkeit der Pseudonymisierung durch einen Datentreuhänder (Treuhandstelle) erforderlich. Es ist sichergestellt, dass identifizierende Daten ausschließlich innerhalb der Treuhandstelle gespeichert und verarbeitet werden. Das erzeugte PSN entspricht einem Pseudonym zweiter Stufe gemäß den Konzepten der TMF (vgl. [2]).

Grundsätzlich beschränkt sich die Pseudonymisierung nicht nur auf die MPI-ID. Im Rahmen unterschiedlicher Abläufe innerhalb der Treuhandstelle werden auf die gleiche Weise Probennummern, Laboraufträge, Bildnummern, u.a. umkehrbar unkenntlich gemacht. Um dabei den verschiedenen Fachdomänen Rechnung zu tragen, werden Pseudonyme domänenspezifisch generiert. Zudem besteht die Möglichkeit bereits erzeugte Pseudonyme erneut zu pseudonymisieren (Sekundärpseudonymisierung), beispielsweise im Rahmen der Daten- und Materialübergabe (Transferstellen-Prozess).

1.3 Einwilligung, Ermächtigung, Widerruf

Bevor Daten zu Forschungszwecken erhoben werden dürfen, ist es notwendig, *„die Einwilligung des Betroffenen in schriftlicher oder elektronischer Form einzuholen, wobei dieser vorab ausführlich über „Bedeutung und Tragweite der Einwilligung, (…) Art und Umfang der Verarbeitung (…) und beabsichtige Empfänger" der Daten zu informieren ist.*" (§8, Abs. 1-3 DSG M-V).

Zu den weiteren Aufgaben der Treuhandstelle zählt die Verwaltung von Einwilligungen, Ermächtigungen und Widerrufen, den sogenannten Informed Consent-Dokumenten (IC). Ein IC ist modular aufgebaut und besteht aus allgemeinen und projekt-/studien-/material-spezifischen Abschnitten.

Die Erstellung eines IC ist Teil des jeweiligen projektspezifischen Ethikkonzeptes. Die Inhalte werden in einem Abstimmungsprozess mit einer zuständigen Ethik-Kommission harmonisiert und durch ein Ethik-Votum bestätigt oder unter Auflagen korrigiert.

Eine Einwilligung muss eine Zweckbindung enthalten. Dies wird durch die Treuhandstelle vor Aufnahme des IC und Beginn des Regelbetriebs geprüft. Ferner muss der IC studienspezifische Aspekte im Detail regeln, für die analog eine Prüfung vorgenommen werden muss. Dazu zählen Bioproben bzw. Materialien, klinische Daten und Daten medizinischer Geräte. Mit der Datenhaltung des jeweiligen Projektes werden Verweise abgestimmt, die diese Module der Einwilligung referenzieren und über die vor der Speicherung medizinischer Daten (MDAT) seitens der Datenhaltung eine Prüfung des aktuellen IC erfolgt. Zudem muss die Einwilligung folgende organisatorische Punkte enthalten, die ebenfalls durch die Treuhandstelle geprüft werden:

- Wem gegenüber wird die Einwilligung erklärt?
- Wird die Person über ihr Widerrufsrecht informiert?
- An wen ist der Widerruf zu richten?
- Welche Folgen hat ein Widerruf?
- Welche Form kann der Widerruf haben?

Widerrufe werden in der Regel direkt durch den Patienten bzw. Studienteilnehmer oder indirekt über eine beteiligte Einrichtung an die Treuhandstelle übermittelt. Der Treuhänder ist für die Dokumentation des Widerrufes verantwortlich. Diese erfolgt elektronisch, enthält einen Mindestsatz Identitätsdaten und wird für die Durchsetzung des geleisteten Widerrufs im Falle einer erneuten Meldung benötigt. Ferner ist der Treuhänder für die Durchsetzung des Widerrufs zuständig. Dies beinhaltet das Einholen von Bestätigungen über das Löschen von Daten in den beteiligten Studienzentren, Registern, etc., sowie die Löschung der Pseudonyme und der Identitätsdaten (bis auf den vorgeschriebenen Mindestsatz in der Treuhandstelle). Abschließend erfolgt die Protokollierung und Rückmeldung an den Übermittler des Widerrufs.

1.4 Arbeit mit Sekundärdaten

Weitere Verantwortlichkeit der unabhängigen THS ist die Mitwirkung beim Abruf von Sekundärdaten. Mögliche Sekundärsysteme sind Melderegister, gesetzliche und private Krankenversicherungen, kassenärztliche Vereinigungen bzw. niedergelassene Ärzte. Die Treuhandstelle unterstützt bei der Durchführung von Datenabrufen, beim Abgleichen von Sekundärdaten und bei der Durchführung von Aktualisierungen.

1.5 Mitwirkung im „Use & Access"-Prozess

Die Bereitstellung von Daten im Rahmen eines Use & Access – Prozesses wird projektspezifisch definiert und erfordert in der Regel die Mitwirkung der unabhängigen Treuhandstelle.

Bevor eine Datenübergabe erfolgt, prüft die Treuhandstelle auf Widerrufe und führt eine domänenspezifische Sekundärpseudonymisierung der Daten bzw. des Materials durch. Dieser Schritt ist notwendig, um im Falle eines möglichen relevanten Zufallsbefundes die Zuordnung zur Person wiederherstellen zu können.

2 Technische Systeme

Technische Systeme (Funktionen) der Treuhandstelle unterstützen den Datentreuhänder bei der rechtskonformen Umsetzung der Prozesse und Arbeitsabläufe.

2.1 Master Person Index – MPI

Der Master Person Index (MPI) stellt die technische Funktionalität für die unter Kapitel 1.1 beschriebene eindeutige Identifizierung von Personen bereit. Es handelt sich um ein modulares Softwaresystem innerhalb der Treuhandstelle, in dem allen Personen einer Quell-Domäne ein eindeutiger systemübergreifender Index (Identifier, Kennzeichen), die MPI-ID zugeordnet wird. Bevor diese eindeutige Zuordnung jedoch erfolgen kann, werden die personenbezogenen Daten einer Dublettenerkennung unterzogen. Hierzu wird eine konfigurierbare Teilmenge aller vorliegenden personenidentifizierenden Daten algorithmisch genutzt; typischerweise fließen zumindest Vorname, Nachname, Geburtsdatum und Geschlecht ein.

Eine Dublettenerkennung wird dann notwendig, wenn die Subsysteme Personendaten und dazugehörige interne lokale Identifier selbst verwalten. Eine eindeutige Zuordnung von medizinischen Daten zu einer Person aus mehreren dieser autonomen Subsysteme auf Grundlage ihres lokalen Identifiers ist nicht möglich, da dieser nur innerhalb seines Systems eindeutig ist. Der vom MPI verwendete Algorithmus zur Dublettenerkennung erlaubt es, auch bei (in gewissen Grenzen) unvollständigen bzw. fehlerhaften demografischen Informationen zu einer Person eine korrekte Zuordnung zu einer eindeutigen systemübergreifenden Kennung (MPI-ID) vornehmen zu können.

Der MPI erweitert das Konzept des in [1] beschriebenen PID-Generators der TMF. Der Unterschied besteht in der zusätzlichen Speicherung domänenspezifischer lokaler Identifier sowie in den konkreten Algorithmen und Wichtungen der genutzten probabilistischen Funktionen. Die Speicherung dieser Zuordnung einschließlich der lokalen Identifier ist gleichermaßen Bestandteil des Prozesses zur Wiedererkennung einer Person.

Der Master Person Index wurde als Web-Service konzipiert. Die notwendige Datenspeicherung erfolgt über eine separate MySQL-Datenbank in der Treuhandstelle.

2.2 Pseudonymisierungsdienst

Der Pseudonymisierungsdienst der Treuhandstelle ist verantwortlich für die Generierung und Zuordnung eines Pseudonyms (Pseudonym zweiter Stufe gemäß [2]) zu einem domänenspezifischen Identifier (z. B. MPI-ID). Der Dienst ist ebenfalls als Web-Service konzipiert und kann gemeinsam mit anderen Services oder eigenständig eingesetzt werden. Alphabet und Länge der Pseudonyme, sowie Art des Prüfzeichenalgorithmus, zur Erkennung von Eingabefehlern, sind konfigurierkonfigurierbar. Die einzelnen Pseudonyme werden in einer Referenzliste innerhalb einer dem Pseudonymisierungsdienst lokal zugehörigen separaten MySQL-Datenbank geführt. Zusätzlich sind Depseudonymisierung und projektspezifische Sekundärpseudonymisierung (Pseudonyme dritter oder höherer Stufe) möglich.

Der PSN der TMF generiert Pseudonyme basierend auf dem der Person zugeordneten Identifier unter Angabe eines gemeinsamen Schlüssels („Shared Secret"). Nachteil dieses Vorgehens ist, dass bei Schlüsselverlust sämtliche Pseudonyme als kompromittiert angesehen werden müssen.

Die in der THS zum Einsatz kommende PSN-Lösung ermöglicht es, Pseudonyme auf Basis generischer Algorithmen für beliebige Eingabewerte zu erzeugen. Die Angabe eines Schlüsselwertes ist nicht erforderlich. Die hypothetische Kenntnis einer einzelnen Zuordnung impliziert keinerlei Kenntnis von Algorithmen oder weiteren Zuordnungen, da die Generierung und Zuordnung arbiträr erfolgen und ein Shared Secret keine Verwendung findet.

2.3 Consent Manager

Der Consent Manager ist für die technische Verwaltung und zentrale Speicherung des Informed Consent der Studienteilnehmer verantwortlich. Aufklärung und Einschluss von Personen ist durch medizinisch geschultes Personal am Ort des Einschlusses umzusetzen, um den einzuschließenden Personen die Möglichkeit für Rückfragen zu geben und diese sofort fachkundig beantworten zu können, so dass im ethischen und rechtlichen Sinne ein informiertes Einverständnis vorliegt. Der Consent Manager kann mittelbar durch die Mitwirkung bei der Generierung von Formularen zur Einwilligung und Ermächtigung bei der elektronischen Erhebung der Einwilligung von Personen unterstützen.

Es wird eine zentrale Schnittstelle zur Verfügung gestellt, über welche die studienspezifischen Einwilligungen und die dazugehörenden Module („Policies") elektronisch abgefragt werden können. Hierbei ist der Zugriff ausschließlich für vorab registrierte Systeme möglich. Im Rahmen der Datenherausgabe durch eine mögliche Transferstelle erlaubt der Consent Manager die automatisierte und tagesaktuelle Prüfung notwendiger mit den konkreten angeforderten Daten korrespondierender IC-Module.

Der Consent Manager wurde ebenfalls als Web-Service konzipiert. Die digitalen Repräsentationen der in den einschließenden Studienzentren verbliebenen, papierbasierten IC-Dokumente werden der jeweiligen Person innerhalb der Treuhandstelle mittels MPI-ID zugeordnet. Die jeweiligen ICs sind grundsätzlich modular aufgebaut. Jedem Einzelmodul ist eine technische Policy zugeordnet. Zudem unterstützt der Consent Manager die Versionierung von IC-Dokumenten, falls diese im Verlauf eines Forschungsprojektes modifiziert oder erweitert werden.

2.4 Architektur

Die Architektur der realisierten Treuhandstellenfunktionalität ist primär auf die Realisierung von Workflows ausgerichtet. Ein direkter Zugriff auf die einzelnen Dienste der Treuhandstelle (MPI, CM, PSN) von außen ist nicht vorgesehen und wird technisch durch Firewall-Regeln und nachgelagerte modulspezifische Autorisierung der Kommunikationspartner unterbunden.

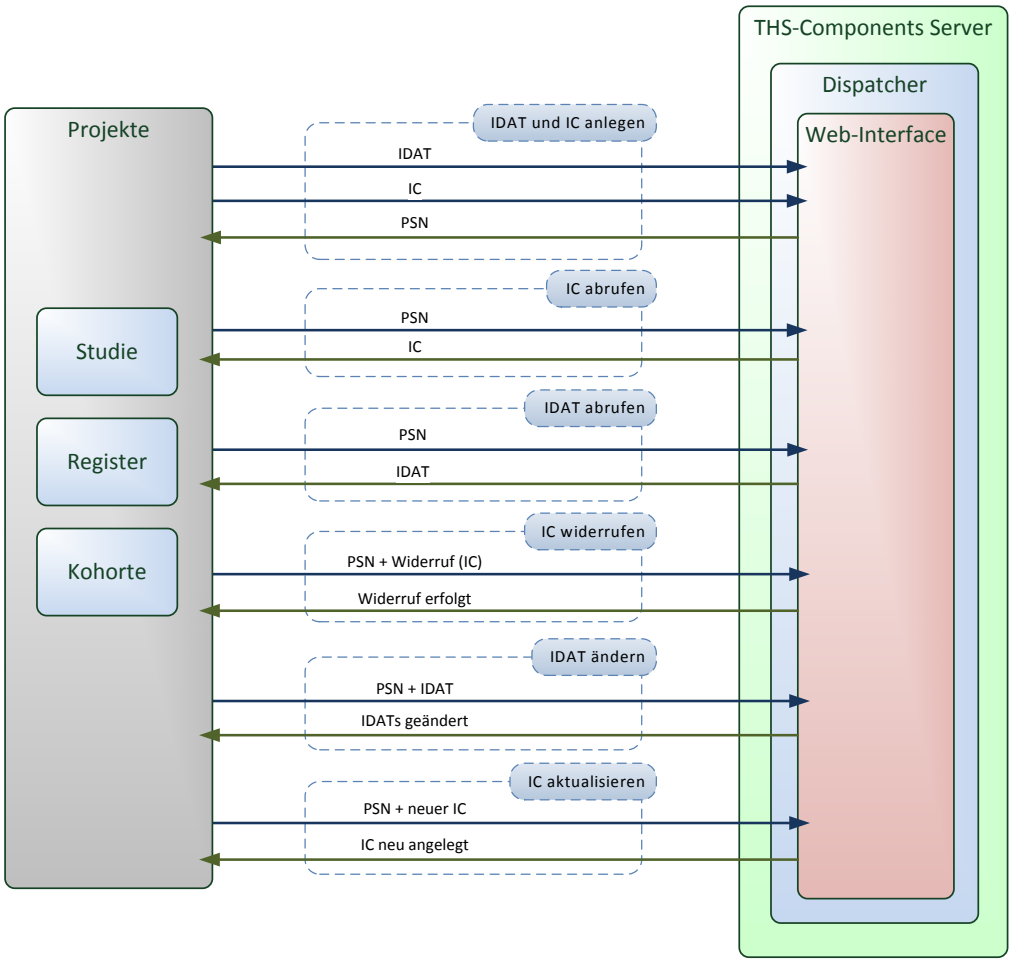


Abbildung 1 Mögliche Einsatzszenarien der THS-Schnittstelle

Extern nutzbare Funktionalitäten der Treuhandstelle werden durch den Dispatcher über eine REST-Schnittstelle bereitgestellt. Die Übergabe der Daten erfolgt im JSON-Format. Das grundsätzliche Design und Nutzungskonzept dieser Schnittstelle ist stark an die Mainzelliste [4] angelehnt. Abbildung 1 zeigt potentielle Anwendungsmöglichkeiten des angebotenen Dienstes.

