DZHK
DEUTSCHES ZENTRUM FÜR
HERZ-KREISLAUF-FORSCHUNG E.V.

Verfahrensbeschreibung und Datenschutzkonzept der Klinischen Forschungsinfrastruktur des DZHK

DEUTSCHES ZENTRUM FÜR HERZ-KREISLAUF-FORSCHUNG E.V.

Version 2.2 vom 20.03.2023

DZHK
DEUTSCHES ZENTRUM FÜR
HERZ-KREISLAUF-FORSCHUNG E.V.

Unabhängige Treuhandstelle
UNIVERSITÄTSMEDIZIN GREIFSWALD

Unabhängige Treuhandstelle

der Universitätsmedizin Greifswald K.d.ö.R.
Ellernholzstraße 1-2
17475 Greifswald

UNIVERSITÄTSMEDIZIN GÖTTINGEN UMG

Institut für Medizinische Informatik
Universitätsmedizin Göttingen

Robert-Koch-Straße 40
37075 Göttingen

DZHK
DEUTSCHES ZENTRUM FÜR
HERZ-KREISLAUF-FORSCHUNG E.V.

Zentrale Koordination
DZHK e.V. Geschäftsstelle
Potsdamer Straße 58
10785 Berlin

HelmholtzZentrum münchen
Deutsches Forschungszentrum für Gesundheit und Umwelt

Ethik-Projekt

Helmholtz Zentrum München
Deutsches Forschungszentrum für Gesundheit und Umwelt (GmbH)
Ingolstädter Landstr. 1
85764 Neuherberg

Universitätsmedizin
GREIFSWALD

LIMS-Betreiber

Universitätsmedizin Greifswald K.d.ö.R.
Fleischmannstraße 6
17475 Greifswald

CHARITÉ
UNIVERSITÄTSMEDIZIN BERLIN
LMU
KLINIKUM
DER UNIVERSITÄT MÜNCHEN

Universitäres Herzzentrum Berlin
Institute for Imaging Science and Computational Modelling in Cardiovascular Medicine
Augustenburger Platz 1
10117 Berlin

Klinikum der LMU
Klinik und Poliklinik für Radiologie
Marchioninistr. 15
81377 München

Inhalt

A Darstellung des Infrastrukturprojekts

1 Organisatorische Struktur

Der nachfolgende Abschnitt stellt den Projektrahmen vor, in dem dieses Dokument der Klinischen Forschungsinfrastruktur innerhalb des Deutschen Zentrums für Herz-Kreislaufforschung (DZHK) e.V. angewandt wird. Derzeitig besteht die Klinische Forschungsplattform aus den Teilprojekten der Unabhängigen Treuhandstelle (THS), der Datenhaltung (DH), dem Laborinformationssystem (LIMS), dem Bilddatenmanagementsystem (BDMS) sowie dem Ethik-Projekt (EP). Weiterhin werden projektspezifische Anforderungen und daraus resultierende Maßnahmen erläutert.

1.1 DZHK

Das DZHK ist eines von sechs deutschen Zentren der Gesundheitsforschung (DZG). Deren Gründungen wurden vom Bundesministerium für Bildung und Forschung (BMBF) initiiert und fanden 2009 bis 2012 statt. Organisiert sind die Gesundheitszentren als eingetragene Vereine (e.V.) innerhalb der Helmholtz-Gemeinschaft Deutscher Forschungszentren e.V., womit sie Forschungsnetzwerke innerhalb der größten deutschen außeruniversitären Wissenschaftsorganisation sind. Es ist vorgesehen, dass die Gesundheitszentren untereinander eng zusammenarbeiten, um ihre Ziele schneller zu erreichen.

Ziel des DZHK ist es, Prävention, Diagnose und Therapie bei Herz- und Kreislauferkrankungen zu verbessern und durch vielfältige Zusammenarbeit dafür zu sorgen, dass Forschungsergebnisse aus diesem Fachgebiet schneller in die reguläre klinische Anwendung aufgenommen werden.

Partnerinstitutionen sind Universitäten, Universitätskliniken und außeruniversitäre Forschungseinrichtungen (mehrere Max-Planck-Institute, das Max-Delbrück-Centrum und ein Leibnitz-Zentrum). Innerhalb des DZHK wurden verschiedene Kooperationen zu einzelnen Einrichtungen in Deutschland aufgebaut. Je nach Partizipationsgrad unterscheiden sich die Rechte und Pflichten dieser Standorte gegenüber dem DZHK[1]. Darüber hinaus werden Studienstandorte in nationale (Deutschland) und internationale (bspw. Griechenland, Polen, Dänemark) differenziert.

Die Arbeit aller Gesundheitszentren wird durch hochrangige, international besetzte Beratergremien begleitet und begutachtet. Hierbei werden neben der wissenschaftlichen Exzellenz auch die strategische Ausrichtung und die aufgebauten Strukturen und Prozesse evaluiert.

Finanziert wird das DZHK, ebenso wie die anderen DZG, vom BMBF. [1]

1.2 Entstehung des Verbundprojekts Klinische Forschungsplattform

Mit dem Schreiben vom 26.03.2013 beauftragte der Vorstand des DZHK die Universitätsmedizin Greifswald, vertreten durch das Institut für Community Medicine (ICM), sowie die Universitätsmedizin Göttingen, vertreten durch das Institut für Medizinische Informatik (MI) mit der Implementierung von einem Zentralen Datenmanagement als Verbundprojekt für multizentrische Studien und Register innerhalb des DZHK. Dieser föderale Ansatz bietet die Möglichkeit, die datenschutzrechtlich

[1]Weitere Informationen sind unter https://dzhk.de/ zu finden.

notwendige Trennung medizinischer und personenidentifizierender Daten organisatorisch und örtlich nach einheitlichem Standard umzusetzen. Die Erfassung der medizinischen Forschungsdaten erfolgt in der Regel im Kontext multizentrischer Studien.

Das Zentrale Datenmanagement war als Verbundprojekt gleichberechtigter und eigenverantwortlich handelnder Partner organisiert und bestand zunächst aus der Treuhandstelle (THS), der Datenhaltung (DH) und das IT-Lab, letzteres angesiedelt an der DZHK Geschäftsstelle. Die Anbindung weiterer Systeme zur Verarbeitung von Biomaterialdaten und Bildinformationen wurden bereits von Anfang an geplant, vergaberechtlich beauftragt und implementiert. Die zuvor organisatorisch genannten Grundlagen bleiben für alle Partner weiterhin erhalten.

Das vom Bereich Informationstechnologie (IT) der Universitätsmedizin Greifswald betriebene Labor-Informations-Management-System (LIMS) wird zur Steuerung und Dokumentation der Gewinnung, Verarbeitung, Lagerung und Ausgabe von Bioproben von Studienteilnehmer:innen verwendet. Technische Grundlage dieser Bioproben-Verwaltung ist die Software CentraXX der Kairos GmbH. Der Anschluss erster Pilotstandorte ist 2017 erfolgt (vgl. Abschnitt D).

Seit März 2018 wird für klinische Bilddaten eine für das DZHK anpasste Version des Datenmanagementsystems Trial Connect der Deutschen Telekom Healthcare and Security Solutions GmbH (DTHS) als Bilddatenmanagementsystem (BDMS) im DZHK eingesetzt. Im Rahmen einer Auftragsdatenverarbeitung des DZHKs wird es von der DTHS betrieben. Verwaltet und betreut wird es durch das Institut für kardiovaskuläre Computer-assistierte Medizin an der Charité-Universitätsmedizin Berlin und der Klinik und Poliklinik für Radiologie der Ludwig-Maximilians-Universität München. Das BDMS ist Grundlage sowohl für die standortübergreifende qualitätsgesicherte Erfassung von klinischen Bilddaten aus klinischen Studien als auch für die Bereitstellung dieser Daten (vgl. Abschnitt E).

Die Verantwortung für die Harmonisierung der Patientenunterlagen der DZHK-Studien (d. h. voll- bzw. überwiegend durch das DZHK finanzierte klinische Studien, Register oder Kohorten) wird im Rahmen des Ethik-Teilprojektes (EP) durch das Institut für Epidemiologie des Helmholtz Zentrums München wahrgenommen. Jede Studie des DZHK erstellt eigenverantwortlich auf den DZHK-Musterunterlagen basierende informierte Einwilligungen (IC, Informed Consent) und lässt diese vor Einreichung bei der zuständigen Ethikkommission durch das Ethik-Projekt bezüglich der Umsetzung der in diesem Konzept dargelegten Prozesse prüfen. Die DZHK-Musterunterlagen des IC enthalten bereits Textbausteine zur Beschreibung der Klinischen Forschungsplattform. Nach Einreichung der Unterlagen bei den zuständigen Ethikkommissionen zur Prüfung leiten die Studien das abschließend-positive Ethik-Votum an die THS und das EP weiter. Aufgabe der einzelnen Studienzentren ist die Rekrutierung von Studienteilnehmer:innen und die anschließende Datenerfassung.

Zusammen bilden die Teilprojekte THS, DH, IT-Lab (heute Zentrale Koordination), LIMS und BDMS die Klinische Forschungsplattform des DZHK.

Jeder Partner der Klinischen Forschungsplattform ist eigenständig verantwortlich den Datenschutz mit der jeweiligen institutionellen und ggf. behördlichen datenschutzbeauftragten Person abzustimmen.