Zentraler Aspekt der Architektur ist – neben den einzelnen funktionalen Modulen – der Workflow-Manager als Teil des Dispatchers. Der Workflow-Manager verwaltet sogenannte Workflow-Adapter, die jeweils die notwendige Logik zur Realisierung studienspezifischer Arbeitsabläufe beinhalten. Zu deren Implementierung wird auf die Basis-Funktionen MPI, CM und PSN der THS zurückgegriffen. Jedes Projekt, jede Studie bzw. jedes Register o.ä. verfügt über eigenständige Adapter. Der Workflow-Manager koordiniert die jeweiligen Anfragen an die zugrundeliegenden Dienste über entsprechende Clients und gibt jeweils die Antworten an das anfragende System zurück.

Die einzelnen Dienste werden als Web-Service bereitgestellt. Die Datenübertragung von Client und Server erfolgt verschlüsselt über HTTPS. Sämtliche notwendigen Daten werden in jeweils separaten Datenbanken vorgehalten, zu denen nur Mitarbeiter der Treuhandstelle Zugriff haben. Abbildung 2 veranschaulicht die beschriebenen Zusammenhänge.

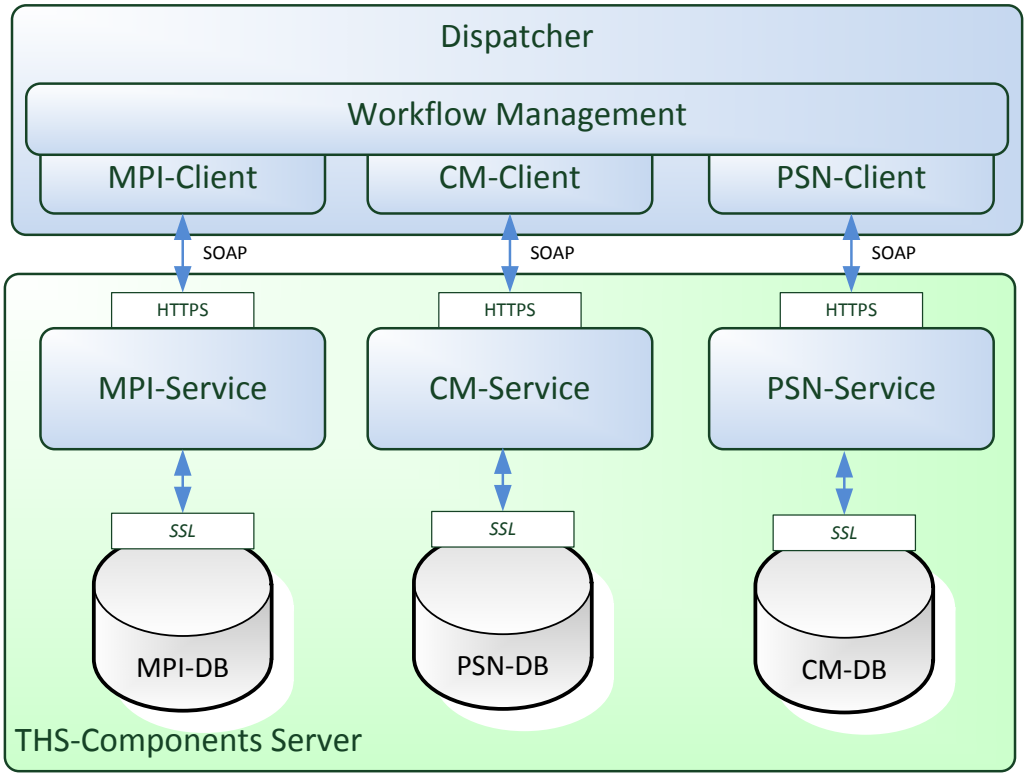


Abbildung 2 Technische Architektur der Treuhandstelle

3 Schutzbedarf

3.1 Rechtsgrundlagen

Die Verarbeitung personenbezogener Daten erfordert die Einhaltung einer Vielzahl von gesetzlichen Rahmenbedingungen. Zweck einer unabhängigen Treuhandstelle ist es, die Einhaltung der datenschutzrechtlich relevanten Forderungen zu gewährleisten und dennoch die für Forschungszwecke nötige Flexibilität gesetzeskonform zu ermöglichen. Nachfolgend werden wesentliche Bestimmungen betrachtet, um so die jeweils zutreffenden datenschutzrechtlichen Aspekte herauszuarbeiten.

Grundgesetz

Aus dem allgemeinen Persönlichkeitsrecht ergibt sich das Recht auf informationelle Selbstbestimmung, welches im Volkszählungsurteil vom Bundesverfassungsgericht als Grundrecht anerkannt wurde. So heißt es in dem Urteil: *„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Er-hebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.*“[1] [5]

1 BVerfGE 65, 1 – Volkszählung, 1983

Geheimnisschutz nach § 203 StGB

Für ein Projekt im medizinischen Kontext ist auch die ärztliche Schweigepflicht zu beachten, die im § 203 StGB geregelt ist. Diese Schweigepflicht betrifft dabei nicht nur Ärzte, Apotheker und ähnliche medizinische Berufe, sondern auch solche, die diesen Personen zuarbeiten. Dies sind z.B. Pflegekräfte und medizinische Fachangestellte. [5]

Datenschutzgesetze

Zur Gewährleistung der Unabhängigkeit der Treuhandstelle erfolgt die Datenverarbeitung in der Treuhandstelle in der Regel auf Grundlage einer Funktionsübertragung an den Betreiber der Treuhandstelle.

In diesem Fall liegt die Verantwortung für die Verarbeitung der Daten im Rahmen der übertragenen Funktionen bei der THS und fällt somit in den Wirkungsbereich des DSG M-V. Erster Ansprechpartner in Datenschutzfragen ist in diesem Fall der Landesbeauftragte für den Datenschutz des Landes M-V. Ferner haben Projektpartner die Möglichkeit weitere Bedingungen an die vereinbarte Funktionsübertragung zu knüpfen, wie beispielsweise die Gewährleistung landesspezifischer Datenschutzbestimmungen.

Das DSG M-V regelt detailliert sämtliche Verarbeitungsschritte personenbezogener Daten (§7 - §23 DSG M-V). Beispielsweise:

- wird eine frühestmögliche Anonymisierung der personenbezogenen Daten gefordert (§5). Hilfsweise ist auch eine Pseudonymisierung zulässig.
- ist die Einwilligung des Betroffenen in schriftlicher oder elektronischer Form einzuholen, wobei dieser vorab ausführlich über „Bedeutung und Tragweite der Einwilligung, (...) Art und Umfang der Verarbeitung (...) und beabsichtigte Empfänger" der Daten zu informieren ist. (§8, Abs.1-3 DSG M-V)
- ist die Nutzung der Daten nur zu dem Zweck zulässig, für den sie erhoben wurden. (§10 Abs. 2). Eine anderweitige Nutzung erfordert die Einwilligung des Betroffenen. (§10 Abs. 3)
- sind unkorrekte Daten zu korrigieren bzw. zu löschen (§13 Abs.1 und 2). Gleichermaßen kann auch eine Sperrung der Daten in Frage kommen (§10 Abs. 3).
- trägt die Verantwortung bei der Datenübermittlung an andere Stellen (Zulässigkeit, Datenschutz, IT-Sicherheit) die übermittelnde Stelle. (§14 bis §16)
- werden konkrete Maßnahmen zur Wahrung der Datensicherheit gefordert (§21).

Gleichermaßen regelt das DSG M-V die Rechte des Betroffenen zur Auskunft, zur Sperrung und zum Widerruf (§24, 25) und stellt gesonderte Forderungen an die wissenschaftliche Forschung (§34). Die zur Umsetzung der geforderten Rahmenbedingungen notwendigen technischen, personellen, räumlichen und organisatorischen Maßnahmen werden in einem Datenschutzkonzept festgehalten und mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit M-V (LfD M-V) abgestimmt.

3.2 Speicherung personenbezogener Daten

Aufgrund des medizinischen Kontexts fordern gesetzliche Rahmenbedingungen eine erhöhte Sensibilität beim Umgang mit personenbezogenen Daten. Die genannten Datenschutzgesetze regeln sämtliche Phasen bei der Verarbeitung medizinischer Forschungsdaten. Gleichermaßen beinhalten sie mögliche Konsequenzen, die eine Verletzung der Vorschriften und Restriktionen mit sich bringen kann.

Um genaue epidemiologische und auch forschungsbezogene Analysen auf Basis erhobener Forschungsdaten realisieren zu können, müssen medizinische und identifizierende Daten einer Person einander eindeutig und möglichst fehlerfrei zugeordnet werden können (vgl. Kapitel 1.1) und gleichzeitig den Ansprüchen des Datenschutzes genügen.

Die identifizierenden Daten (IDAT) bestehen i.d.R. aus Vornamen, Nachnamen, Geburtsnamen (falls abweichend), Geschlecht, Geburtsdatum, Geburtsort, Anschrift und ggf. auch Kontaktdaten wie Telefon, Fax und E-Mail-Adresse (vgl. Tabelle 1). Nach Rücksprache mit der Treuhandstelle ist eine Erweiterung des IDAT-Datensatzes im Rahmen einer Studie möglich. IDATs werden frühestmöglich von den medizinischen Informationen (MDAT) getrennt; der Treuhandstelle sind in keinem Fall medizinische Daten (MDAT) der eingeschlossenen Personen bekannt. Die konkreten Anforderungen an die IDAT sind jedoch abhängig vom jeweiligen Studiendesign. Geburtsdatum und Geschlecht der Person werden neben dem Namen für eine fehlerfreie Zuordnung pseudonymisierter Daten und im Rahmen wissenschaftlicher Auswertungen verwendet. Adressdaten und Kontaktinformationen dienen in aller Regel einer späteren (eingewilligten) Kontaktaufnahme.

Die Treuhandstelle übernimmt zusätzlich die Speicherung der erforderlichen Dokumente des Informed Consent, bestehend aus Einwilligungen, Ermächtigungen und Widerrufen.

Die Dauer der Datenspeicherung wird von der jeweiligen Studie bzw. dem jeweiligen Register im Informed Consent und im Ethik-Votum definiert. Bei der Festlegung der Dauer müssen gesetzliche Regelungen beachtet werden.

IDAT	Zweck
Name, Vorname, Geschlecht, Geburtsdatum, Geburtsort, Adresse, Mail, Telefon, Fax	Identifikation der Person innerhalb der Treuhandstelle, zur eindeutigen Zuordnung ihrer MDAT Durchführung von Registerabrufen, Sekundärdatenabgleich und Zusammenführung mit Sekundärdaten, Durchführung von Follow-Ups (z.B.: Vitalstatus), Mitwirkung bei Re-Kontaktierung
Elektronisch auswertbare Einwilligung der teilnehmenden Person	Grundvoraussetzung zur Speicherung und Abruf der IDAT innerhalb der Treuhandstelle

Tabelle 1 Übersicht der in der THS gespeicherten personenbezogenen Daten

3.3 Feststellung des Schutzbedarfs

Bei den zu speichernden personenbezogenen Daten handelt es sich um Einzelangaben über persönliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Daraus ergibt sich ein hoher Schutzbedarf in Bezug auf die Vertraulichkeit der zu speichernden Daten. Im Folgenden wird der Schutzbedarf für die Systeme der Treuhandstelle auf Grund der Anforderungen an die Grundwerte der IT-Sicherheit und in Bezug auf allgemeine Maßnahmen zur Datensicherheit (§21 LDSG-

MV) dargestellt. Der Schutzbedarf wird in die drei Schutzbedarfskategorien (normal, hoch und sehr hoch) eingestuft (vgl. [6]). Die konkrete Ausprägung des Schutzbedarfs ist im projektspezifischen Teil(Tabelle 3) definiert und erläutert.

4 Technische und organisatorische Maßnahmen

4.1 Organisationsstruktur der Treuhandstelle

Zur Übernahme von Funktionen eines Datentreuhänders in Projekten der klinischen, klinisch-epidemiologischen und epidemiologischen Forschung sowie in medizinischen Registern zur Qualitätssicherung an der Universitätsmedizin wird durch die Universitätsmedizin Greifswald eine unabhängige Treuhandstelle mit der Funktionsbezeichnung „Unabhängige Treuhandstelle der Universitätsmedizin Greifswald" eingerichtet, im Weiteren als Treuhandstelle bezeichnet.