Die beschriebenen Zusammenhänge werden im nachstehenden Organigramm veranschaulicht. (vgl. Abbildung 1)

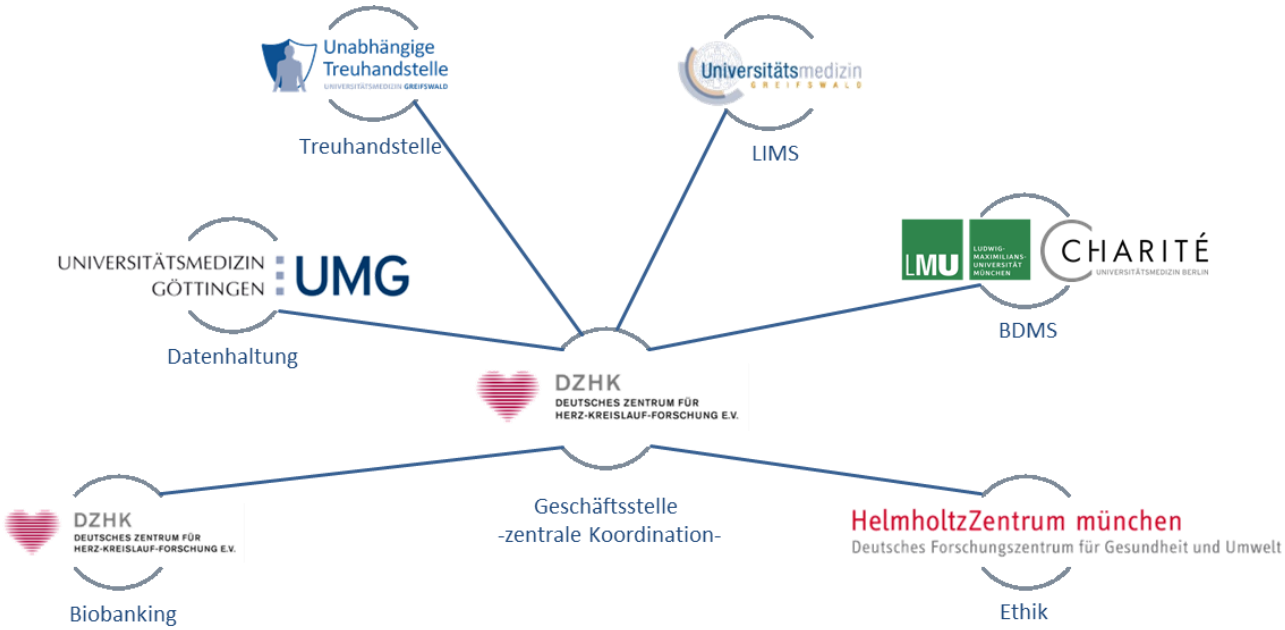


Abbildung 1: Partner des Verbundprojekts Klinische Forschungsplattformdes DZHK

1.3 Unabhängige Treuhandstelle

Die Unabhängige Treuhandstelle der Universitätsmedizin Greifswald wurde per Beschluss des Vorstandes der Universitätsmedizin Greifswald vom 22.04.2014 als zentrale Einrichtung der Universitätsmedizin Greifswald errichtet.

Mit ihrer Errichtung wird der Treuhandstelle die **Unabhängigkeit und Weisungsfreiheit gegenüber der Universitätsmedizin Greifswald zugesichert**. Im Rahmen der Aufsichtspflicht besteht für den Vorstand der Universitätsmedizin Greifswald eine Einsichts- und Kontrollmöglichkeit gegenüber der Treuhandstelle (weitere Details im Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2] Abschnitt 1.3)

Für die Einrichtung der Treuhandstelle stellt die Abteilung Versorgungsepidemiologie und Community Health des **Instituts für Community Medicine** (ICM-VC) geeignete Räume und technische Systeme zur Datenverarbeitung (z.B. Server-Hardware, Software, Speichertechnik, Arbeitsplatzrechner) zur Verfügung. Diese werden den spezifischen Anforderungen der Treuhandstelle an die Informationssicherheit entsprechend ausgestattet, u.a. mit einer separaten Schließ- und Alarmanlage für die THS-Räumlichkeiten.

Alle Tätigkeiten im Rahmen der Treuhandstelle werden ausschließlich in den Räumen der Treuhandstelle und mit den für die Treuhandstelle zur Verfügung gestellten Ressourcen ausgeführt. Ergänzende Informationen sind dem Datenschutz- und IT-Sicherheitskonzept der Unabhängigen Treuhandstelle der Universitätsmedizin Greifswald (Anlagen I.1, A1.5) zu entnehmen. [2]

Im DZHK verwaltet die Unabhängige Treuhandstelle die personenidentifizierenden Daten (IDAT) der Studienteilnehmer.

1.4 Institut für Medizinische Informatik

Seit 1999 widmet sich das **Institut für Medizinische Informatik** der Universitätsmedizin Göttingen (gegründet 1972) der medizinischen Verbundforschung und entwickelt in Kooperation mit Forschenden im In- und Ausland neue methodische Verfahren zur interdisziplinären multizentrischen Zusammenarbeit. Neben zahlreichen Einzelstudien wurden und werden die Kompetenznetze Demenzen, Angeborene Herzfehler und Multiple Sklerose sowie mehrere klinische Forschungsbereiche und der Sonderforschungsbereich 1002 durch das Institut methodisch und technisch unterstützt.

Gegenwärtig arbeiten über 40 Wissenschaftler:innen, Dokumentar:innen und Verwaltungskräfte in enger Abstimmung mit anderen Einrichtungen an den genannten Langzeitprojekten, sowie an der methodischen Unterstützung der Nationalen Zentren der Gesundheitsforschung in Deutschland. Im DZHK betreibt das Institut für Medizinische Informatik sowohl die Datenhaltung der medizinischen Daten (MDAT) als auch die Transferstelle.

1.5 Ethik-Projekt (EP)

Das **Institut für Epidemiologie** des Helmholtz-Zentrums München erforscht die Zusammenhänge von Umwelt, Lebensstil und Genetik bei der Entstehung und Progression verschiedener Krankheiten. Die Forschung stützt sich unter anderem auf die einzigartigen bevölkerungsbasierten KORA-Ressourcen (Kohorte, Herzinfarktregister, Aerosol-Messstation), die vom Institut verwaltet werden. Darüber hinaus kommen Daten und biologische Proben aus den Geburtskohorten GINI und LISA. Das Institut ist zudem an der NAKO Gesundheitsstudie beteiligt und für das zentrale Bioproben-Lager der NAKO verantwortlich.

Durch die langjährige Erfahrung innerhalb der KORA (Cooperative Health Research in der Region Augsburg) hat sich die **Arbeitsgruppe Biobank** der Abteilung Molekulare Epidemiologie des Instituts für Epidemiologie des Helmholtz-Zentrums München zu einem Expertenteam für alle Themen rund um das Biobanking entwickelt – angefangen bei ELSI Fragestellungen (ethische, rechtliche und soziale Aspekte), Bioprobenerfassung, -verarbeitung und -speicherung, bis hin zu Datenmanagement und Zugang zu Bioproben.

Das **Ethik-Projekt** des DZHK, angesiedelt innerhalb der Arbeitsgruppe und Teilprojekt der Klinischen Forschungsplattform, ist unter anderem verantwortlich für die Pflege des „Ethikkonzept des Bereichs Klinische Forschung des Deutschen Zentrums für Herz-Kreislauf-Forschung e.V.“, auf das im Folgenden für ergänzende Informationen für den Bereich Ethik verwiesen wird.

1.6 LIMS-Betreiber (Universitätsmedizin Greifswald)

Der Bereich Informationstechnologie (IT) der Universitätsmedizin Greifswald stellt für das DZHK sowohl Komponenten für den Netzwerk- und Serverbetrieb als auch umfassendes Know-How mit der CentraXX-Software der Kairos GmbH zur Verfügung, da die Software-Produkte der Firma Kairos an der Universitätsmedizin Greifswald bereits für unterschiedliche Anwendungsszenarien betrieben werden. Neben dem Betrieb als Biobanking-Labor-Informations-Management-System (LIMS) für das DZHK, werden an der Universitätsmedizin Greifswald auch CentraXX-Instanzen für das forschungsorientierte Klinische-Arbeitsplatz-System KAS+ und die Core Unit Biobanking bereitgestellt.

Die Betreuung der Endanwender:innen des DZHK erfolgt in enger Kooperation mit der Zentralen Koordination – der DZHK Geschäftsstelle (DZHK-GSt.).

1.7 BDMS-Betreiber

Die Deutsche Telekom Healthcare and Security Solutions GmbH (DTHS) betreibt die Software „Trial Connect“ für das Bilddatenmanagementsystem und speichert die Bilddaten. Das Institut für kardiovaskuläre Computer-assistierte Medizin an der Charité-Universitätsmedizin Berlin übernimmt die technische Koordination für das BDMS und die Klinik und Poliklinik für Radiologie der Ludwig-Maximilians-Universität München verantwortet die Nutzerschulung sowie die Qualitätssicherung der Bilddaten.

1.8 Zentrale Koordination (DZHK-GSt.)

Die Zentrale Koordination der sechs Projekte der Klinischen Forschungsplattform des DZHK ist in der DZHK-GSt. angesiedelt und ist unter anderem verantwortlich für die Koordination des Gesamtkonstruktes, sowie für die Interaktion der Forschungsinfrastruktur mit den geförderten klinischen Studien in Vorbereitung und in Rekrutierung.

1.9 Vertragliche Grundlage der Zusammenarbeit

Die Klinische Forschungsplattform des DZHK kann nur als Gesamtheit die ihr übertragenen Aufgaben erfüllen. Alle Projektpartner stellen notwendige Komponenten für das Erreichen der im Vorfeld beschriebenen Ziele dar. Für die Zusammenarbeit aller Teilbereiche wurden Kooperationsverträge mit dem DZHK geschlossen.

1.10 Aufgaben im Verbundprojekt Klinische Forschungsplattform

Die zur erfolgreichen Implementierung der Klinischen Forschungsplattform notwendigen technischen und organisatorischen Maßnahmen werden im Folgenden durch die Teilprojekte der Klinischen Forschungsplattform näher beschrieben. Abbildung 2 stellt den Weg der gewonnenen Daten in den Studienzentren über die Infrastruktur bis hin zur Herausgabe von Daten und Biomaterial an Wissenschaftler:innen dar. Die organisatorischen und technischen Prozesse werden im Rahmen des hier vorliegenden Datenschutzkonzeptes, verschiedenster datenschutzrechtlicher Regularien, eines Ethik-Konzeptes, sowie der DZHK Nutzungsordnung verwaltet.