Mit der Einrichtung der Treuhandstelle wird die Abteilung Versorgungsepidemiologie und Community Health des Institutes für Community Medicine (ICM-VC) auf Basis einer Vereinbarung mit der Universitätsmedizin Greifswald betraut.

In der Treuhandstelle arbeiten vertraglich angestellte Mitarbeiter der Universitätsmedizin Greifswald. Die Finanzierung aller Mitarbeiter der Treuhandstelle erfolgt durch die Mittel des Haushaltes der Universitätsmedizin Greifswald und durch projektbezogene Drittmittel. Der Leiter der Treuhandstelle wird von der Universitätsmedizin Greifswald eingesetzt.

Der Leiter der Treuhandstelle ist auf Basis der oben genannten Vereinbarung in seiner Tätigkeit zur Erfüllung der Aufgaben der Treuhandstelle sachlich unabhängig und weisungsfrei gegenüber dem Leiter der Abteilung ICM-VC sowie gegenüber der Universitätsmedizin Greifswald.

Für die Einrichtung der Treuhandstelle stellt die Abteilung ICM-VC für die Dauer des Bestehens der Treuhandstelle geeignete Räume zur Verfügung, welche den spezifischen Anforderungen der Treuhandstelle an die Informationssicherheit entsprechend ausgestattet werden, u.a. mit einer separaten Schließ- und Alarmanlage.

Technische Systeme zur Datenverarbeitung (z.B. physikalische Server, Software, Speichertechnik, Arbeitsplatzrechner) werden durch die Abteilung ICM-VC bereitgestellt. Hierbei wird durch geeignete technische Maßnahmen, wie in den folgenden Absätzen beschrieben, sichergestellt, dass jeder Zugriff auf Daten der Treuhandstelle durch die Abteilung ICM-VC ausgeschlossen ist.

4.2 Institutionelles Datenschutzkonzept des Instituts für Community Medicine

Organisation, räumliche Verteilung, personelle Besetzung und technische Ausstattung des Instituts für Community Medicine der UMG sind im „Rahmenkonzept Datenschutz und IT-Sicherheit für das Institut für Community Medicine der Universitätsmedizin Greifswald" [7] beschrieben. Die im Rahmenkonzept definierten Regelungen zu Datenschutz und IT-Sicherheit wurden mit dem Landesbeauftragten für den Datenschutz des Landes M-V abgestimmt, beschreiben die Grundsätze der Arbeit mit Daten am ICM-VC und gelten somit normativ als Basis für die projektspezifischen Ausprägungen der am ICM-VC geführten Unabhängigen Treuhandstelle. Diese werden im nachfolgenden Kapitel 5 präzisiert und ergänzt.

4.3 Netzwerkschutz

Grundsätzlich erfolgt der Betrieb der Treuhandstelle und der beteiligten Dienste in einem vom Netzwerk der Universitätsmedizin Greifswald separierten, isolierten Netzwerkbereich („THS-Zone").

Zur weiteren Verbesserung der Sicherheit wird auf Initiative des Institutes für Community Medicine an der Universitätsmedizin Greifswald das *Drei-Zonen-Konzept*[2] gemäß BSI-Grundschutz-Maßnahmenkatalog *„M 5.117 Integration eines Datenbank-Servers in ein Sicherheitsgateway"*[3] umgesetzt. Webservices und zugehörige Datenbanken werden in separaten Zonen betrieben.

Aus dem Internet (Zone „Extern") ist der Zugriff in die Demilitarisierte Zone (DMZ THS) möglich. Aus dieser wird eine Verbindung zur Transferzone (TZ THS) aufgebaut. Ebenso sind Zugriffe aus der Militarisierten Zone (MZ THS) zur Transferzone erlaubt. Ein „Durchstich" durch die TZ THS ist nicht möglich, Verbindungen können nur in die TZ THS hinein, nicht jedoch aktiv aus ihr heraus aufgebaut werden. Zwischen den Zonen ist der Kommunikationsfluss im Hinblick auf die Richtung des Verbindungsaufbaus durch Firewalls der Universitätsmedizin Greifswald eingeschränkt. Innerhalb des Gesamt-Netzwerkes existieren in sich geschlossene projektspezifische Zonen. Zwischen den einzelnen Subnetzen ist nur im jeweiligen Projekt- bzw. Anwendungskontext ein Verbindungsaufbau möglich. Abbildung 3 zeigt die beschriebenen Zusammenhänge. Zugriffe auf Services der THS sind nach erfolgreicher Authentifizierung nur über verschlüsselte Verbindungen möglich. Die Kommunikation zwischen Projekten und den Diensten der THS wird über zonenspezifische Proxy-Server realisiert und ist nur für registrierte IP-Adressen und Ports möglich.

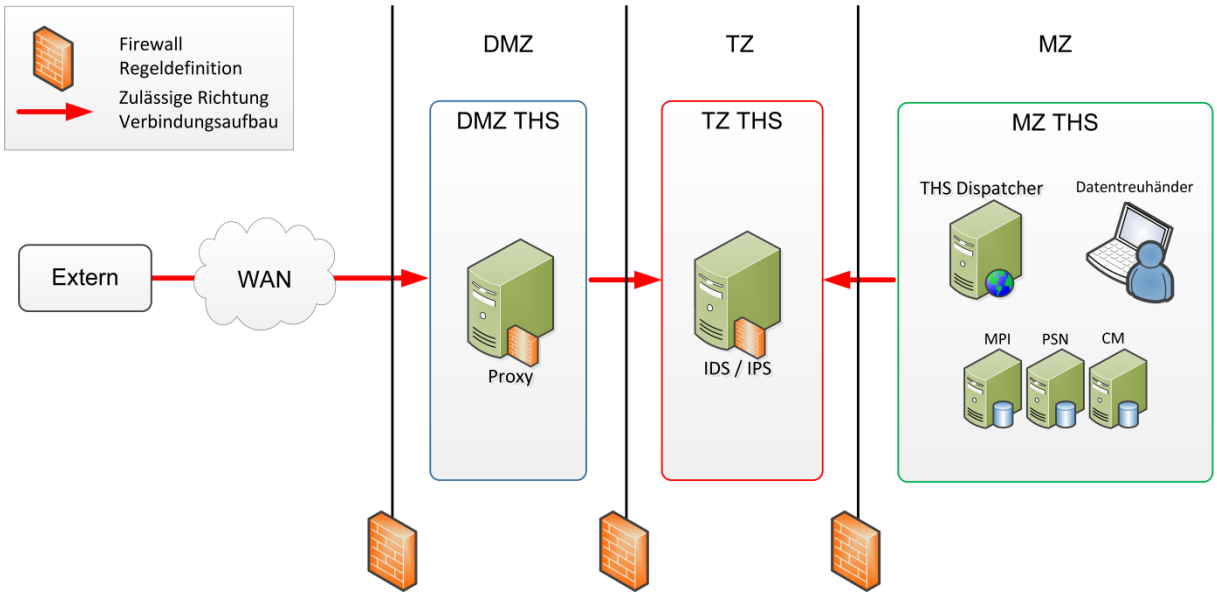


Abbildung 3 Zonenkonzept der Treuhandstelle

[2] Siehe Anlage „Konzept für den sicheren internen und externen Zugriff auf Forschungsdienste"

[3] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05117.html

4.4 Audit Trail

Innerhalb der Treuhandstelle werden alle Zugriffe auf Systeme und Daten durch ein Audit-Trail-Verfahren dokumentiert. Sämtliche Subsysteme protokollieren, durch wen der Zugriff erfolgte, wann der Zugriff erfolgte und auf welche Daten im Einzelnen zugegriffen wurde. Dies gilt sowohl für externe als auch für interne Zugriffe, wie beispielsweise durch technisches Personal der Treuhandstelle. Auf diese Weise lassen sich sämtliche Änderungen an den Daten nachvollziehen und die Integrität der Daten ist zu jedem Zeitpunkt gewährleistet. Zudem sind unterschiedliche Versionen von Datenständen im Fehlerfall wieder herstellbar.

4.5 Datenübertragung

Zur Datenübertragung wird standardmäßig HTTP als Übertragungsprotokoll genutzt. Externe Systeme sind verpflichtet, die verschlüsselte Variante HTTPS mit 256-Bit Verschlüsselung (oder höher) zur Datenübertragung zu nutzen. Um eine entsprechend hohe Sicherheit zu gewährleisten, wird HTTPS mit TLS-Verschlüsselung in der Version 1.0 oder höher verwendet. Browser die nur TLS in der Version 1.0 unterstützen, sollten zudem ein Client-Zertifikat nutzen. Browser, die TLS 1.2 oder höher einsetzen werden auch ohne den Einsatz von Client-Zertifikaten als sicher betrachtet. Als Algorithmen werden RSA mit einer Schlüssellänge von 2048 Bit, AES 256 und SHA256 verwendet. Diese entsprechen den Empfehlungen der Bundesnetzagentur[4] und gelten als sicher bis Ende 2018.

Die Kommunikation zwischen Treuhandstelle und externen Systemen wird zudem durch die Beschränkung von IP-Adressen abgesichert. Nur autorisierten IP-Adressen und Ports ist ein Verbindungsaufbau zu Diensten der Treuhandstelle gestattet (vgl. Zonenkonzept in Kapitel 4.3).

4.6 Datensicherheit

Datensicherheit wird durch die Umsetzung eines Rechtekonzepts auf Basis von Zugriffsebenen realisiert. Sämtliche Server der Treuhandstelle sind auf Betriebssystemebene verschlüsselt (AES-512), d.h. die Verschlüsselung wird eigenständig vom lokalen Betriebssystem durchgeführt. Jegliche Kommunikation über das Netz wird automatisch oder auf Anforderung verschlüsselt. Das notwendige Passwort besitzt der Datentreuhänder. Eine Kopie dieses Passworts befindet sich im Bankschließfach der Treuhandstelle, zu dem nur der Leiter der Treuhandstelle und der Datentreuhänder Zugriff haben. Es werden wöchentlich Komplett-Sicherungen der Server zum Schutz vor Elementarschäden durch autorisierte Administratoren durchgeführt. Diese können jedoch die Daten aufgrund der Verschlüsselung in keinem Fall einsehen. Die Sicherungen werden auf einem separaten Bandlaufwerk im selben Netzabschnitt gespeichert, das gemäß institutionellem Sicherheitskonzept [7] im Anschluss im Bankschließfach der Treuhandstelle hinterlegt wird. Zusätzlich werden automatisiert tägliche Backups der Systeme auf ein weiteres Bandlaufwerk zum Zweck der Disaster Recovery durchgeführt.

---

4 http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2012Algorithmenkatalog.pdf

4.7 Ausfallschutz

Die von der unabhängigen Treuhandstelle zur Verfügung gestellten Dienste müssen, um den ordnungsgemäßen Betrieb externer Partner gewährleisten zu können, permanent und zuverlässig online verfügbar sein. Im Folgenden werden Maßnahmen dargestellt, die die Wahrscheinlichkeit der Verfügbarkeit des Systems erhöhen und mögliche Ausfallzeiten minimieren. Dabei werden in der Spalte „Ursachen" mögliche Ursachen für eine Nicht-Verfügbarkeit des Systems aufgeführt.

Ursachen	Maßnahmen
fehlerhafte Systemkonfiguration (Software)	Test von Konfigurationsänderungen auf Testsystem Protokollierung der durchgeführten Änderungen durch geeignete Software Automatisierte Überwachung der Services durch geeignete Software, wie z.B. Nagios oder Xymon Änderungen und Anpassungen werden nur von fortlaufend geschultem Personal durchgeführt
fehlerhafte Systemkonfiguration (Hardware)	Vor dem Produktionsbetrieb erfolgen System- und Lasttests um die korrekte Funktion des Servers sicherzustellen. Dieselben Tests werden nach Austausch von Komponenten durchgeführt.
Ausfall von Einzelkomponenten (Hardware)	Betrieb des Systems auf zwei parallelen Servern in einem Hochverfügbarkeits-Cluster
Ausfall von Server-Systemen (Hardware)	Betrieb des Systems auf zwei parallelen Servern in einem Hochverfügbarkeits-Cluster
Ausfall von Stromversorgung (Infrastruktur)	Anschluss der Server an eine unterbrechungsfreie Stromversorgung (USV) zur Überbrückung kurzer Stromausfälle Aufgrund der nicht zwingenden Notwendigkeit des Systems für die med. Versorgung erfolgt bei längeren Stromausfällen keine Stromversorgung über ein Notstromaggregat (Nachdokumentation im System, sobald Strom wieder verfügbar).
Angriff auf Server	Einsatz restriktiv konfigurierter Firewalls Umfassendes Monitoring von Authentifizierung und ungewöhnlichen Datenanfragen

Tabelle 2 Maßnahmen zum Ausfallschutz

Zusätzlich zu den vorhergehend beschriebenen Maßnahmen wird sowohl bei ungeplanten Verfügbarkeitseinschränkungen als auch bei geplanten (z.B. Update mit Systemneustart) mit einer Nicht-Erreichbarkeit von mehr als 6 Stunden ein Ausfall-Bewertungsprozess gestartet. In einer grundle-

genden Dokumentation werden dabei die Dauer der Verfügbarkeitseinschränkung, der Grund der Verfügbarkeitseinschränkung und die Einflüsse der Verfügbarkeitseinschränkung auf die Nutzbarkeit des Systems festgehalten. Im Anschluss werden technische und organisatorische Maßnahmen erarbeitet um die Verfügbarkeitseinschränkung in Zukunft zu verhindern oder früher zu erkennen und ggf. automatisiert zu beheben.

4.8 Räumliche Trennung

Die Räumlichkeiten der Treuhandstelle befinden sich in einem separaten Gebäude in räumlicher Nähe zu der Abteilung Versorgungsepidemiologie und Community Health. Dadurch lässt sich uneingeschränkt gewährleisten, dass die im Rahmenkonzept Datenschutz und IT-Sicherheit des Instituts für Community Medicine festgelegten Maßnahmen und Prozesse beim Betrieb der THS sichergestellt werden.

Die THS verfügt über einen eigenen Eingang, einen separaten Schließkreis und eine eigene Alarmanlage. Ohne die Anwesenheit des berufenen Datentreuhänders ist kein Zugang zu den abgeschlossenen Räumlichkeiten möglich.

4.9 Personelle Maßnahmen

Für die Organisation der Treuhandstelle ist der „Datentreuhänder" verantwortlich, der keinem speziellen Projekt zugeordnet ist und der gegenüber den Projektpartnern oder dem beheimatenden Institut für Community Medicine (und übergeordnet der Universitätsmedizin Greifswald) weisungsfrei ist. Der Datentreuhänder i.S. des Gesetzes (DSG M-V) besteht aus einer definierten Gruppe von THS-Mitarbeitern, die in ihrer Funktion als Datentreuhänder nur dem Leiter der Treuhandstelle unterstehen. Dieser wiederum ist, in seiner Eigenschaft als Datentreuhänder weisungsfrei.

Eine gesetzliche Regelung zum Einsatz eines Datentreuhänders gibt es derzeit noch nicht, wohl aber wird der Einsatz seit dem Jahr 2000 empfohlen. [8] [9]

B. Projektspezifischer Teil

5 Projektspezifische Ausprägungen

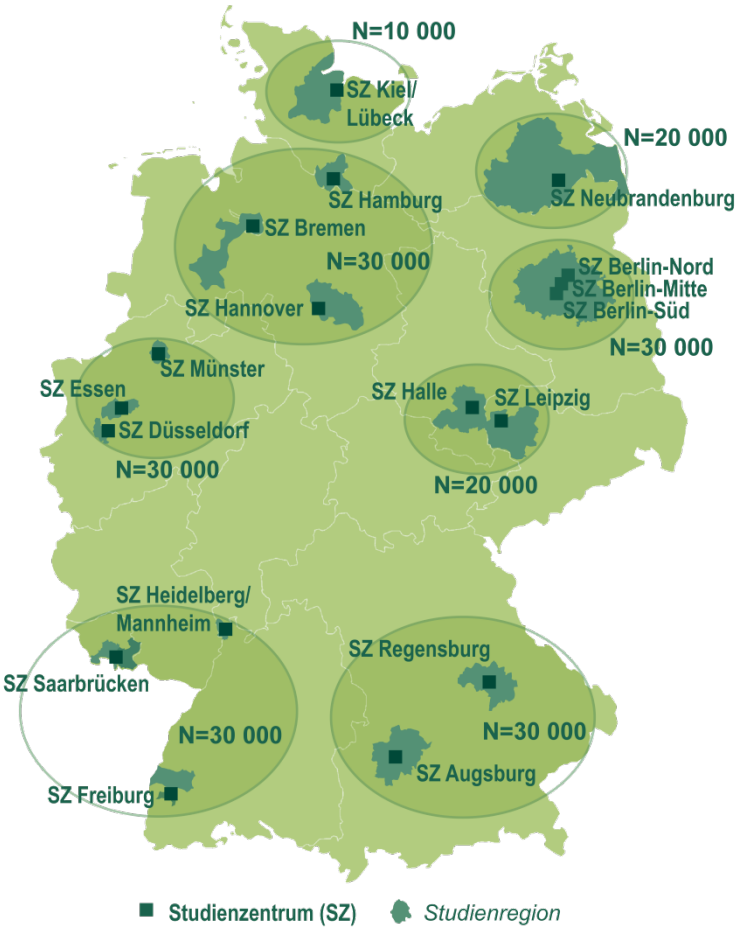


Abbildung 4 Studienzentren der Nationalen Kohorte

5.1 Projektbeschreibung

Die Nationale Kohorte ist ein gemeinsames interdisziplinäres Vorhaben von Wissenschaftlern aus der Helmholtz-Gemeinschaft, den Universitäten und anderen Forschungsinstituten in Deutschland. Ihr Ziel ist die Untersuchung der Entwicklung der wichtigsten chronischen Krankheiten (Krankheiten des Herz-Kreislaufsystems und der Lunge, Diabetes, Krebs, neurodegenerative/-psychiatrische und Infektionskrankheiten), ihrer subklinischen Vorstufen und funktionellen Veränderungen.

Für die Nationale Kohorte werden 200.000 Studienteilnehmer - Männer und Frauen im Alter von 20 bis 69 Jahren - aus verschiedenen Regionen Deutschlands rekrutiert. Für eine Subgruppe innerhalb der Kohorte von 40.000 Männern und Frauen ist ein intensiviertes Untersuchungsprotokoll vorgesehen. Zusätzlich werden bei einer Teilstichprobe Magnet-Resonanz-Tomographie (MRT)-Aufnahmen angefertigt. Rekrutierung und Nachbeobachtung der Teilnehmer der Nationalen Kohorte werden von 18 lokalen Studienzentren in acht geographischen Clustern, verteilt über fast

alle deutschen Bundesländer, durchgeführt (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**). Verantwortlich ist der „Nationale Kohorte e. V.".

Der Vereinsvorstand ist das verwaltende/leitende Organ der Nationalen Kohorte und wird die Gesamtverantwortung für die interne Handhabung der Daten und Proben im Rahmen der im Datenschutzkonzept festgelegten Aufgabenteilung haben. Er ist auch für die Überwachung der Umsetzung in den Studienzentren und weiteren beteiligten Stellen verantwortlich. Die erforderlichen vertraglichen Vereinbarungen werden unter den beteiligten Institutionen vor Beginn der Feldarbeit abgeschlossen.

5.1.1 *Beteiligte Institutionen und Kooperationspartner*

Abbildung 6 Beteiligte Institutionen

5.2 Projektspezifische Feststellung des Schutzbedarfs

Ergänzend zu den Definitionen zum Datenschutz im projektunabhängigen Teil erfolgt in der folgenden Darstellung die Feststellung des Schutzbedarfs der in der THS verarbeiteten Daten in Bezug auf die Funktionen, welche der THS im Rahmen der Nationalen Kohorte übertragen wurden.

Grundwert	Schutz-bedarf	Erläuterung	Begründung

Vertraulichkeit	Hoch	Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten als auch während der Datenübertragung.	Innerhalb der Treuhandstelle werden IDAT von Personen gemäß geltendem LDSG verarbeitet (siehe DSG M-V §§24, 25 und 34, analog gelten die entsprechenden Paragraphen des jeweiligen LDSG). Es werden Zuordnungen zwischen MPI-ID und PSN gespeichert, wodurch Rückschlüsse auf die Identität eines Projekt-/Studienteilnehmers möglich sind. Beeinträchtigungen der Vertraulichkeit durch unautorisierte Zugriffe beeinflussen Vertrauen in der Öffentlichkeit negativ. Das kann zum Rückgang der Studienbeteiligung führen und somit die Qualität der Studie beeinflussen.
Verfügbarkeit	Normal	Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden (gemäß GEP, GCP, IT-/ IS des LDSG).	Bei Ausfall der THS ist eine Beeinträchtigung der Arbeitsfähigkeit in den Studienzentren bzw. Registern möglich.
Integrität	Hoch	Personenbezogene Daten müssen während der Verarbeitung unversehrt, vollständig und aktuell bleiben.	Verlust der Datenintegrität durch fehlerhafte oder unvollständige Zuordnungen bedeutet finanziellen Schaden für das Projekt. Daten können zudem unbrauchbar werden.
Authentizität	Hoch	Echtheit und Glaubwürdigkeit einer Person oder eines Dienstes müssen überprüfbar sein.	Personenbezogene Daten müssen jederzeit ihrem Ursprung zuzuordnen sein. Kann die Korrektheit der Daten nicht gewährleistet werden, führt dies zu einer Beeinträchtigung der Integrität und des persönlichen Selbstbestimmungsrechts. Zudem kann eine fehlerhafte Zuordnung, z.B. bei Zufallsbefund, eine fehlerhafte Behandlung und somit erhebliche persönliche und psychische Belastungen verursachen.
Revisionsfähigkeit	Hoch	Es muss zu jedem Zeitpunkt feststellbar sein, wer wann welche personenbezogenen Daten auf welche Weise verarbeitet hat.	Verlust der Revisionssicherheit kann zur Beeinträchtigung des informationellen Selbstbestimmungsrechts führen und somit Ansehen der THS und Vertrauen in die THS in der Öffentlichkeit schaden. Vollständige Revisionsfähigkeit kann zur Klärung der Haftungsfrage durch Protokollierung beitragen.
Transparenz	Hoch	Verarbeitende Verfahren müssen vollständig und zeitlich zumutbar nachvollzogen werden können.	Nur durch vollständige Dokumentation kann die gesetzliche Forderung nach Auskunftserteilung realisiert werden. Ein Verlust der Transparenz kann in diesem Fall einen Gesetzesverstoß darstellen und eine negative Außenwirkung nach sich ziehen. Vollständige Transparenz kann im Fehlerfall Fehlerfindung und Klärung von Haftungsfra-

	gen ermöglichen.

Tabelle 3 Schutzbedarfsfeststellung der Systeme der Treuhandstellen (nach [5])

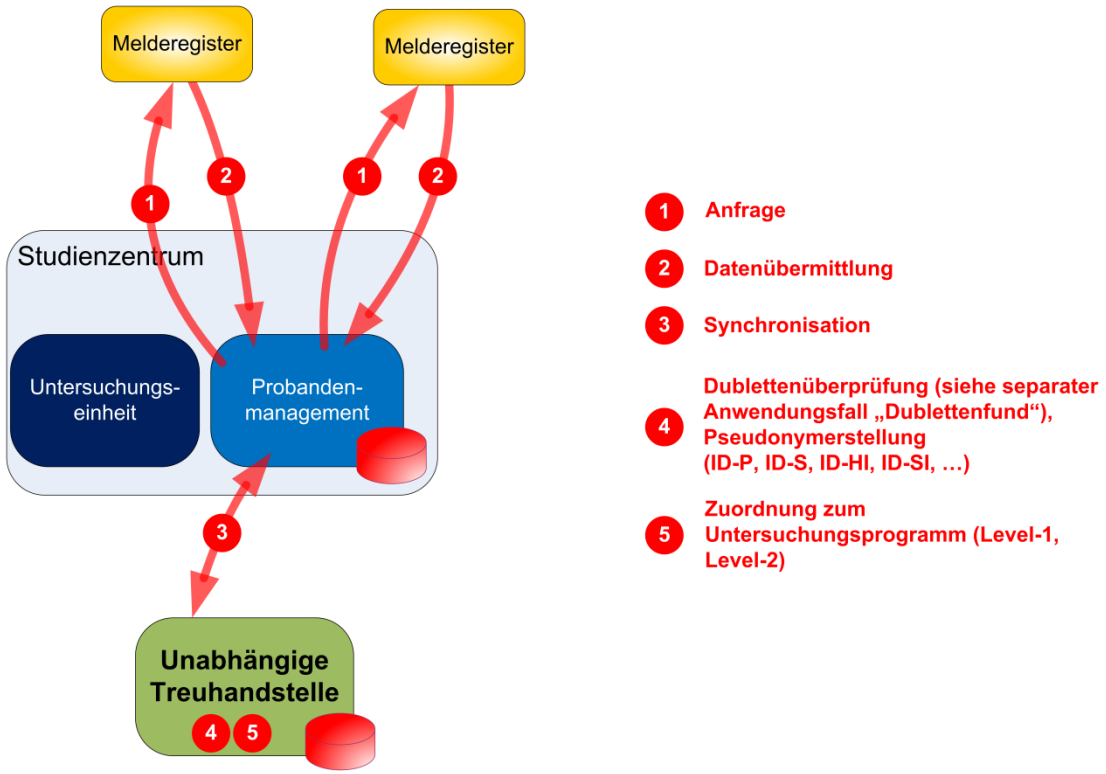
5.3 Arbeitsabläufe und Datenflüsse

5.3.1 *Stichprobenziehung*

Mit der Stichprobenziehung werden natürliche Personen ermittelt, die an der Studie teilnehmen sollen. Dieser Anwendungsfall wird in Abbildung 7 gezeigt. Dabei wird die Anfrage vom lokalen Probandenmanagement jedes Studienzentrums an die jeweiligen Melderegister oder Einwohnermeldeämter gestellt. Von diesen erhält das Probandenmanagement dann Datensätze von mehreren Tausend Probanden in unterschiedlichen Ausprägungen, bspw. nur mit einer Altersangabe an Stelle des kompletten Geburtsdatums. Die Datensätze werden an die Treuhandstelle gesendet und dort wird eine Dublettenprüfung sowie die Erstellung und Speicherung von Pseudonymen durchgeführt. Geprüfte Daten werden, inklusive der benötigten Pseudonyme, dem jeweiligen Probandenmanagement zur Verfügung gestellt. Das Probandenmanagement ist der primäre Ansprechpartner für die Probanden.

Eventuell treten bei der Prüfung auch unsichere Fälle auf, bei denen nicht eindeutig geklärt werden kann, ob die Person bereits in der Datenbank gespeichert ist. Diese Fälle werden im Kapitel 5.3.3 Dublettenfund im Detail erläutert. Im Anschluss an die Erstellung der Pseudonyme werden die Probanden bereits dem Untersuchungsprogramm (Level 1/2) zugeordnet um eine statistische Unabhängigkeit und Erfüllung der Fallzahlen zu erreichen.