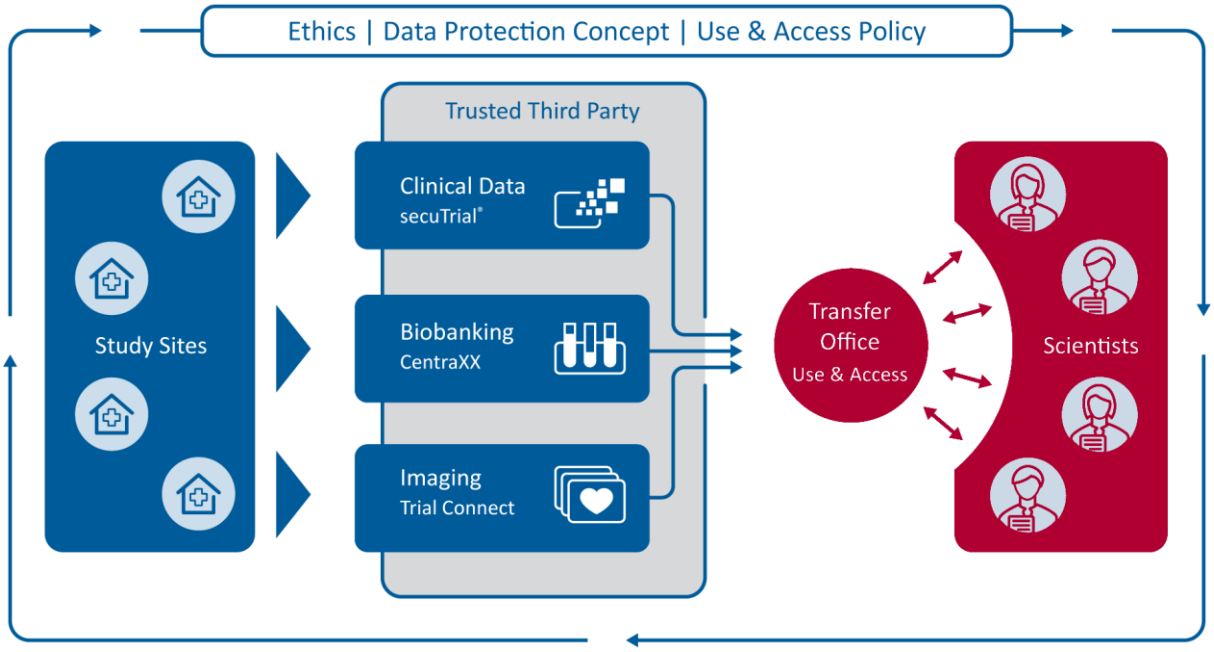


Abbildung 2 Aufbau und Aufgabenbereiche der einzelnen Partner innerhalb der Klinischen Forschungsplattform

Ethik-Projekt (EP)

Das Ethik-Projekt unterstützt DZHK-Studien bei der Umsetzung der in diesem Konzept dargestellten Prozesse in die Patientenunterlagen sowie bei Bedarf bei der Umsetzung in relevante Abschnitte von Prüfplänen/Studienprotokollen. Zusätzlich bietet das Projekt Hilfestellung an bei der Ergänzung weiterer Formulare und Unterlagen sowie bei Rückfragen bezüglich der wissenschaftlichen Infrastruktur des DZHK im Rahmen der Einreichung bei den jeweils zuständigen Ethikkommissionen.

Es ist Aufgabe des Ethik-Projektes, das „Ethik-Konzept des Bereichs Klinische Forschung des Deutschen Zentrums für Herz-Kreislauf-Forschung e.V. (DZHK)“, im Folgenden „Ethik-Konzept“ genannt, zu erstellen und in regelmäßigem Turnus zu aktualisieren.

Außerdem ist das Ethik-Projekt federführend verantwortlich für die Umsetzung der textbasierten Inhalte von Einwilligungserklärungen in Excel-basierte Abfragesysteme, auf deren Basis die Einwilligungsmodalitäten einzelner Teilnehmer:innen in der Treuhandstelle hinterlegt werden.

Die finale Prüfung der Inhalte von Einwilligungsunterlagen bezüglich vom DZHK verabschiedeter Prozesse und Grundsätze liegt in der Hand des Projektes. Das Verbundprojekt der Klinischen Forschungsplattform setzt ausschließlich die bereits vorab abgestimmten und harmonisierten Informed Consent-Dokumente um, die für die Studien und Projekte individuell angepasst und mit den zuständigen Ethikkommissionen abgestimmte wurden.

Treuhandstelle (THS)

Die Treuhandstelle übernimmt die Verwaltung und Speicherung der personenidentifizierenden Daten (IDAT) im Rahmen einer Funktionsübertragung. Die Datenübergabe an die THS wird durch die teilnehmenden DZHK-Studien mit den jeweils zuständigen Landesbeauftragten Personen für den

Datenschutz abgestimmt (vgl. Votum des LDSB MV vom 18. Dez. 2013[2]). Die Verarbeitung der Daten innerhalb der THS erfolgt ausnahmslos auf Basis einer informierten Einwilligung.

Für die Verwaltung der personenidentifizierenden Daten sind drei wesentliche technische Funktionalitäten notwendig: ein Identitätsmanagement, ein Einwilligungsmanagement sowie ein Pseudonymmanagement [3]. Die Treuhandstelle nimmt die IDAT entgegen und erzeugt eine dazu passende Menge von Pseudonymen, welche zusammen mit den medizinischen Daten bei der Datenhaltung verwendet und gespeichert werden (vgl. Abschnitt B1).

Datenhaltung (DH)

In Göttingen erfolgt die Datenhaltung für sämtliche im DZHK durchgeführten Studien und Register. Es wurde eine DZHK-Studiendatenbank aufgebaut, die durch das Institut für Medizinische Informatik betrieben wird. Im Rahmen der Studienplanung werden die Datenelemente seitens der Göttinger Data Manager in enger Abstimmung mit den Studienleitungen modelliert und umgesetzt. Die Abstimmung ist zum einen beratender Natur (d.h. es wird bei der einheitlichen und somit nachhaltigen Auswahl der zu dokumentierenden Items geholfen) und zum anderen praktischer, umsetzender Natur. Ausgebildete Dokumentar:innen sowie Dokumentar:innen mit einem zusätzlichen Masterstudium in Medizinischer Informatik stehen für diese Beratungs- und Umsetzungsleistung zur Verfügung.

In der DH wird weiterhin ein Metadaten-Verzeichnis geführt, welches zwei Aufgaben zur langfristigen Vergleichbarkeit der DZHK-Studien erfüllt: Zum einen ist es möglich, ein konkretes Item (z.B. „Blutdruck diastolisch“) in jeder durchgeführten Studie gleichermaßen zu erfassen (z.B. „sitzend nach fünf Minuten Ruhe“), zu speichern (zwei- bis dreistelliger Ganzzahlwert ohne nachgestellte Dezimalstelle) und innerhalb der Datenbank mit dem gleichen Namen zu versehen (z.B. bld_prsr_dia). Dies ermöglicht eine langfristige Vergleichbarkeit der durchgeführten DZHK-Studien. Zum anderen können innerhalb eines Metadaten-Verzeichnisses jedoch auch konkrete Informationen gespeichert werden, z.B. Informationen über die Umstände (Environmental Meta Data) einer Untersuchung. Gleiches gilt für andere Datentypen wie Bilder oder Informationen über gesammelte Biomaterialien.

Mit der Weiterentwicklung der Infrastruktur des DZHK werden neue Datentypen relevant. Dies können bspw. elektrophysiologische Daten, mobil (möglicherweise duch Studienteilnehmer:innen selbst) erfasste Follow-Up-Daten oder etwa die oben genannten Untersuchungs-Metadaten sein.

Labor-Informations-Management-System (LIMS)

Das vom Bereich Informationstechnologie (IT) der Universitätsmedizin Greifswald betriebene Labor-Informations-Management-System (LIMS) wird im Rahmen von Forschungsprojekten des DZHK zur Steuerung und Dokumentation der Gewinnung, Verarbeitung, Lagerung und Ausgabe von Bioproben (Bioproben-Management) von Studienteilnehmer:innen verwendet. Als technisches System wird für das LIMS die Software CentraXX der Kairos GmbH verwendet.

Das LIMS ist Teil der Forschungsinfrastruktur des DZHK. Durch automatisierte Schnittstellen erfolgt ein regelmäßiger Datenaustausch zwischen den angeschlossenen Systemen der THS und der DH.

Die THS übermittelt Pseudonyme an das LIMS direkt nach Anlegen von Studienteilnehmer:innen. Das LIMS ruft selbst dennoch keinerlei Einwilligungsinformationen von der THS ab. Langfristig soll die

[2] Kann bei der Unabhängigen Treuhandstelle der Universitätsmedizin Greifswald angefragt werden.

Zusammenführung von Studienteilnehmer:innen innerhalb der THS automatisch an das LIMS übermittelt und dort anschließend die Studienteilnehmerzusammenführung ebenfalls umgesetzt werden. Gleiches gilt für die möglichst automatisierte Verarbeitung von Widerrufen. Beide Vorgänge erfolgen derzeit papierbasiert.

Bilddatenmanagementsystem (BDMS)

Das Bilddatenmanagementsystem (BDMS) dient als integrierte Datenplattform für die a) klinischen Bilddaten (BDAT) und b) anderen DICOM-kompatiblen Daten im Rahmen der Studien des DZHKs. Es ermöglicht Interaktionen zwischen den Studienzentren, der Qualitätssicherung, den Auswerteeinheiten (CoreLabs) der Studien und der Transferstelle unter Beteiligung der Treuhandstelle und der Datenhaltung. Das BDMS basiert auf einer kundenspezifisch angepassten Software - TrialConnect – bereitgestellt von der Deutsche Telekom Healthcare and Security Solutions GmbH.

Für Studienzwecke werden THS-vermittelte Datenaustausche mit der DH durchgeführt, ohne dass klinische Daten über die THS übertragen werden. Das BDMS interagiert mit der THS durch die Abfrage von Pseudonymen und einer regelmäßigen Abfrage des Einwilligungsstatus. Umgesetzte Widerrufe in der THS führen somit automatisch zu Zugriffssperren, die feingranular über die THS gesteuert werden können. (Die Zusammenführung von Studienteilnehmer:innen innerhalb der THS wird automatisch an das BDMS übermittelt und dort wird anschließend die Studienteilnehmerzusammenführung ebenfalls umgesetzt. Gleiches gilt für die möglichst automatisierte Verarbeitung von Widerrufen.

Datenaustausch und Schnittstellen

Einige der Anwendungsfälle erfordern einen Datenaustausch zwischen den beteiligten Infrastrukturpartnern bzw. zwischen den einzelnen Partnern und den Studien. Dieser kann z.B. auf elektronischem Weg oder mittels Papierdokumenten automatisiert oder manuell erfolgen. Nicht nur durch die örtliche Trennung der Daten, sondern auch durch die technologisch unterschiedlichen Systeme sind sowohl im Hinblick auf elektronischen Austausch wie auch für (teil-) manuelle Arbeitsabläufe gemeinsame Schnittstellen und Verfahren definiert, die den datenschutzrechtlichen Anforderungen entsprechen. Die folgenden Kapitel erläutern Annahmen, Bedingungen und Anwendungsfälle der einzelnen Infrastrukturpartner untereinander als auch im Zusammenspiel mit Studien, identifizieren Schnittstellen und definieren diese somit näher.

2 Datenverarbeitung im DZHK

EU-Datenschutzgrundverordnung und weitere Regularien

Die Rechtsgrundlage zur Verarbeitung der die Studienteilnehmer:innen betreffenden personenbezogenen Daten bildet primär deren freiwillige schriftliche Einwilligung nach Art. 6(1)a DS-GVO. Da es sich im Fall der Gesundheitsforschung um besondere Kategorien personenbezogener Daten handelt, gilt in diesem Fall die Legitimation der Verarbeitung personenbezogener Daten nach ausdrücklicher Einwilligung wie dargelegt in Art. 9(2)a DS-GVO.