Stichprobenziehung

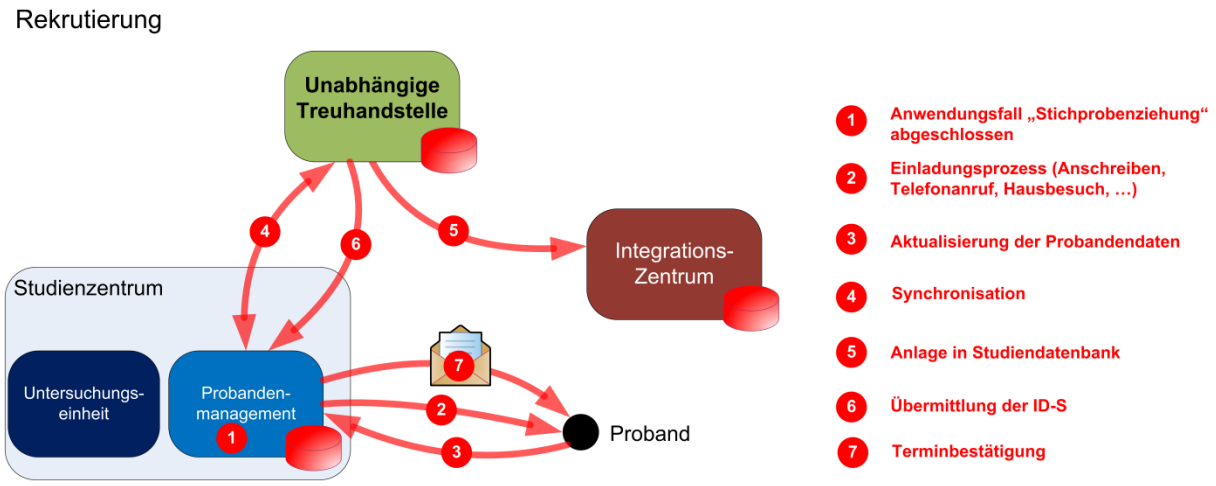


Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 25.02.2014

Abbildung 7 Melderegisterabfrage

5.3.2 *Rekrutierung*

An die Melderegisterabfrage schließt sich die Rekrutierung, die in Abbildung 8 gezeigt wird, an. Dabei werden vom Probandenmanagement des Studienzentrums die Probanden zur Teilnahme an der Studie eingeladen. Im Kontakt mit Probanden können sich Aktualisierungen der Probandendaten ergeben.. Das Probandenmanagement veranlasst eine Aktualisierung der personenidentifizierenden Daten bei der Treuhandstelle. Konnte der Proband erreicht werden, wird er vollautomatisch über eine Schnittstelle zwischen Treuhandstelle und Integrationszentrum mit seinem zugeordneten Untersuchungsprogramm in der Studiendatenbank angelegt. Dem Probandenmanagement wird daraufhin die ID-S übermittelt, mit der die Terminbestätigung gedruckt wird.



Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 25.02.2014

Abbildung 8 Rekrutierung

5.3.3 *Dublettenfund*

Dubletten können in mehreren Fällen auftreten, beispielsweise bei:

- Doppelter Übermittlung der Daten einer natürlichen Person durch das Melderegister
- Umzug eines Probanden in den Rekrutierungsbereich eines anderen Studienzentrums (durch die zeitlich asynchronen Melderegisterabfragen kann dies bereits in der ersten Rekrutierungswelle auftreten und nicht erst bei folgenden Wellen)
- Änderung des Namens durch Heirat, Scheidung oder Namensänderung
- Aktualisierung der Adresse eines Probanden

Die Prüfung auf Dubletten ist ein sehr komplexer Vorgang, der nicht immer vollautomatisch zu einem Ergebnis führt, sondern teilweise eine manuelle Nachkontrolle erfordert. Folgende Ergebnisse sind möglich:

- Person tatsächlich vorhanden („sicherer Match“)
- Person nicht vorhanden („kein Match“)
- Person möglicherweise vorhanden („unsicherer Match“)

Ist die Person tatsächlich vorhanden, wird das zugeordnete Pseudonym an den Nutzer im Probandenmanagement mit dem Hinweis zurückgeliefert, dass die Person bereits in der Datenbank existiert. Dies kann auftreten, wenn eine Person in den Rekrutierungsbereich eines anderen Studienzentrums zieht und dann im Rahmen der Melderegisterabfrage erneut ausgewählt wird. In Absprache mit beiden Studienzentren wird der Proband in diesem Fall dem Studienzentrum des aktuellen Wohnortes des Probanden zugewiesen.

Liegt dagegen ein unsicherer Match vor, kann also nicht automatisch zweifelsfrei geklärt werden, ob eine neu anzulegende Person bereits in der Datenbank vorhanden ist, muss der Fall per Hand geprüft werden. Es ist zwischen zwei Szenarien zu unterscheiden: die Dublette betrifft nur ein Studienzentrum oder mehrere Studienzentren.

Wenn ein unsicherer Match ausschließlich für ein Studienzentrum auftritt, wie in Abbildung 9 dargestellt, wird in der THS automatisch ein Ticket mit den beiden IDATs erstellt und das Probandenmanagement aufgefordert, die Daten, gegebenenfalls durch Kontaktaufnahme zum

Probanden, zu überprüfen und zu korrigieren. Dies schließt auch die Zusammenführung oder Auftrennung der IDATs ein. Das Probandenmanagement muss also aufklären, ob es sich bei dem unsicheren Match um eine oder zwei natürliche Personen handelt, um anschließend einen Datensatz mit zusammengeführten und bereinigten Daten oder zwei Datensätze zu erhalten. Nach der Datenbereinigung findet eine Synchronisation mit der THS statt.

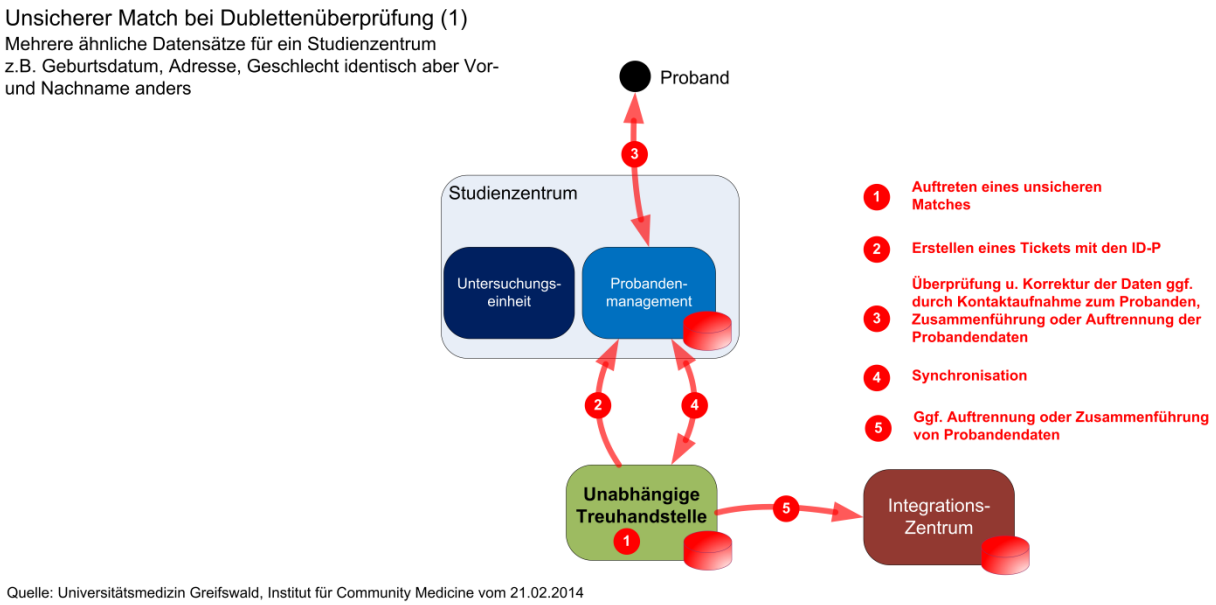


Abbildung 9 Dublettenfund bei einem Studienzentrum

Sollte ein unsicherer Match mehrere Studienzentren betreffen, wie in Abbildung 10 dargestellt, wird in der THS ein Ticket für das Studienzentrum angelegt, das die aktuelleren EMA-Daten besitzt. Das Probandenmanagement dieses Studienzentrums klärt ggf. durch Kontaktaufnahme zum Probanden, ob es sich um eine oder mehrere natürliche Personen handelt. Mit den aktualisierten Informationen des Probanden führt die THS die Auflösung des unsicheren Matches herbei. Die Pseudonyme werden von der THS im Anschluss überprüft und gegebenenfalls neu zugewiesen.

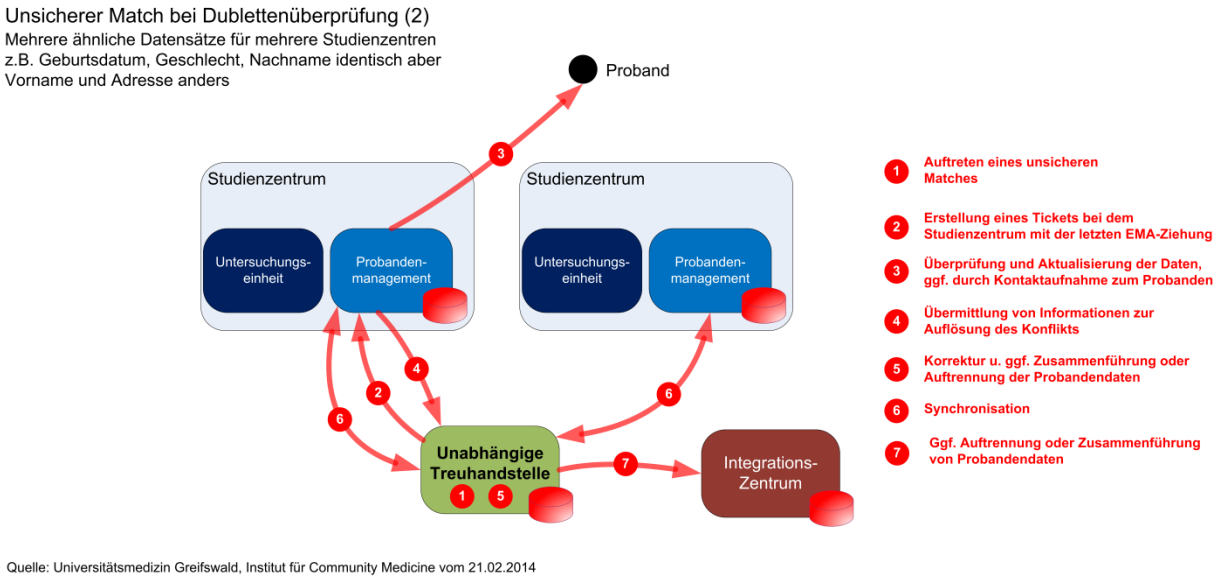
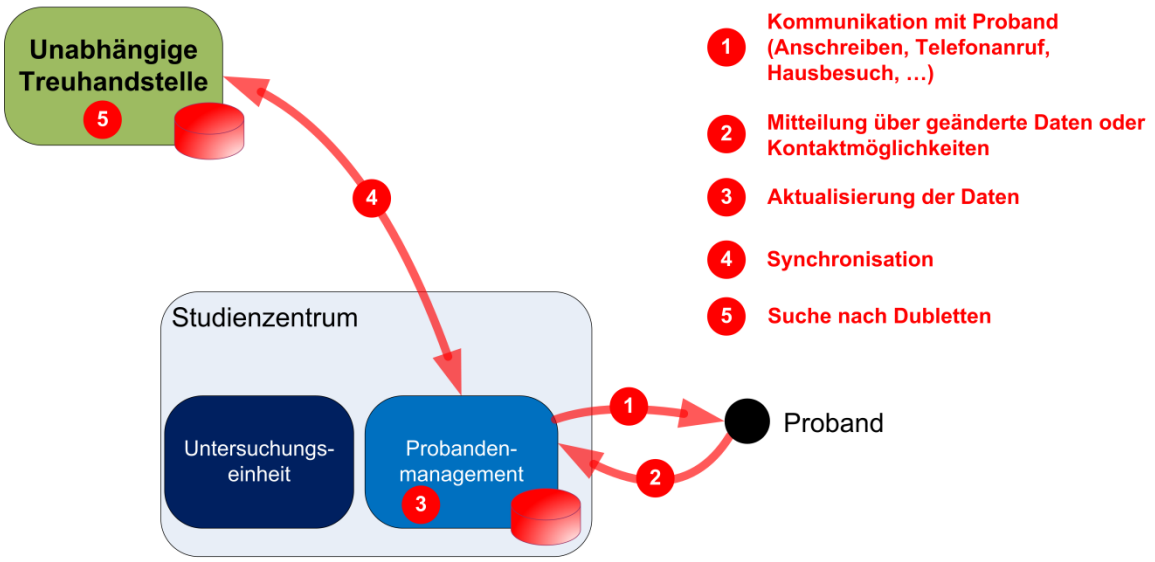


Abbildung 10 Dublettenfund bei mehreren Studienzentren

5.3.4 *Aktualisierung personenidentifizierender Daten*

Die Aktualisierung von personenidentifizierenden Daten kann aus verschiedenen Gründen und an verschiedenen Stellen notwendig sein. In Abbildung 11 wird der Prozess für die Aktualisierung der IDATs dargestellt, wenn sich im Verlauf der Kontaktaufnahme eine Datenänderung ergibt. In diesem Beispiel wird der Proband kontaktiert und teilt dem Probandenmanagement beispielsweise eine neue Adresse mit, die weiterhin im Rekrutierungsbereich des Studienzentrums liegt. Das Probandenmanagement nimmt diese Änderung auf. Daran schließt sich eine Synchronisierung über die Schnittstelle zur Treuhandstelle an, so dass in der THS die aktualisierten Daten vorliegen und vom Probandenmanagement im Bedarfsfall abgefordert werden können.



Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 21.02.2014

Abbildung 11 Aktualisierung IDAT bei Probandenkontaktaufnahme

Der Prozess einer sich im Untersuchungsablauf ergebenden Aktualisierung der IDATs wird in Abbildung 12 dargestellt. Als Beispiel wird hier der Fall betrachtet, dass das gespeicherte Geburtsdatum nicht dem tatsächlichen Geburtsdatum entspricht. Das Geburtsdatum wird bereits im Kontext der Aufklärung und Erfassung der Einwilligungen abgefragt und bei Bedarf korrigiert. Da es sich bei diesen Daten um personenidentifizierende Daten handelt, muss, nachdem die Daten im Integrationszentrum geändert wurden, der Datensatz in der Treuhandstelle aktualisiert werden. Dies soll vollautomatisch durch eine Schnittstelle zwischen Integrationszentrum und THS erfolgen. Eine sofortige Aktualisierung ist notwendig, da die THS die zentrale Instanz in der Datenverarbeitung der Nationalen Kohorte ist, die die personenidentifizierenden Daten der Probanden speichert und bei der diese abgerufen werden können. Eine Sonderstellung nehmen die Einwilligungen ein, die im folgenden Abschnitt beschrieben werden.

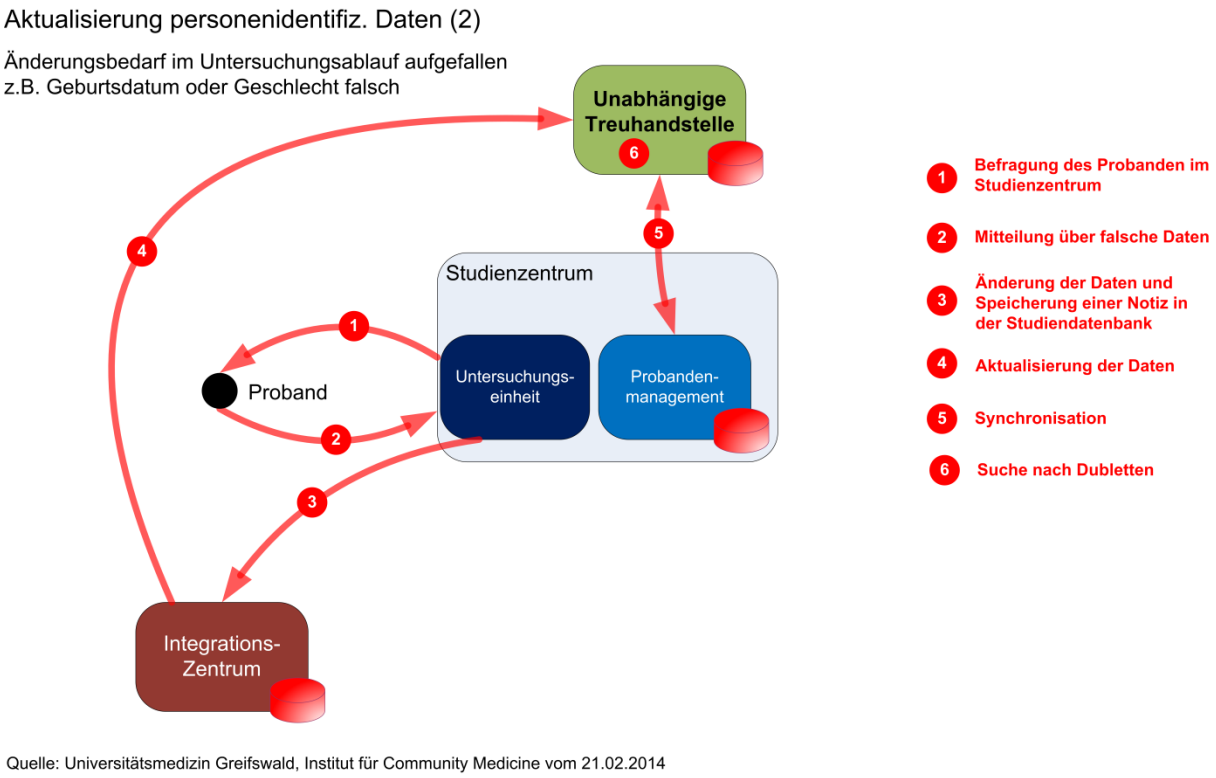


Abbildung 12 Aktualisierung IDAT im Untersuchungsablauf

5.3.5 *Widerruf*

Entsprechend des Ethik-Kodex der Nationalen Kohorte [10] ist der Widerruf einer Einwilligung in folgenden Ausprägungen möglich:

(1) "Kein weiterer Kontakt": Das Team der Nationalen Kohorte wird den Teilnehmer nicht mehr persönlich kontaktieren, wird aber nach wie vor die Erlaubnis haben, die Daten und Bioproben zu verwenden sowie Informationen aus sekundären Datenquellen (z. B. aus medizinischen Registern, Gesundheitsämtern) einzuholen.

(2) "Kein weiterer Zugang, aber weitere Nutzung": Das Team der Nationalen Kohorte wird den Teilnehmer nicht mehr kontaktieren und keine weiteren Informationen aus sekundären Datenquellen einholen. Die bereits erhobenen Daten und Bioproben dürfen jedoch weiterhin für Auswertungen verwenden werden.

(3) "Keine weitere Nutzung": Der Teilnehmer wird weder weiterhin kontaktiert, noch werden weitere Informationen eingeholt. Alle bisher gesammelten Daten werden gelöscht und noch vorhandene Bioproben werden vernichtet. Daten und Bioproben stehen damit für zukünftige Forschungsprojekte nicht mehr zur Verfügung. Bioproben, die zum Zeitpunkt dieses Widerrufs analysiert werden, werden zum frühestmöglichen Zeitpunkt blockiert. Allerdings wird es nicht möglich sein, Daten des Teilnehmers aus Analysen, die bereits durchgeführt wurden, wieder zu entfernen. Personen-identifizierende Daten werden gelöscht, soweit diese nicht zur Dokumentation des Widerrufs erforderlich sind.

Der Widerruf der Einwilligung geht vom Probanden aus und kann entweder an das Probandenmanagement des verantwortlichen Studienzentrums oder an die Geschäftsstelle des NaKo e.V. gerichtet werden, welche den Widerruf an die Treuhandstelle weiterleiten.

Entsprechend der Ausprägung des Widerrufs ermittelt die Treuhandstelle die folgenden notwendigen auszuführenden Maßnahmen.

(1) „Kein weiterer Kontakt": Es erfolgt eine Sperrung des Datensatzes für weitere Kontaktierungen. Der Widerruf wird dem Probanden bestätigt.
(2) „Kein weiterer Zugang, aber weitere Nutzung": Es erfolgt eine Sperrung des Datensatzes für weitere Kontaktierungen und den Abruf von Daten aus Sekundärdatenquellen. Der Widerruf wird dem Probanden bestätigt.
(3) „Keine weitere Nutzung": Es erfolgt eine Sperrung des Datensatzes für weitere Kontaktierungen und den Abruf von Daten aus Sekundärdatenquellen. Integrationszentren und Zentrales Biorepository werden mit der Löschung der Studiendaten und der Vernichtung der noch im Zentralen Biorepository und den dezentralen Probenlagern vorhandenen Proben beauftragt. Diese Einrichtungen bestätigen die Durchführung des Auftrages. Eine Aufbewahrungspflicht der personenidentifizierenden Daten in der Treuhandstelle wird bis zum Ende der Rekrutierungsphase wahrgenommen. Die gespeicherten IDATs werden genutzt, um eine korrekte Dublettenprüfung zu garantieren und um zu vermeiden, dass der Widerrufer erneut kontaktiert wird. Der Widerruf wird dem Probanden bestätigt.

Die Sperrung eines Datensatzes führt im Zusammenwirken der Treuhandstelle mit dem Probandenmanagement sowie anderen Organisationseinheiten der Nationalen Kohorte zu einem Ausschluss dieses Datensatzes bei der Übermittlung identifizierender Daten an diese Einheiten.

Für die Löschung von Daten und die Vernichtung von Bioproben gelten die Fristen gemäß Datenschutzkonzept der Nationalen Kohorte.

5.3.6 *Terminverwaltung*

Die Studienzentren vereinbaren mit dem Probanden einen Termin, an dem dieser befragt und untersucht werden soll. Dieser Prozess erfolgt im Probandenmanagement. Das Probandenmanagement stellt der Untersuchungseinheit die Daten zu den vereinbarten Terminen in Form von Tageslisten zur Verfügung. Die IDATs der Tageslisten werden vom Probandenmanagement über eine Schnittstelle zur THS abgerufen. Der Umgang mit den Tageslisten ist im Datenschutzkonzept der NAKO geregelt.

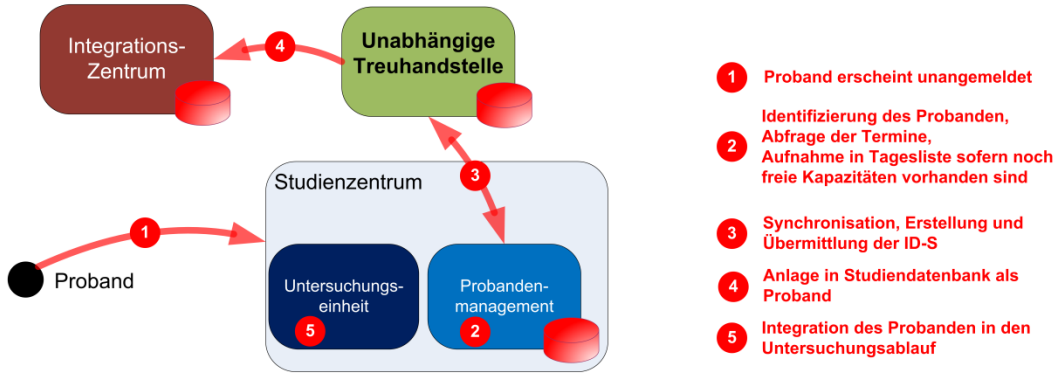
Im Fall, dass eine Person in der Untersuchungseinheit erscheint, die nicht auf der Tagesliste steht, prüft das Probandenmanagement des Studienzentrums, ob die Person rekrutiert und bereits als Teilnehmer der Studie in diesem Studienzentrum angelegt wurde. Sollte das der Fall sein, dann kann das Probandenmanagement, sofern es organisatorisch von der Untersuchungseinheit zu leisten ist, den Probanden in die Tagesliste aufnehmen oder anderenfalls einen neuen Untersuchungstermin vereinbaren. Da der Proband zu diesem Zeitpunkt noch keine ID-S und kein zugewiesenes Programm hat, muss eine Synchronisation der Datenbestände zwischen THS und Probandenmanagement erfolgen. Die THS erzeugt in diesem Zug die ID-S und veranlasst die Anlage des Probanden in der Studiendatenbank. Die Untersuchungseinheit kann dann den Probanden in

den Untersuchungsablauf integrieren. Sollte die Person im Probandenmanagement nicht als Proband aufgefunden werden können, erfolgt kein Einschluss in die Studie und es wird keine Untersuchung durchgeführt.

Der Fall, dass ein Proband bereits zur Teilnahme an der Studie eingeladen wurde, aber noch kein Termin vereinbart wurde, oder der Proband den Tag verwechselt hat, ist beispielhaft in Abbildung 13 dargestellt.

Terminverwaltung

Proband erscheint ohne Termin



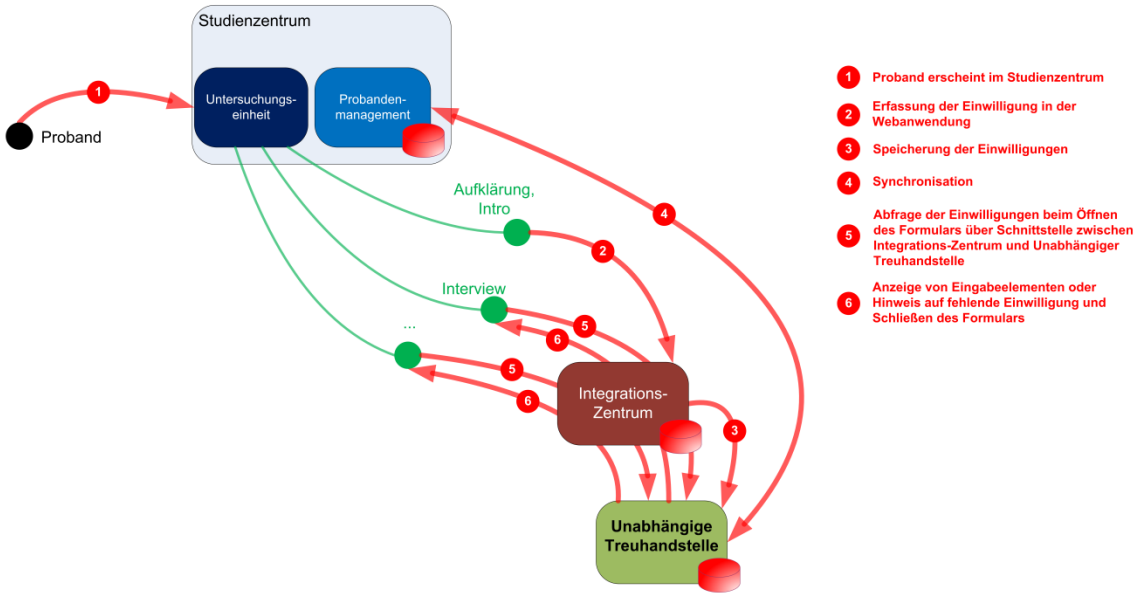
Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 21.02.2014

Abbildung 13 Proband erscheint ohne Termin

5.3.7 *Erfassung von Studiendaten*

Damit der Proband im Studienzentrum befragt und untersucht werden kann, müssen mehrere Anwendungsfälle bereits abgeschlossen sein. Der Proband muss mittels Melderegisterabfrage gezogen, rekrutiert und eingeladen worden sein. Wenn der Proband im Studienzentrum erscheint, wird er als erstes begrüßt, seine personenidentifizierenden Daten werden anhand der Tagesliste überprüft und gegebenenfalls geändert, wie in Abbildung 14 dargestellt. Im Anschluss wird er über die Studie aufgeklärt und nach seinen Einwilligungen gefragt, die schriftlich und mittels Webanwendung dokumentiert und über eine Schnittstelle zwischen Integrationszentrum und Treuhandstelle in der Treuhandstelle gespeichert werden. Die elektronischen Daten zu Einwilligungen stehen mittels Synchronisation auch dem Probandenmanagement zur Verfügung. Bei nachfolgendenen Befragungen, Untersuchungen und Speicherungen von Gerätedaten wird im Vorfeld in jedem Fall über die Schnittstelle zwischen Integrationszentrum und Treuhandstelle die Einwilligung abgefragt. Sollte die Einwilligung des Probanden vorliegen, kann die Befragung bzw. Untersuchung vorgenommen werden. Sollte sie nicht vorliegen, wird dem Untersucher ein Hinweis angezeigt und das Formular automatisch geschlossen. Um der Schriftform zu genügen und um langfristig nachweisen zu können, in welche Module der Proband eingewilligt hat, werden die Einwilligungsdokumente des Probanden mit seiner Unterschrift auch in Papierform im Probandenmanagement des Studienzentrums archiviert.

Erfassung von Studiendaten (1)

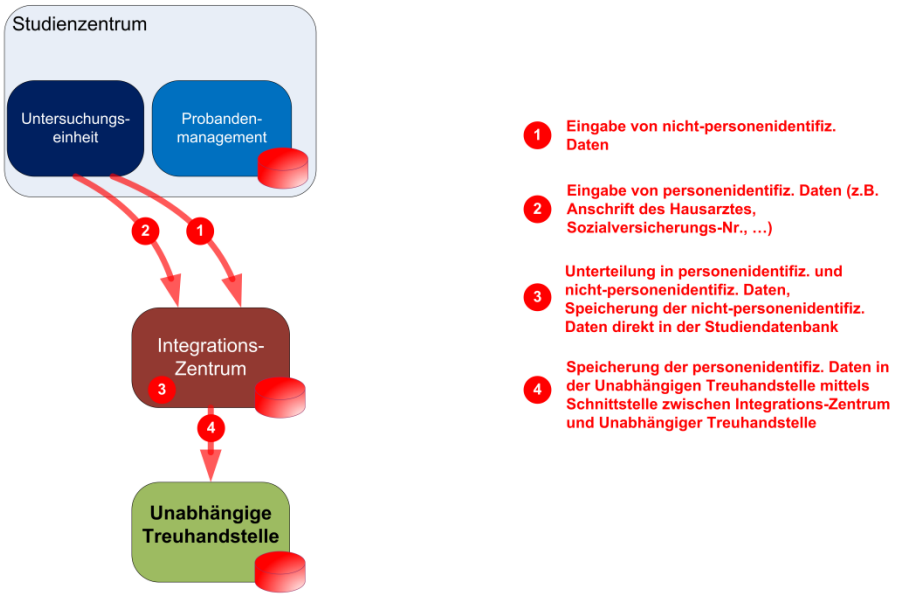


Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 21.02.2014

Abbildung 14 Erfassung von Studiendaten

Bei der Speicherung der Daten muss, wie in Abbildung 15 demonstriert, zwischen personenidentifizierenden Daten und Studiendaten unterschieden werden. Im Untersuchungsablauf tritt vereinzelt der Fall ein, dass in einem Formular beide Arten von Daten abgefragt werden, wobei die personenidentifizierenden Daten nicht in der Studiendatenbank des Integrationszentrums gespeichert werden dürfen. Aus diesem Grund besitzt das Integrationszentrum eine Schnittstelle zur Treuhandstelle, um die personenidentifizierenden Daten in der Treuhandstelle zu speichern. Die Studiendaten werden direkt im Integrationszentrum gespeichert. Diese Vorgehensweise stellt sicher, dass die personenidentifizierenden Daten zu jeder Zeit getrennt von den Studiendaten gespeichert werden.

Erfassung von Studiendaten (2)



Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 21.02.2014

Abbildung 15 Erfassung von Studiendaten und IDATs

5.3.8 *Abfrage von Sekundärdatenquellen*

Bei der Abfrage von Sekundärdatenquellen fragt die Kompetenzeinheit das Integrationszentrum nach Probanden, die ihre Kriterien erfüllen. Das Intergrationszentrum übermittelt passende Probanden mit ihren Studiendaten und der ID-S an die Kompetenzeinheit.

Die Kompetenzeinheit übermittelt die Liste dieser ID-S zusammen mit der Anfrageinformation zur Sekundärdatenquelle an die Treuhandstelle. Die Treuhandstelle prüft die Einwilligung aller betreffenden Probanden und erstellt jeweils ein neues Zweitpseudonym („ID-X", spezifisch für jede Sekundärdatenquelle). Die Treuhandstelle übermittelt die IDATs zusammen mit den ID-X an die Sekundärdatenquelle zur Durchführung der Datenerhebung. Die Sekundärdatenquelle stellt die Daten zusammen und übersendet sie nach Entfernung der personenidentifizierenden Daten zusammen mit der ID-X direkt an die Kompetenzeinheit. Mit Hilfe der Zuordnung zwischen ID-S und ID-X kann die Kompetenzeinheit die übergebenen Studiendaten und Sekundärdaten zusammenführen und auswerten. Nach der Analyse speichert die Kompetenzeinheit die aufbereiteten Sekundärdaten über eine Schnittstelle in der Studiendatenbank des Integrationszentrums.

Die Prozesse des Abrufs von Sekundärdaten von spezifischen Datenquellen (z.B. gesetzliche und private Krankenversicherungen, Kassenärztliche Vereinigung, ...) werden im Datenschutzkonzept der Nationalen Kohorte definiert und ausführlich beschrieben.

5.3.9 *Vitalstatusabfrage*

Zur Vitalstatusabfrage werden im ersten Schritt die personenidentifizierenden Daten mit einer Vitalstatus-ID (ID-V) an die Kompetenzeinheit übermittelt. Diese Daten werden in der Kompetenzeinheit nur für die Zeit der Abfrage gespeichert und im Anschluss daran wieder gelöscht. Mit den personenidentifizierenden Daten und der ID-V stellt die Kompetenzeinheit die Anfragen an die zuständigen Melderegister. Von den Melderegistern erhält es die Information, ob der Proband noch am Leben oder verstorben ist. Je nach Vitalstatus erhält die Kompetenzeinheit eine aktuelle Adresse des Probanden oder das Sterbedatum und den –ort. Diese Datensätze analysiert die Kompetenzeinheit und übersendet die aufbereiteten Daten an die Treuhandstelle. In der Treuhandstelle findet eine automatische Rückabbildung der ID-V auf die ID-P statt, gefolgt von der Aktualisierung der personenidentifizierenden Daten. Wie bereits in den vorherigen Abschnitten beschrieben, erfolgt in der Treuhandstelle bei der Aktualisierung der personenidentifizierenden Daten auch die Dublettenprüfung. Nach der erfolgreichen Übertragung werden die personenidentifizierenden und die im Zuge der Vitalstatusermittlung angefallenen Daten in der Kompetenzeinheit gelöscht. Parallel findet bereits die Synchronisation zwischen der Treuhandstelle und den Studienzentren statt. Sollte der Proband verstorben sein, werden Sterbeort und -datum mithilfe der Schnittstelle zum Integrationszentrum auch in der Studiendatenbank gespeichert.

5.3.10 *Todesursachenermittlung*

Für die Ermittlung der Todesursache durch die Kompetenzeinheit werden von der Treuhandstelle automatisch Datensätze mit den personenidentifizierenden Daten, der Todesursachen-ID (ID-TU), dem Sterbedatum und –ort und der Zuordnung zwischen ID-S und ID-TU von Probanden zusammengestellt, die verstorben sind, für die aber noch keine Todesursache bekannt ist. Anhand des Sterbeorts wählt die Kompetenzeinheit das zuständige Gesundheitsamt aus und fragt dieses mit den personenidentifizierenden Daten an. Als Antwort erhält die Kompetenzeinheit die Todesbescheinigung. Nach der Analyse und Codierung der Todesursache speichert die Kompetenzeinheit die Ergebnisdaten in der Studiendatenbank. Dies erfolgt in Kenntnis der Zuordnung zwischen ID-TU und ID-S direkt mit der ID-S. Nach der erfolgreichen Speicherung der Ergebnisdaten werden die personenidentifizierenden und die im Zuge der Todesursachenermittlung angefallenen Daten in der Kompetenzeinheit gelöscht.

5.3.11 *Ergebnisbrief*

Der Prozess der Erstellung des Ergebnisbriefs beginnt 10 Tage nach dem Abschlussgespräch. Im Integrationszentrum werden dabei die Ergebnisse eines Probanden zusammengestellt und über die Schnittstelle zur Treuhandstelle die Einwilligung zur Rekontaktierung und Ergebnismitteilung abgefragt. Bei einer fehlenden Einwilligung endet dieser Prozess mit dem Abschluss des Formulars „Ergebnisbrief". Sollten die Einwilligungen vorliegen, werden die Daten im Formular „Ergebnisbrief" angezeigt und in der Tagesübersicht des Studienzentrums als offen angezeigt. Die Untersuchungseinheit des Studienzentrums prüft, korrigiert und erweitert die Daten in diesem Formular mit Unterstützung des Studienarztes. Mit Abschluss des Formulars wird ein Dokument erzeugt, dass ausgedruckt und in einen Briefumschlag, versehen mit der ID-S, gelegt wird. Dieser verschlossene Brief wird dem Probandenmanagement des Studienzentrums übergeben, welches über die Schnittstelle zur Treuhandstelle die personenidentifizierenden Daten zur ID-S ermittelt, den Brief mit einem Adressaufkleber des Probanden versieht und dann verschickt. Die von der THS

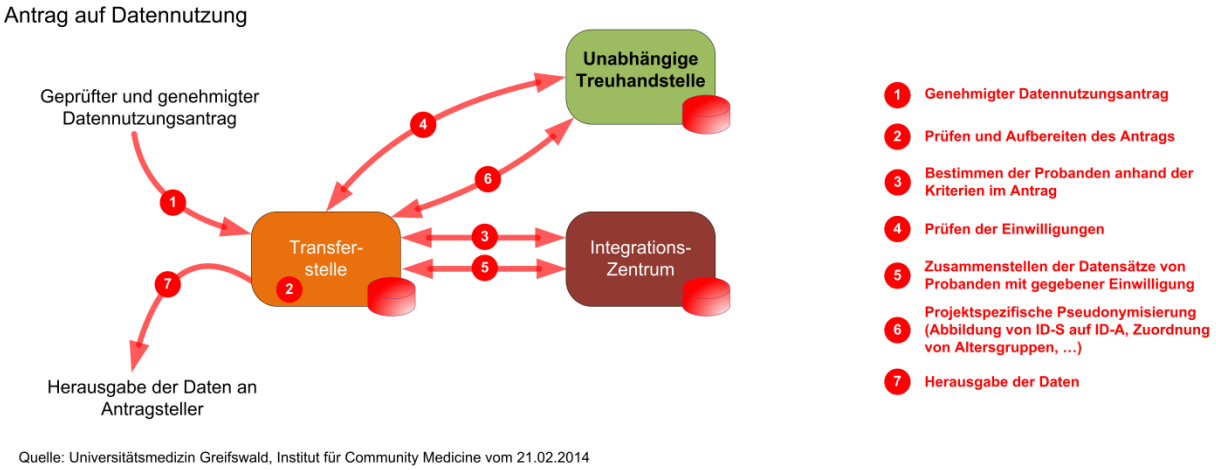
übermittelten personenidentifizierenden Daten werden unmittelbar im Anschluss an den Vorgang im Probandenmanagement gelöscht.

5.3.12 *Zufallsbefund*

Dieser Prozess beginnt mit einem Zufallsbefund auf den Studiendaten. Dies kann zum Beispiel bei der Befundung der MRT-Bilder auftreten. In diesem Fall muss bereits vor der Übermittlung des Befundes durch den Befunder eine Klassifizierung der Dringlichkeit vorgenommen werden. Sollte es sich um einen Notfall handeln, wird der Befund an das Studienzentrum übermittelt, wo der Befundbrief ohne Prüfung der Einwilligung erstellt, in einen Briefumschlag gelegt und mit der ID-S versehen wird. Dieser Brief wird dem Probandenmanagement übergeben und dort werden mittels Zuordung der ID-P zur ID-S die personenidentifizierenden Daten aufgerufen. Der Brief wird, wie in Absatz 5.3.11 beschrieben, mit der Adresse des Probanden versehen und verschickt. Sollte es sich um keinen Notfall handeln, wird im Probandenmanagement die Einwilligung des Probanden abgefragt und bei gegebener Einwilligung der Befundbrief erstellt und wie in Absatz 5.3.11 beschrieben mit der Adresse des Probanden versehen und verschickt.