Da es sich bei der Daten- und Biomaterialsammlung des DZHK um wissenschaftliche Forschung in öffentlichem Interesse handelt, dürfen Daten und Biomaterialien für unbestimmte Zeit gespeichert/gelagert (Art. 5e DS-GVO) („Speicherbegrenzung“) und für die wissenschaftliche Gesundheitsforschung für verschiedene Zwecke (Art. 5b DS-GVO) („Zweckbindung“) genutzt werden. Auf diesen Umstand wird ein:e Studienteilnehmer:in in einer ausführlichen Patienteninformation hingewiesen.

Um dem Schutz der Rechte und Freiheiten betroffener Studienteilnehmer:innen gerecht zu werden, wird das wie in der einschlägigen Literatur zum Thema beschriebene Konzept [TMF generisches Datenschutzkonzept] der informationellen Gewaltenteilung genutzt. Die Daten werden somit in einer Form gespeichert, die eine größtmögliche Sicherheit gewährleistet. Die Umsetzung erfolgt wie in diesem Konzept beschrieben. Dies wird gefordert als Grundlage, um die in der DS-GVO vorgesehenen Freiheiten der wissenschaftlichen Forschung nutzen zu dürfen Art. 89(1) DS-GVO [2, 3, 4], BDSG §27(3) [2].

Nach einer Aufbewahrungsfrist von 10/15 Jahren nach Ende der Klinischen Studie werden abschließend sämtliche gespeicherte personenbezogene Datensätze der Studienteilnehmer:innen bezüglich dem Vorliegen folgender Policies geprüft: Vorliegen der Einwilligung zur Speicherung und Verarbeitung der Daten und Vorliegen der Einwilligung zur unbefristeten Nutzung und Weitergabe der Daten. Ist letztere nicht vorhanden, werden sämtliche personenbezogene Daten der Studienteilnehmer:innen gelöscht. Bei Vorhandensein einer Einwilligung zur unbefristeten Nutzung der Daten wird überprüft, ob die individuellen personenbezogenen Daten in einer potentiell zukünftig nutzbaren Form vorliegen. Ist das nicht der Fall, werden sie gelöscht.

Bei Widerruf der Studienteilnahme werden noch vorhandene Biomaterialien auf Nachfrage grundsätzlich vernichtet, da von einer Anonymisierbarkeit nicht ausgegangen werden kann. Personenbezogene Daten werden technisch anonymisiert (siehe Kapitel C1 dieses Konzeptes), sofern nicht spezialrechtliche Regelungen dagegenstehen (bspw. Arzneimittelgesetz, Strahlenschutzverordnung) oder die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt Art. 17(3)d DS-GVO. Eine Löschung personenbezogener Daten wird nicht unmittelbar durchgeführt, Rechtsgrundlage dafür ist - neben der Einwilligung zur Verarbeitung der Daten wie Art. 6 (1) a DS-GVO und Art. 9 (2) a DS-GVO darlegen - die Verarbeitung aus Gründen wissenschaftlicher Forschung nach Art. 89 (1) DS-GVO. Daten ohne Personenbezug, z. B. aggregierte Daten, stehen nach Widerruf der Einwilligung nur noch für die Studienauswertung und zu Zwecken der Qualitätssicherung zur Verfügung.

Eine Weiternutzung von anonymisierten Daten für weitere Forschungszwecke sieht die Nutzungsordnung des DZHK zu diesem Zeitpunkt nicht vor (NO §3(2)). Dem:der Studienteilnehmer:in

wird außerdem in eingeschränktem Maße (nicht im Falle widersprechender spezialrechtlicher Regelungen, Studienauswertung, Qualitätssicherung) das Recht eingeräumt, eine Löschung seiner:ihrer personenbezogenen Daten jederzeit zu verlangen (Art. 17(1)b DS-GVO). Diese wird durchgeführt, sobald die Daten für oben genannte Zwecke nicht mehr notwendig sind und die Verwirklichung der Ziele der Forschung nicht unmöglich gemacht oder ernsthaft beeinträchtigt werden (Art. 17(3)d DS-GVO).

Dem:der Studienteilnehmer:in wird das Recht auf Auskunft über die ihn:sie betreffenden personenbezogenen Daten, sowie auf die Aushändigung einer kostenfreien Kopie gewährt, sofern es nicht einen unverhältnismäßigen Aufwand erfordert (BDSG §27(2)). In der Regel gehen wir von der Durchführbarkeit einer Auskunftserteilung aus (siehe Kapitel C3.5 dieses Konzeptes). Auch unrichtige personenbezogene Daten können von Studienteilnehmer:innen jederzeit berichtigt werden.

Gemäß Art. 30 DS-GVO wurden für die Verarbeitung der personenbezogenen Daten Verzeichnisse über die Verarbeitungstätigkeiten[3] erstellt.

Die zur Umsetzung der rechtlichen Rahmenbedingungen notwendigen technischen, personellen, räumlichen und organisatorischen Maßnahmen werden in dem vorliegenden Datenschutzkonzept festgehalten.

Tabelle 1: Übersicht der datenschutzrechtlich zugrundeliegenden Regularien für die Einrichtungen der Infrastruktur

Einrichtung	DS-GVO[4]	Bundesdaten-schutzgesetz (BDSG-Neu)[5]	Landesdaten-schutzgesetz MV (DSG M-V)[6]	Landesdaten-schutzgesetz Niedersachsen (NDSG)[7]	Berliner Datenschutzgesetz (BlnDSG)[8]
THS	x	x	x		
DH	x	x		x	
LIMS	x	x	x		
BDMS	x	x			x

[3] Diese können bei Bedarf bei den zuständigen Partnern der Klinischen Forschungsplattform angefragt werden.

[4] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union L 119/1, mit Wirkung zum 25.05.2018.

[5] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), mit Wirkung zum 25.05.2018.

[6] Datenschutzgesetz für das Land Mecklenburg-Vorpommern (Landesdatenschutzgesetz - DSG M-V) vom 22. Mai 2018, GVOBl. M-V S. 193, 194, mit Wirkung zum 25.05.2018.

[7] Niedersächsisches Datenschutzkonzept vom 16.05.2018 (NDSG), Nds. GVBl. 2018, 66, mit Wirkung zum 25.05.2018

[8] Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz –BlnDSG) vom 13.06.2018, GvBl. 2018, 418, mit Wirkung vom 24.06.2018

Die Verarbeitung personenbezogener Daten erfolgt innerhalb der Infrastruktur des DZHK außerdem nach der in Tabelle 1 dargestellten Bundes- und Landesrechtlichen Vorgaben.

Neben den der Datenschutzgesetzgebung haben folgende weitere Gesetze und Richtlinien Einfluss auf dieses Datenschutzkonzept:

- EU-Medizinprodukte-Verordnung (MDR)
- Arzneimittelgesetz (AMG)
- Medizinproduktegesetz (MPG)
- Good Clinical Practice (GCP-V)

Umsetzung von Betroffenrechten

In jedem Fall haben die Studienteilnehmer:innne der DZHK-Studien die Möglichkeit, sich an alle Einrichtungen des DZHK zu wenden, um die Betroffenrechte nach DS-GVO (bspw. Löschung von Daten oder Widerruf) umsetzen zu lassen. In der Regel wenden sich die Studienteilnehmer:innen direkt an die Studienzentren, die für DZHK-Studien rekrutieren. Die Studienzentren sind dazu aufgefordert, diese Anliegen an die Infrastruktur weiterzuleiten. In den meisten Fällen wird hierbei als erstes die Treuhandstelle kontaktiert, da Sie die nachgelagerten Vorgänge (bspw. Probenvernichtung, Beauftragung zur Datenlöschung) mit den anderen Infrastrukturpartnern orchestriert.

Die Teilnehmer:innen können sich darüber hinaus auch direkt bei den Infrastrukturpartnern oder der Gst. des DZHK melden. DH, LIMS, BDMS und Gst. sind dann ebenso verpflichtet, die Anliegen der Teilnehmer:innen an die THS zur weiteren Bearbeitung weiterzuleiten, wie die Studienzentren.

Die Treuhandstelle wird die Anfragen ggf. in Rücksprache mit der meldenden Einrichtung oder direkt mit dem:der Studienteilnehmer:in vorbereiten und weitere Prozesschritte (wie z.B. Datenlöschung, Aktualisierung von Daten) veranlassen. Eine abschließende Bestätigung über die durchgefühten und abgeschlossenen Prozesse wird entweder direkt oder über ein Studienzentrum an den:die Studienteilnehmer:in übermittelt. Die genauen Abläufe zur Umsetzung der Betroffenenrechte lassen sich den nachfolgenden Kapiteln sowie den jeweiligen SOPs der einzelnen Einrichtungen entnehmen.

2.1 Risikobeurteilung

Für den wissenschaftlichen Erfolg des DZHK sind die Gewährleistung der Integrität, der Authentizität, der Vertraulichkeit und der Verfügbarkeit der erhobenen und verarbeiteten Daten sowie der Daten-verarbeitenden Verfahren notwendige Voraussetzung. Zu den dafür wesentlichen Aufgaben der Infrastruktur zählen:

- Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO
- Gewährleistung der Sicherheit personenbezogener Daten gemäß Abschnitt 2 DS-GVO (Art. 32-34)

In der Klinischen Forschungsplattform des DZHK werden neben den allgemeinen Schutzzielen und Rahmenbedingungen gemäß DS-GVO (Art. 35 Abs. 7 lit. c) stets die Risiken für die „Rechte und Freiheiten" der Betroffenen (Studienteilnehmer:innen) berücksichtigt. Die Notwendigkeit einer DSFA ist gegeben, da in den Studien des DZHK personenbezogene Daten verarbeitet werden, bei denen voraussichtlich zwei der neun Kriterien erfüllt werden, die nach Einschätzung der Datenschutzgruppe nach Artikel 29 für eine Verarbeitung mit einem („wahrscheinlich") hohen Risiko sprechen[9] .

Eindämmung der Risiken durch geeignete Abhilfemaßnahmen

Im Rahmen der Etablierung der Klinischen Forschungsplattform für das DZHK wurden bereits vor Inkrafttreten der DS-GVO ausführliche Schutzbedarfsanalysen und Risikobewertungen gemäß BSI Standard 100-2 durchgeführt und entsprechende technische und organisatorische Maßnahmen (TOM) zur Risikominimierung vorgenommen. Diese TOMs sind in den nachfolgenden Kapiteln der einzelnen Partner beschrieben und senken die Eintrittswahrscheinlichkeit von Schäden für die Teilnehmer:innen an Forschungsprojekten des DZHK. Die umgesetzten TOMs gewährleisten einen nach den vorhandenen Möglichkeiten bestmöglich und ausreichend wirksamen Schutz der personenbezogenen Daten, die in der Klinischen Forschungsplattform des DZHK verarbeitet werden.

Bestimmung des Restrisikos

Auf Basis der bereits etablierten TOMs stellt die nachfolgende Tabelle zur Bewertung des verbleibendes Restrisikos potentielle Schäden dar, verweist auf die mögliche Schwere des Schadens (gemäß Einordnung ErwGr75[10] in *geringfügig, überschaubar, substanziell und groß*), führt mögliche, den Schaden auslösende Ereignisse auf, nennt Risikoquellen und nimmt eine Schätzung der potentiellen Eintrittswahrscheinlichkeit des Schadens nach Umsetzung der TOM gemäß den von der Datenschutzkonferenz empfohlenen Kategorien[11] vor (*geringfügig, überschaubar, substanziell, groß*). Abschließend erfolgt eine Rest-Risikoabstufung gemäß Empfehlung der Datenschutzkonferenz (geringes Risiko, Risiko und hohes Risiko). Durch die hohen datenschutztechnischen Vorkehrungen ist der unbefugte Zugriff auf die Daten der Klinischen Forschungsplattform des DZHK mit vertretbarem Aufwand praktisch nicht durchführbar. Insbesondere die strikte Trennung der Datenbestände nach dem TMF Datenschutz-Leitfaden [4], schützt die Daten vor Angreifern von außen. Das Restrisiko für den Einzelnen wird damit auf ein Mindestmaß reduziert.

[9] Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", Datenschutzgruppe nach Artikel 29, Stand 4. 10.2017, https://www.datenschutz-bayern.de/technik/orient/wp248.pdf

[10] Erwägungsgrund 75: Risiken für die Rechte und Freiheiten natürlicher Personen, https://dsgvo-gesetz.de/erwaegungsgruende/nr-75/

[11] Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapiere der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) 26.04.2018, https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf

Tabelle 2 Rest-Risikobeurteilung nach Umsetzung der in den weiteren Kapitel beschriebenen Maßnahmen; einschließlich Risikoidentifikation, Abschätzung der Eintrittswahrscheinlichkeit und Schwere möglicher Schäden, sowie Abstufung des Rest-Risikos gemäß Empfehlungen der Kurzpapiere der Datenschutzkonferenz (Stand April 2019) und unter Berücksichtigung der Schutzziele nach BSI-Standard 100-2

Nr.	Schaden	Schwere des Schadens	Bedrohtes Schutzziel nach BSI 100-2	Auslösende(s) Ereignis(se)	Risikoquelle(n)	Verbleibende Eintritts-wahrschein-lichkeit	Abstufung Restrisiko
1	Datenzugang durch unbefugte Personen auf Servern	substanziell	Vertraulichkeit	Unbefugter Zugang zu Daten: Angriff auf Web-Server durch Hacker mit dem Ziel des Datendiebstahls	Äußere Einflüsse: Unbefugte Angreifer, Cyberkriminelle	geringfügig	Geringes Risiko
2	Datenzugang durch unbefugte Personen auf Netzwerk und Übergangspunkte	groß	Vertraulichkeit	Unbefugter Zugang zu Daten: Unberechtigte oder unbeabsichtigte Aufzeichnung der Daten-kommunikation	Äußere Einflüsse: Unbefugte Angreifer, Cyberkriminelle	geringfügig	Geringes Risiko
3	Datenzugang durch unbefugte Personen auf Notebooks und PCs	groß	Vertraulichkeit, Integrität	Unberechtigter Zugriff durch Administratoren über Remote Desktop oder administrative Freigaben	Menschliches Versagen bzw. gezielter unberechtigter Zugriff durch Mitarbeiter	geringfügig	Geringes Risiko
4	Unbefugte Offenlegung von Daten durch Mitarbeiter	groß	Vertraulichkeit, Integrität	Unbewußter oder vorsätzlicher Verstoß durch Mitarbeiter gegen Anweisungen zum Umgang mit personenbezogenen Daten: Unberechtigter Zugriff auf Storage-Systeme durch Personen mit administrativen Zugang zu den Systemen (Server, Softwaresysteme auf den Servern, physikalische Server, Storage und Backup-Systeme)	Menschliches Versagen bzw. gezielter unberechtigter Zugriff durch Mitarbeiter	geringfügig	Geringes Risiko
5	Unbefugte Offenlegung von Daten durch Dritte	groß	Vertraulichkeit	Unberechtigter Zugriff auf physikalische Datenträger des Storage Systems (Wartung, Garantiefall) und /	Menschliches Versagen	geringfügig	Geringes Risiko

				oder unbefugter Zugriff auf Daten durch Dritte bei Verlassen des Arbeitsplatzes			
6	Zufällige Vernichtung von Daten des Storage Systems	substanziell	Integrität	Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten: Datenverlust durch Defekt des Storagesystems	Technische Fehlfunktion	geringfügig	Geringes Risiko
7	Unbeabsichtigte / unbefugte Veränderung der Daten	groß	Integrität	Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten: Verlust der Revisions-sicherheit durch unbeabsichtigtes Löschen von Daten und Log-Dateien	Menschliches Versagen	geringfügig	Geringes Risiko
8	Zufällige Vernichtung von Daten durch Schadsoftware über Internet, Mail, mobile Datenträger auf Notebooks und PCs	groß	Vertraulichkeit, Integrität	Unbewußter oder vorsätzlicher Verstoß durch Mitarbeiter gegen Anweisungen zum Umgang mit Arbeitsplatz-PCs, mobilen Datenträgern	Menschliches Versagen	geringfügig	Geringes Risiko
9	Gesamtausfall der Systeme und vollständiger Verlust der vorgesehenen datenver-arbeitenden Prozesse	substanziell	Integrität, Verfügbarkeit	Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten	Höhere Gewalt (Ele-mentarschäden)	geringfügig	Geringes Risiko
10	Ausfall der Softwaresysteme (Basissoftware und Anwendungen)	substanziell	Integrität, Verfügbarkeit	Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten	Technische Fehlfunk-tionen (Fehlerhafte Updates, Software-fehler)	geringfügig	Geringes Risiko
11	Ausfall von Web-Servern	groß	Verfügbarkeit	Einschränkungen vorgesehener datenverarbeitender Prozesse durch gezielte Schädigung von Systemen (Denial of Service Attacken)	Äußere Einflüsse: Unbefugte Angreifer, Cyberkriminelle	geringfügig	Geringes Risiko

12	Nichterfüllung eines Löschanspruchs	groß	Vertraulichkeit	Verarbeitung von Daten über die Speicherfrist hinaus und/oder unrechtmäßige Verarbeitung	Menschliches Versagen (Unbeabsichtigtes Anlegen von Datenkopien oder unsicheres Löschen)	geringfügig	Geringes Risiko

B Ethik-Projekt

1 Allgemeine Prozesse

1.1 Aufbau der Dokumente zur Informierten Einwilligung

Dem Ethik-Konzept des DZHK sind Musterunterlagen für Patienteninformation und Einwilligung angegliedert. Der strukturelle Aufbau orientiert sich an der spezialrechtlichen Einordnung der Studie nach AMG, MPG oder als sonstige Studie.

Das DZHK nutzt die Musterpatientenunterlagen des Arbeitskreises medizinischer Ethikkommissionen, welche um spezifische Punkte des Datenmanagement sowie der Nachnutzung von medizinischen Daten und gegebenenfalls Biomaterialien ergänzt werden.

Folgende Möglichkeiten des Aufbaus der Einwilligungsunterlagen, bezogen auf nachstehende aggregierte Einwilligungselemente, sind derzeit gegeben:

1. Studienteilnahme: Teilnahme an einer Klinischen Studie/klinischen Prüfung unter den in der studienspezifischen Patienteninformation dargestellten klinischen Bedingungen (medizinische Eingriffe, Medikation, ggf. Randomisierung/ Einteilung in Gruppen, Nebenwirkungen, …).
2. Datenmanagement: Datenerhebung, -speicherung sowie -verarbeitung für Qualitätsmanagement und Controlling sowie die Auswertung von Medizinischen Daten (MDAT, BDAT) für die vordefinierte(n) Studienfragestellung(en).
3. Datenweitergabe: Weitergabe von medizinischen Daten (MDAT, BDAT) für Forschungsvorhaben laut Nutzungsordnung §1(5) unter den Use and Access Bedingungen des DZHK (siehe auch dieses Dokument Teil D2.4).

   Optional angeboten wird die pseudonymisierte Weitergabe der Biomaterialien in Länder außerhalb der EU in den Fällen, in denen kein Angemessenheitsbeschluss der Europäischen Kommission oder ein vergleichbares Verfahren vorliegt.
4. Studienbezogene Biomaterialnutzung: Biomaterialentnahme, -lagerung und -verarbeitung von Studienbiomaterialien sowie Analyse dieser für die vordefinierte(n) Studienfragestellung(en).
5. Biomaterialweitergabe: Weiternutzung übrig gebliebener Studienbiomaterialien (NO §4(5)Satz 4) sowie Entnahme, Lagerung und Verarbeitung von Basisbiomaterialien (NO §4(7)) und Analyse dieser für Forschungsvorhaben unter den Use and Access Bedingungen des DZHK (siehe auch dieses Dokument Teil D2.4).

Die genannten Einwilligungselemente werden studienspezifisch angepasst, die Inhalte der Punkte 1. bis 4. jedoch dem:der Studienteilnehmer:in in der Regel in einem IC-Dokument zur Verfügung gestellt. Punkt 5. wird stets in einem eigenen Dokument zur Verfügung gestellt oder ist optional durch den:die Studienteilnehmer:in auszuwählen. Tiefergehende Details zur Einwilligungserklärung sind den Anlagen des Ethik-Konzeptes zu entnehmen.

1.2 Umsetzung der Inhalte der Informierten Einwilligung in eine Abfragematrix

Die Inhalte der Informierten Einwilligungserklärung (IC) werden in eine Excel-basierte Abfragematrix überführt. Jede Studie wird in einer eigenen Modultabelle dargestellt, Angaben wie der Originaltitel der Studie, die Versionsnummer und der Dateiname des gültigen Studien-IC sind obligat.

Da die Einwilligungserklärung modular aufgebaut ist, finden sich auch in der Abfragematrix entsprechende Module (z.B. StudieXY_Datenschutzerklärung). Diese können z.T. optional eingewilligt werden, was ebenfalls erfasst wird. Der Text der Einwilligungserklärung wird an der entsprechenden Stelle eingefügt.

Jedem inhaltlichen Modul werden definierte Policies zugeordnet. Ein Modul kann mehrere Policies umfassen, pro Studie kann jede Policy einmal oder keinmal zugeordnet werden.

Durch Policies werden Handlungsanweisungen (Events) definiert, die im Falle eines Daten- oder Biomaterialtransfers standardisiert abgefragt werden können.