5.3.13 *Nutzung von Studiendaten und Proben*

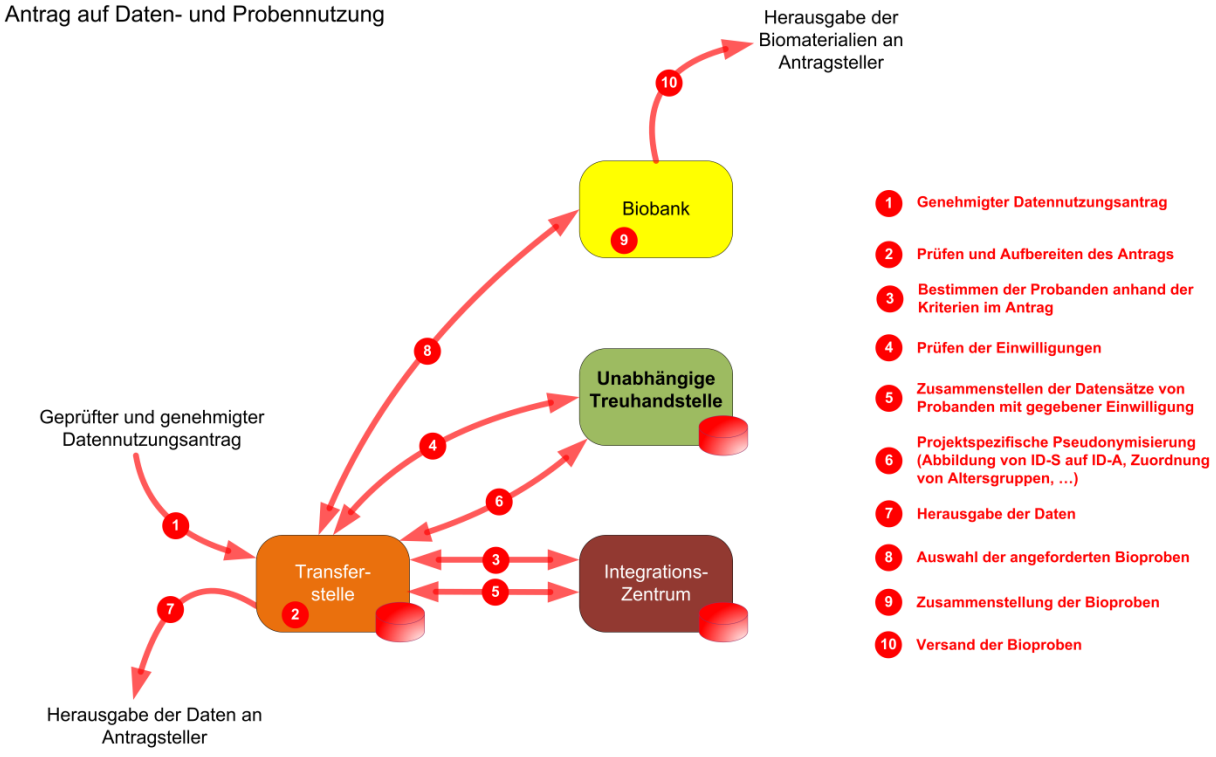
Die Nutzung der Studiendaten und Proben erfordert einen Datennutzungsantrag, der vom Use & Access Comitee bewilligt worden sein muss. Dies stellt auch den Startpunkt des Prozesses bis zur Übergabe der Daten in Abbildung 16 dar. Nach der Prüfung geht der Antrag in der Transferstelle ein, wo er geprüft und die angefragten Probanden ausgewählt werden. Da die Nutzung der Studiendaten die Einwilligung des Probanden erfordert, wird diese mittels Schnittstelle zur Treuhandstelle abgefragt. Für die Probanden, für die die Einwilligung vorliegt, werden die Studiendaten mittels Schnittstelle zum Integrationszentrum angefragt und dann über die Schnittstelle zur Treuhandstelle für diesen Datennutzungsantrag pseudonymisiert, d.h. die ID-S wird durch eine projektspezifische Transfer-ID (ID-A) ersetzt. Dies stellt sicher, dass es auch bei mehreren Anträgen durch einen Antragsteller nicht möglich ist, die Daten eines Probanden zusammenzuführen. Die Zuordnung zwischen ID-S und ID-A wird in der Treuhandstelle gespeichert, um die spätere Integration von Analysedaten zu ermöglichen. Die Datensätze werden von der Transferstelle aufbereitet und dem Antragsteller in der gewünschten Form (SAS-Dataset, XML-Datei, ...) in einem verschlüsselten Container übermittelt.



Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 21.02.2014

Abbildung 16 Antrag auf Datennutzung

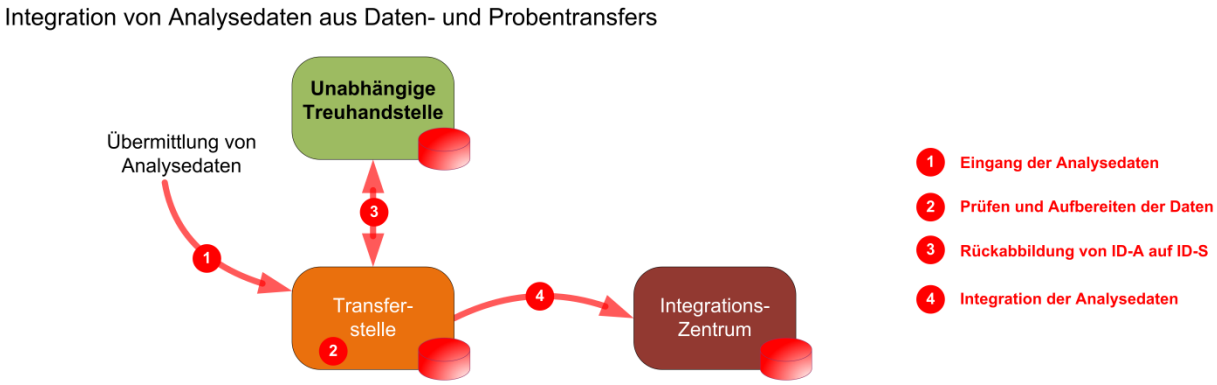
Sollten bei dem Antrag auch Bioproben angefordert worden sein, wird, wie in Abbildung 17 gezeigt, ein weiterer Vorgang angestoßen. Nach der Prüfung der Einwilligungen wird über die Schnittstelle zwischen Transferstelle und Biobank die Verfügbarkeit der angeforderten Bioproben festgestellt. Die angeforderten Bioproben werden in der Biobank zusammengestellt und direkt an den Antragsteller verschickt.



Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 21.02.2014

Abbildung 17 Antrag auf Daten- und Probennutzung

Die Integration der Analysedaten wird in Abbildung 18 verdeutlicht. Dabei gehen die Analysedaten in der Transferstelle ein und werden dort über die Schnittstelle zur Treuhandstelle von der ID-A auf die ID-S zurückabgebildet. Somit liegen die Daten dann für jeden Probanden zur ID-S zugeordnet vor und können über die Schnittstelle zum Integrationszentrum in der Studiendatenbank gespeichert werden.



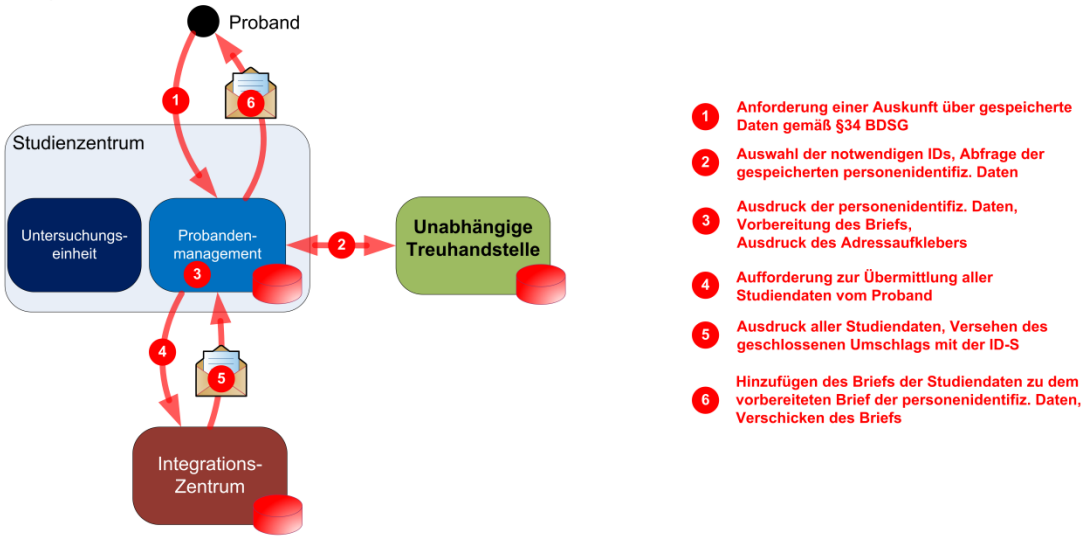
Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 21.02.2014

Abbildung 18 Integrations von Analysedaten

5.3.14 *Auskunft gemäß §34 BDSG*

Dem Probanden steht gemäß §34 des Bundesdatenschutzgesetzes das Recht auf Mitteilung seiner gespeicherten Daten zu. Dieser Prozess wird in Abbildung 19 gezeigt und beginnt mit der Anfrage des Probanden an das Probandenmanagement bzw. über die Geschäftsstelle an das Probandenmanagement. Im Probandenmanagement werden über die Schnittstelle zur Treuhandstelle die notwendigen IDs und die gespeicherten personenidentifizierenden Daten abgefragt. Die personenidentifizierenden Daten werden ausgedruckt und bereits in einen Briefumschlag gelegt, der mit dem Adressaufkleber des Probanden versehen wird. Mit der ID-S beauftragt das Probandenmanagement das Integrationszentrum, die Studiendaten dieses Probanden zu übersenden. Dies erfolgt aus Datenschutzgründen in der Regel als Ausdruck in einem mit der ID-S versehenen Brief. Dieser wird ungeöffnet dem vorbereiteten Brief mit den personenidentifizierenden Daten hinzugefügt so an den Probanden verschickt.

Auskunft gemäß §34 BDSG



Quelle: Universitätsmedizin Greifswald, Institut für Community Medicine vom 21.02.2014

Abbildung 19 Auskunft gemäß §34 BDSG

C. Anhang

6 Abkürzungsverzeichnis

IDAT – Identifizierende Daten

MDAT – Medizinische Daten

PSN – Pseudonym

MPI – Master Person Index

MPI – ID – Master Person Index Identifier

IC – Informed Consent

eCRF – Electronic Case Report Form

THS – Treuhandstelle

LfD M-V – Landesbeauftragter für Datenschutz und Informationsfreiheit M-V

BDSG – Bundesdatenschutzgesetz

DSG M-V Datenschutzgesetz für das Land Mecklenburg-Vorpommern

7 Glossar

Pseudonym – „Ersetzung des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren". (§3 BDSG, [3])

Informed Consent – Einwilligung, Einwilligungserklärung

Master Person Index – Softwaresystem, das mit Hilfe von Matching-Algorithmen system-übergreifend Personen eindeutig identifizieren und unterscheiden kann. Essentiell bei der Zusammenführung personenbezogener Daten unterschiedlicher Sub-Systeme.

Homonymfehler – Daten, die von unterschiedlichen Personen stammen, werden fälschlicherweise einer einzigen Person-zugeordnet.

Synonymfehler– Daten, die von einer einzigen Person stammen, werden fälschlicherweise mehreren scheinbar verschiedenen Personen zugeordnet

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

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

Einverständnis– Vereinbarung zwischen Patient, datenerhebender Stelle und Dritten, die die Nutzungsrechte der erhobenen Daten regelt, den zuständigen Arzt von der Schweigepflicht entbindet und Dritten weitere Schritte auf Grundlage der erhobenen Daten einräumt.

Register– Verzeichnis zur Erfassung der Fälle (und Todesfälle) einer bestimmten Krankheit oder einer Gruppe von Krankheiten in einem festgelegten Einzugsgebiet (z.B. Deutschland). Ein Register ist vollzählig, wenn alle Fälle im Einzugsgebiet erfasst wurden. Ein Register ist vollständig, wenn für jeden Fall alle notwendigen Informationen erfasst wurden.

8 Literaturverzeichnis

[1] C.-M.-. Reng, P. Debold, C. Specker und K. Pommerening, Generische Lösungen zum Datenschutz für die For-schungsnetze in der Medizin, Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006.

[2] TMF e.V., „tmf-ev.de," 2 Juli 2013. [Online]. Available: http://www.tmf-ev.de/Themen/Projekte/V000_01_PSD/tabid/303/EntryId/2525/Command/Core_Download/Method/attachment/Default.aspx. [Zugriff am 1 August 2013].

[3] juris.de, „gesetze-im-internet.de," 1990. [Online]. Available: http://www.gesetze-im-internet.de/bdsg_1990/__3.html. [Zugriff am 23 01 2013].

[4] M. Lablans, A. Borg und F. Ückert, „unimedizin-mainz.de," 2013. [Online]. Available: http://www.unimedizin-mainz.de/imbei/informatik/opensource/mainzelliste.html. [Zugriff am 02 August 2013].

[5] W. Hoffmann, M. Gerlich, C. Schäfer und J. Piegsa, „Datenschutz- und IT-Sicherheitskonzept für die HARMONIC-Studie im Rahmen des HICARE-Verbundprojektes," Greifswald, 2013.

[6] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-2, Bonn, 2008.

[7] W. Hoffmann, „Rahmenkonzept Datenschutz und IT-Sicherheit für das Institut für Community Medicine der Ernst-Moritz-Arndt-Universität Greifswald (3. überarbeitete Fassung)," Greifswald, 2010.

[8] H. Landtag, „29. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten," Kanzlei des Hessischen Landtags, Wiesbaden, 31.12.2000.

[9] N. Pöttgen, „Medizinische Forschung und Datenschutz, Dissertation," in *Schriften zum deutschen und europäischen öffentlichen Recht*, Frankfurt am Main, Peter Lang, Internationaler Verlag der Wissenschaften, 2009.

[10] E. Wichmann, C. Kleiser, I. Thiele, S. Ostrzinski und W. Hoffmann, „Ethik-Kodex der Nationalen Kohorte," München/Greifswald/Heidelberg, 2014.

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

[12] „Bundesministerium für Bildung und Forschung," [Online]. Available: www.bmbf.de/gesundheitszentren.php. [Zugriff am 01 08 2013].

[13] iAS GmbH, „secutrial.com," 2013. [Online]. Available: http://www.secutrial.com/. [Zugriff am 1 August 2013].

9 Anlagen

I.1 Rahmenkonzept Datenschutz und IT-Sicherheit für das ICM

I.2 Konzept für den sicheren internen und externen Zugriff auf Forschungsdienste