Das zur Durchführung eines Events jeweils zuständige Teilprojekt bestimmt in Zusammenarbeit mit dem EP die Zuordnung von Policies zum Event. Die genaue Bedeutung der Policies wird vom EP vorgeschlagen und von den Teilprojekten gemeinsam bestimmt. Das EP verantwortet die initiale Zuordnung von Policies zu den Modulen eines Studienconsent. Unklare Fälle und Ergänzungen des Abfragesystems werden in enger Zusammenarbeit mit den betroffenen Teilprojekten diskutiert und abgestimmt.

C Unabhängige Treuhandstelle

1 Allgemeine Prozesse

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 [4].

Zu den typischen Aufgaben der unabhängigen Treuhandstelle zählen:

- die Zuordnung von personenidentifizierenden Daten und entsprechenden Kennungen für Quell- und Sekundärsysteme
- die Verwaltung von personenbezogenen Einwilligungen, Ermächtigungen und Widerrufen
- die Pseudonymisierung bzw. De-Pseudonymisierung von Daten
- Durchführung von Registerabrufen
- Sekundärdatenabgleich und -zusammenführung
- Mitwirkung bei der Durchführung von Follow-Ups (z. B. Vitalstatus)
- Mitwirkung bei Re-Kontaktierung sowie Mitteilung von Zufallsbefunden
- Umsetzung von Widerrufen bzw. deren prozessualen Folgen
- Mitwirkung beim Transferstellen-Prozess zur Daten- und Materialübergabe
- Auskunft an Betroffene über gespeicherte Daten und deren Verwendung

Intern werden die Prozesse der Treuhandstelle projektspezifisch durch festgelegte einheitliche Standard Operating Procedures (SOPs) abgesichert. Nachfolgend werden zentrale Verantwortlichkeiten der Treuhandstelle, die zur erfolgreichen Erfüllung der übertragenden Funktionen wesentlich sind, näher betrachtet.

1.1 Eindeutige Identifizierung von Teilnehmer:innen

Um Teilnehmer:innen von Studien auch bei unvollständigen oder fehlerbehafteten Identitätsdaten (IDAT) standortübergreifend und gleichzeitig eindeutig identifizieren zu können, werden in der THS eingehende IDAT im Rahmen eines Record Linkage mit vorhandenen Daten abgeglichen und ihnen eine eindeutige Kennung nach dem Konzept des Master Person Index (MPI ID oder auch Teilnehmer ID) zugeordnet. Details zum Matching-Prozess und verwendeten Werkzeugen können in Kapitel 3.6.1 des Datenschutzkonzeptes der THS der Universitätsmedizin Greifswald [2] nachgelesen werden.

1.2 Pseudonymisierung

Nach eindeutiger Identifizierung der:des Studienteilnehmer:in auf Basis der an die THS übermittelten IDAT, wird dem:der Studienteilnehmer:in für die THS-interne Verarbeitung eine eindeutige Teilnehmer-ID zugewiesen.

Für die weitere Verarbeitung werden durch die THS geeignete Pseudonyme (PSN) mit Hilfe des Pseudonymisierungsdienstes gPAS® (nähere Informationen dazu siehe https://www.ths-greifswald.de/forscher/gpas/) generiert und zugeordnet. Eine nachträgliche Auflösung von Pseudonymen zu IDAT ohne Einsatz der Treuhandstelle ist nicht möglich. Wie in nachstehender Abbildung dargestellt, werden im DZHK je Datenquelle (z. B. LIMS oder BDMS) und Datenherausgabevorgang (dargestellt als Transfer-PSN) unterschiedliche Pseudonyme generiert (vgl. Abbildung 3)[12].

Jede:r Teilnehmer:in wird bei der Studienrekrutierung als erstes bei der Treuhandstelle mit seinen:ihren IDAT initial angelegt. Dabei erhält jede:r Studienteilnehmer:in eine eineindeutige Teilnehmer-ID – den sogenannten Master Patient Index Identifier (MPI ID). Teilnehmer:innen erhalten zusätzlich für jede Studie, an der sie teilnehmen, jeweils eine Study-ID. Damit kann selbst bei Austausch der Pseudonyme zwischen Studien kein Rückschluss auf einzelne Teilnehmer:innen erfolgen. Die Treuhandstelle stellt anschließend diese Pseudonyme den weiteren Daten-erfassenden Systemen (z. B. LIMS, BDMS) zur Erhebung der medizinischen Daten zur Verfügung.

Vorteil dieses Vorgehens ist, dass auf diese Weise die Erfassung der medizinischen Daten mittels secuTrial® bereits in pseudonymisierter Form erfolgen kann und zu keinem Zeitpunkt medizinische Daten innerhalb der Treuhandstelle verarbeitet werden oder identifizierende Daten in der Datenhaltung vorhanden sind. Mit Stand vom 17. Jan. 2018 werden in der THS des DZHK in Summe 15.273 Pseudonyme verwaltet.

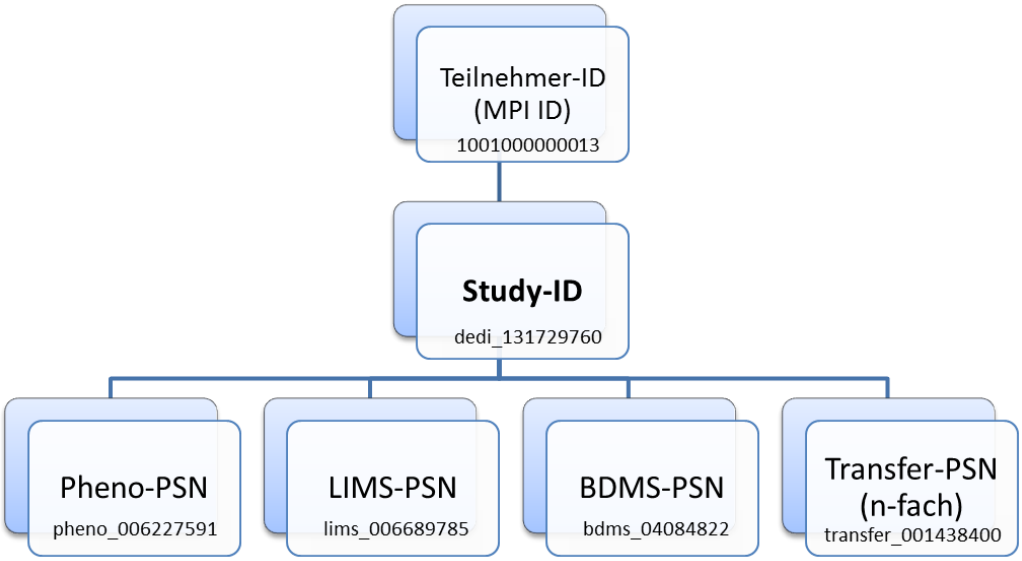


Abbildung 3 Hierarchie der durch die THS bereitgestellten Pseudonyme

Weitere Details zum Pseudonymisierungsprozess und verwendeten Werkzeugen sind dem Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2] Abschnitt 3.6.2 zu entnehmen.

[12] Zum Zeitpunkt der Dokumenterstellung ist die nötige Abstimmung zum Einsatz unterschiedlicher (N-fach) Pseudonyme je Datenherausgab bzw. zur Verwendung eines einheitlichen Datenherausgabepseudonyms je Studienteilnehmer noch nicht abgeschlossen.

1.3 Einwilligung und Widerruf

Sofern nicht anderweitig gesetzlich geregelt, setzt die Verarbeitung personenidentifizierender Daten (PII oder auch IDAT) und medizinischer Daten zu Forschungszwecken gemäß Art. 6, 9 DS-GVO die *freiwillige und informierte* Einwilligung der betroffenen Person (Studienteilnehmer:in) voraus. Diese Einwilligung hat unmissverständlich und ausdrücklich durch eine eindeutige bestätigende Handlung (z. B. Anklicken einer Auswahl-Box oder Unterschrift auf Papier) zu erfolgen.

Potentielle Studienteilnehmer:innen werden vor Ort in den Studienzentren durch Ärzt:innen über Umfang und Folgen ihrer Einwilligung sowie Möglichkeiten des Widerrufs aufgeklärt. Das Vorgehen stellt sicher, dass die Studienteilnehmer:innen die einzelnen Punkte der Patienteninformation und des jeweiligen ICs verstanden haben und sich über deren Auswirkungen im Klaren sind. Der:die Studienteilnehmer:in hat jederzeit die Möglichkeit, Fragen zu stellen. Diese werden durch den:die aufklärende:n Arzt:Ärztin beantwortet.

Die inhaltliche Erstellung einer Einwilligung ist Teil des jeweiligen projektspezifischen Ethikkonzeptes. Die Inhalte werden in einem Abstimmungsprozess mit dem Ethik-Projekt des DZHK und der/den zuständigen Ethik-Kommission(en) harmonisiert und durch ein Ethik-Votum bestätigt oder unter Auflagen korrigiert.

Das verwendete Einwilligungsdokument ist modular aufgebaut. Auf diese Weise hat der:die Teilnehmer:in die Möglichkeit zu ausgewählten Abschnitten (und entsprechenden Datenverarbeitungsschritten) seine:ihre Einwilligung zu geben. Die Einwilligungserklärung regelt weiterhin die Dauer der Datenspeicherung, sowie die Aufbewahrung der Biomaterialien. Je nach gesetzlicher Vorgabe können die Angaben zwischen den einzelnen DZHK-Studien voneinander abweichen. Die Speicherfristen sind somit den jeweiligen Dokumenten der DZHK-Studien zu entnehmen.

Die studienspezifischen modularen Inhalte werden in Zusammenarbeit mit dem Ethikprojekt definiert und verwaltet.

Im DZHK werden Einwilligungen derzeit studien-spezifisch, zweckbezogen, papier-basiert und in Schriftform eingeholt.

Der:die Studienteilnehmer:in willigt aktiv in die Studie ein und bestätigt rechtswirksam, in der Regel durch Unterschrift, dass er:sie der Erfassung, Verarbeitung und Speicherung seiner:ihrer Daten im beschriebenen Umfang zustimmt, und ermächtigt die Verantwortlichen im Rahmen des DZHK, seine:ihre Daten zu Forschungszwecken zu erheben. Die Einwilligung zur Entnahme und Verwaltung von Bioproben erfolgt aus organisatorischen Gründen in der Regel separat.

Gemäß Art. 7 Abs. 3 DS-GVO haben Betroffene die Möglichkeit ihre Einwilligung vollständig oder in Teilen ohne Angabe von Gründen zu jedem Zeitpunkt zu widerrufen, wobei der Widerruf der Einwilligung so einfach sein muss, wie die Erteilung. In der Regel werden Widerrufe durch das meldende Studienzentrum an die Treuhandstelle in schriftlicher Form übergeben. Das Studienzentrum ist für die Weiterleitung eines eingegangenen Widerrufes zuständig, der Treuhänder ist für Durchsetzung und Dokumentation des Widerrufes verantwortlich (vgl. Anlagen: DZHK-*SOP*-P-*0*5 *Widerruf, Studienausschluss, Kontaktsperre*sowie *SOP THS_12 Umgang mit Widerruf intern*).

Die THS verwaltet Einwilligungen und Widerrufe (vgl. Datenschutzkonzept der THS UMG, Abschnitt 3.6.3 *[2]*). Um der Rechenschaftspflicht nach Art. 5 Abs. 2 und Art 7 Abs. 1 DS-GVO zu genügen, wird die Informierte Einwilligung (IC) des:der Teilnehmer:in schriftlich eingeholt, elektronisch in der THS

angelegt und als Scan der Papier-Einwilligung in der THS archiviert. Weiterhin können im Bereich internationaler Studien Sonderlösungen erarbeitet werden, sofern die nationale Gesetzgebung von den hier beschriebenen Verfahren abweicht. Nähere Informationen können zu den DZHK-Studien bei der Klinischen Forschungsplattform eingeholt werden.

Im Rahmen der Qualitätssicherung und der Prüfung der Gültigkeit des Studienteilnehmerwillens werden die elektronisch erfassten ICs gegen die Scans der Papier-ICs auf Vollständigkeit und Korrektheit geprüft. Statistisch gesehen, haben an die THS übermittelte Einwilligungen eine inhaltliche Fehlerquote von ca. 40% (z. B. falsch oder undeutlich angekreuzt, Stand: 2017). Diese Einwilligungen „mit Handlungsbedarf", aber auch Einwilligungen „ohne Handlungsbedarf" (rund 10 %) werden THS-intern dokumentiert. Auf diese Weise können automatisch Qualitätssicherungsberichte generiert und an die Mitarbeiter:innen in den Studienzentren zurückgemeldet werden. Deren Aufgabe ist es im Anschluss, erkannte Fehler zu bereinigen und im Zweifelsfall den:die Studienteilnehmer:in zu kontaktieren. Im Zweifel können bis zur Klärung des Vorgangs Datensätze für die weitere Bearbeitung gesperrt werden.

1.4 Mitwirkung im „Use & Access"-Prozess

Die Bereitstellung von Daten im Rahmen eines Use&Access-Prozesses wird an der Universitätsmedizin Göttingen durch eine eigens eingerichtete Transferstelle realisiert. Dieser Prozess erfordert die Mitwirkung der Unabhängigen Treuhandstelle, da die Daten aus den unterschiedlichen Fachsystemen zusammengeführt verarbeitet werden müssen (Record Linkage). Hierzu wird vor der Zuordnung der nach Fachsystemen getrennten Pseudonyme durch die THS das Bestehen der Einwilligung auf Basis des Anlasses der Zusammenführung geprüft.

Forschende stellen Daten- und Materialanfragen an die Transferstelle. Diese prüft die Anfrage auf Korrektheit gemäß der Nutzungsordnung des DZHK und leitet ein Antragsverfahren ein. Die Transferstelle ermittelt anhand der angegebenen Parameter den notwendigen Daten- bzw. Materialbestand und gibt diese Informationen an das Use&Access Committee zur Begutachtung. Nach erfolgter Bewilligung wird ein Material Transfer Agreement zwischen dem DZHK und der Institution des Antragstellers geschlossen. Bevor die Übergabe durch die Transferstelle erfolgt, prüft die Treuhandstelle auf Widerrufe. Anschließend werden die DZHK-Pseudonyme der Daten bzw. des Materials entfernt und die Daten mittels Export-spezifischer Zufallszahlen erneut pseudonymisiert. Dieser Schritt ist notwendig, um im Falle eines möglichen relevanten Zufallsbefundes die Zuordnung zur Person wiederherstellen zu können[13].

1.5 Weitere Aufgaben

Neben der Möglichkeit des Widerspruchs bzw. Widerrufs werden die weiteren Betroffenenrechte ebenfalls von der THS gewahrt. So werden beispielsweise Auskunftsersuche nach Art. 15 DS-GVO einzeln und in angemessenem zeitlichen Rahmen bearbeitet. Auch können Studienteilnehmer:innen ihre Daten direkt bei der Treuhandstelle berichtigen lassen. Erforderliche Kontaktinformationen werden den betroffenen Personen in Patienteninformation und Einwilligung zur Verfügung gestellt.

[13] Ein Fließschema zum Antragsprozess befindet sich unter : https://dzhk.de/forschung/klinische-forschung/nutzung-von-daten-und-biomaterialien-use-and-access/

Bislang wurden hierzu noch keine spezifischen Prozesse ausgearbeitet. Dies erfolgt erst mit auftretenden Anfragen und wird beispielhaft an ausgearbeiteten Konzepten der NAKO Gesundheitsstudie oder dem Krebsregister Mecklenburg-Vorpommern nachvollzogen.

Darüber hinaus unterstützt die THS der Universitätsmedizin Greifswald die Arbeit mit Sekundärdaten (z. B. Melderegisterabrufe). Mehr Informationen dazu befinden sich im Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2].

2 Arbeitsabläufe und Datenflüsse

Die nachfolgenden Darstellungen beschreiben den zum Zeitpunkt der Dokumenterstellung gültigen Stand der Planungen und Absprachen.

2.1 Grundlegende Rahmenbedingungen

Neben den hier beschriebenen treuhandstellenspezifischen Aspekten ist sowohl für das DZHK als auch für das Teilprojekt Datenhaltung eine detaillierte Abstimmung sämtlicher Abläufe bezüglich einer gemeinsamen Schnittstelle notwendig. Dies erfolgt mit Fokus auf technische Ausprägungen und Abläufe (Workflows, Use Cases). Eine Übersicht der innerhalb der Treuhandstelle umgesetzten SOPs wird in Tabelle 7 im Anhang dargestellt. Ergänzend wurde das gemäß Art. 30 Abs. 5 DS-GVO geforderte Verfahrensverzeichnis erstellt und kann auf seperate Anfrage eingesehen werden.

Der Anschluss einer neuen Studie oder eines neuen Studienstandortes an die Klinische Infrastruktur des DZHK macht umfangreiche organisatorische Standards erforderlich. Um notwendige Arbeitsabläufe abzubilden, werden durch die Klinische Infrastruktur Formulare (z. B. zur Beantragung von Client-Zertifikaten und Nutzer-Zugängen) sowie entsprechende Installationsbeschreibungen bereitgestellt. Es werden vor Studienstart Webinare für das Studienpersonal durchgeführt. Nach ausführlichen System-Tests, Vorliegen eines Ethikvotums und finaler Einrichtung der studienspezifischen Konfiguration werden durch den Studienverantwortlichen Abnahmeprotokolle unterzeichnet, wodurch die Produktivsetzung des neuen Standorts/der Studie erfolgen kann (vgl. Formulare; Protokolle und Anträge in Tabelle 8- Tabelle 10). Alle standardisierten Unterlagen werden zentral bereitgestellt[14] und können von allen Studienmitarbeiter:innen auf Deutsch und Englisch genutzt werden.

2.2 Datenintegration und Speicherung personenbezogener Daten

Durch die Zusammenarbeit der Treuhandstelle mit dem Teilprojekt Datenhaltung der Universitätsmedizin Göttingen ergeben sich für die Implementierung der Treuhandstelle folgende Rahmenbedingungen:

Die Erfassung der pseudonymisierten medizinischen Daten in den Studienzentren erfolgt über elektronische Fragebögen (electronic Case Report Forms, eCRF). Es wird in allen DZHK-Studien ein Basisdatensatz verwendet. Jede Studie verfügt zudem über einen studienspezifischen Datensatz. Für

[14] https://dzhk.de/das-dzhk/klinische-dzhk-studien/studienvorbereitung-durchfuehrung/

die Erstellung der benötigten Pseudonyme ist die Erfassung der IDAT notwendig. Diese werden jedoch nicht in den eCRF der DH gespeichert.

Die Abnahme von Bioproben und das Erfassen von Bildern erfolgt analog zu dem beschriebenen Vorgehen. DZHK-weit wurden einheitliche Proben-Abnahmesets für Biomaterial definiert. Ergänzend sind studienspezifische Abnahmen möglich. Für die Erfassung von Bilddaten im DICOM[15]-Format, sowie möglicherweise auch EKG-Daten wird das BDMS genutzt, wobei derzeit kein einheitlicher Abnahmedatensatz definiert ist. Die notwendige technische Infrastruktur wird durch die Partner in Greifswald bereitgestellt. Die DH in Göttingen stellt zusätzlich die erforderlichen Komponenten der Transferstelle (für den teilweise notwendigen Datenaustausch zwischen den Fachsystemen) zur Verfügung.

Für die strukturierte Erfassung von Formulardaten werden erforderliche eCRF mit Hilfe des von der iAS Berlin GmbH entwickelten, webbasierten Werkzeugs secuTrial® erstellt. Alleiniger Vertragspartner der iAS GmbH ist die Universitätsmedizin Göttingen. Über die Kooperationsvereinbarung des Verbundprojektes Klinische Forschungsplattform ist geregelt, dass für die THS ein Recht besteht, an der Definition und Testung der Schnittstelle mitzuwirken. Für Form und Inhalt der elektronischen Erfassungsformulare sind die jeweiligen Studien verantwortlich. secuTrial® verfügt über ein zentrales Rollen- und Rechte-System. Somit ist es wie gefordert möglich nur einer Auswahl von Personen bzw. Personengruppen (Ärzt:innen, Studien) das Ändern von Kontaktdaten zu gestatten.

Zudem werden weitere Metadaten zu Studie, Projekt und Standort durch die THS verwaltet. Die Daten werden gemäß dem Datenschutzkonzept der THS [2] verschlüsselt gespeichert und mit den entsprechenden Sicherheitsbestimmungen bezüglich Zugriff und Backup gesichert (vgl. Datenschutzkonzept der THS der UMG [2]).

Definierte, vertraglich vereinbarte Schnittstellen erlauben die notwendige Interaktion zwischen Treuhandstelle und secuTrial®. So umfasst der derzeitige Funktionsumfang der versionierten Schnittstelle zwischen Datenhaltung und Treuhandstelle das Anlegen neuer a) Teilnehmer:innen und b) Einwilligungen, sowie c) das Editieren von Kontaktdaten bestehender Teilnehmer:innen, d) die Anzeige von Stammdaten, e) die Bearbeitung von Einwilligungen (vgl. Abbildung 5) und f) den Austausch von von-der-THS-erzeugten Pseudonymen. Die Funktionalitäten a-e werden ausschließlich auf THS-Systemen bereitgestellt. Um ein einheitliches Look-and-feel für Anwender:innen zu ermöglichen, werden diese Funktionalitäten durch Buttons im secuTrial®-System aufgerufen und eine direkte Verbindung zwischen Studiensystem und Treuhandstelle mittels eines Tunnels initiiert. Die Treuhandstelle ist somit für das DZHK als autarkes System in secuTrial® integriert. Weitere Funktionen befinden sich derzeit im Abstimmungsprozess mit der iAS GmbH Berlin.

2.3 Datenflüsse innerhalb der Klinischen Forschungsplattform

Die vorstehende Abbildung 4 zeigt den geplanten Datenfluss zwischen den einzelnen Teilprojekten. Technische Details der einzelnen Abläufe sind dem Anhang zu entnehmen.

[15] Digital Imaging and Communications in Medicine (DICOM; deutsch Digitale Bildgebung und -kommunikation in der Medizin)

Bei Einschluss einer Person werden zuerst Informed Consent-Informationen und identifizierende Daten an die Treuhandstelle übertragen. Das daraufhin durch die THS für diese Person generierte, eindeutige PSN wird im Anschluss an das Studienzentrum übertragen (vgl. Abbildung 4).

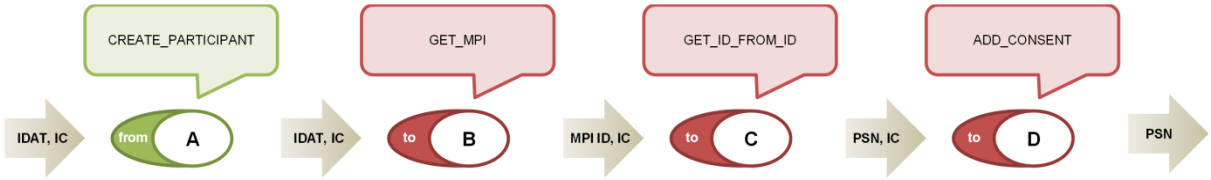


Abbildung 4 Schematische Darstellung des Workflows " Studienteilnehmer anlegen" in der Treuhandstelle des DZHK. [3]

Im Rahmen des DZHK werden zu keinem Zeitpunkt Primärpseudonyme bzw. Pseudonyme erster Stufe an die DH bzw. an die Projekte übergeben, sondern der DZHK-spezifische THS-Workflow sieht vor, dass sofort Sekundärpseudonyme bzw. Pseudonyme zweiter Stufe abgeleitet und übergeben werden (siehe Abbildung 3). Aktuell speichert die Datenhaltung eCRF-, Labor- und Bioprobendaten in secuTrial®. Langfristig sollen Labor- und Bioprobendaten ausschließlich in CentraXX in Form des DZHK-LIMS gespeichert werden. Dabei kommen für eine Person jeweils spezifische Sekundärpseudonyme zur Anwendung. Durch den DZHK-spezifischen THS-Workflow ist sichergestellt, dass für das Primärpseudonym einer Person mehrere jeweils eindeutige Sekundärpseudonyme abgeleitet werden können.

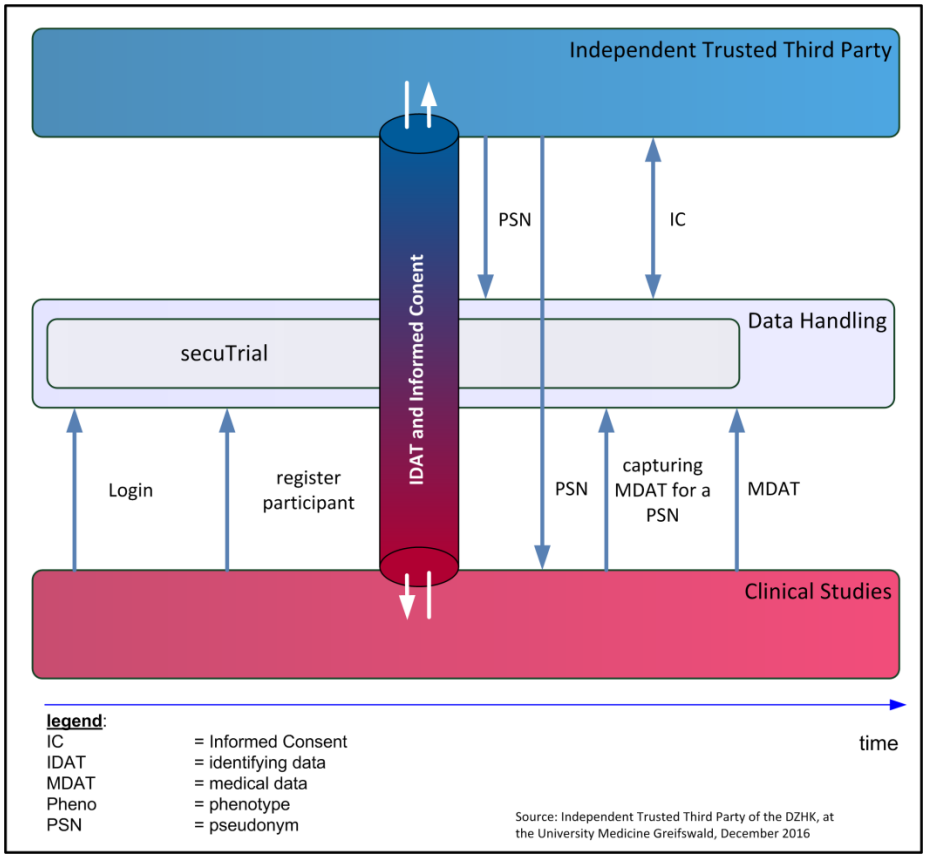


Abbildung 5 Interaktion der beteiligten Systeme am Beispiel „Anlegen eines Teilnehmers“

Unter Angabe der PSN kann das Studienzentrum daraufhin die MDAT der Person in Form von medizinischen Daten und Bioprobendaten u.a. an die Datenhaltung in Göttingen übermitteln.

Ergänzend veranschaulicht Abbildung 5, dass die Übergabe der personenidentifizierenden Daten direkt zwischen Studienzentrum und Treuhandstelle durch einen Tunnel stattfindet. Die Datenhaltung hat zu

keinem Zeitpunkt Zugang zu den IDAT der teilnehmenden Person. Die THS hat zu keinem Zeitpunkt Zugang zu medizinischen Daten der teilnehmenden Person.

Nachstehend zeigt Tabelle 3, dass außerhalb der behandelnden und datenerhebenden Kliniken in keinem Teilprojekt der Klinischen Forschungsplattform IDAT, MDAT und PSN gemeinsam vorliegen. Zudem ist ersichtlich, dass innerhalb der Datenhaltung, dem LIMS und BDMS ausschließlich pseudonymisierte Daten gespeichert werden.

Tabelle 3 Datenverteilungsmatrix

Teilprojekt	IDAT	MDAT gemäß Einwilligung	Study-ID	n-PSN
Studien (Kliniken)	Ja	Ja	Nein	Nein
Treuhandstelle	Ja	Nein	Ja	Ja
LIMS	Nein	Ja	Nein	Ja
BDMS	Nein	Ja	Nein	Ja
Datenhaltung	Nein	Ja	Nein	Ja

2.4 Anwendungsfälle

Anmeldung am eCRF-System

Um die Funktionen der Treuhandstelle im Studienzentrum nutzen zu können, ist eine Authentifizierung des Nutzers über secuTrial® erforderlich. secuTrial® verwaltet stellvertretend für die Treuhandstelle Rollen und Rechte von Nutzer:innen (Trusted Delegation). Auf diese Weise kann die Treuhandstelle einen rollenspezifischen Funktionsumfang anbieten. Bei erfolgloser Authentifizierung ist eine Verwendung der Treuhandstellenfunktionalität ausgeschlossen. Gleiches gilt für den Versuch Treuhandstellenfunktionalitäten ohne den Einsatz der secuTrial®-Instanz der Datenhaltung Göttingen anzusprechen.

Die Anmeldung wird durch Nutzer:innen im Studienzentrum initiiert. Die Maske zur Eingabe der Anmeldeinformationen stellt die Datenhaltung Göttingen bereit. Ein:e Nutzer:in gibt Nutzernamen und Passwort ein und die Daten werden verschlüsselt über HTTPS an secuTrial® übertragen. Nach Überprüfung der Anmeldedaten und Zuordnung von Rollen und Rechten wird ebenfalls über HTTPS eine Session-bezogene Kommunikation zur Treuhandstelle aufgebaut. Die übermittelten Anmeldeinformationen (Nutzername, Institution, Nutzer-ID, Rolle, Vorname, Nachname, Titel) dienen innerhalb der Treuhandstelle gleichzeitig als Audit-Informationen. Im Anschluss wird eine Session-bezogene Kommunikation zwischen secuTrial® und Nutzer:in im Studienzentrum hergestellt, so dass Anfragen direkt an die Treuhandstelle weitergeleitet werden können.

Studienteilnehmer:innen und Informed Consent anlegen

Grundvoraussetzung für die Teilnahme einer Person an einer Studie des DZHK ist die Einwilligung in die Datenverarbeitung (Pflichtmodul). In Abstimmung mit dem Ethik-Projekt des DZHK werden die Einwilligungen zur Teilnahme an der jeweiligen Studie und zur Entnahme / Verwaltung von Bioproben

in der Regel unabhängig voneinander eingeholt. Durch Verwendung optionaler Module (z. B. Datenherausgabe an Dritte, Wiederkontaktierung) sind Teil-Einwilligungen, aber auch Teil-Widerrufe möglich.

Um eine:n neuen Studienteilnehmer:in anlegen zu können, wird die Funktion zur Anlage neuer Studienteilnehmer in secuTrial® durch das Studienpersonal im Studienzentrum aufgerufen. Das Web-Formular zur Erfassung der IDAT (vgl. Abbildung 6 und Abbildung 7) wird durch die Treuhandstelle bereitgestellt. Der:die Nutzer:in gibt die identifizierenden Daten gemäß der Spezifikation der Treuhandstelle in die Eingabemaske ein und übersendet sie über einen verschlüsselten Tunnel direkt an die Treuhandstelle (vgl. Kapitel 2.3). Abbildung 19 im Anhang veranschaulicht den beschriebenen Workflow aus technischer Sicht.

Innerhalb der Treuhandstelle werden anhand der übermittelten IDAT Vergleichsprozesse angestoßen, die die eingehenden IDAT mit bereits bekannten IDAT abgleichen (vgl. Anlagen: DZHK-SOP-*P*--06 Erfassung IDATInformed Consent). Ist die spezifizierte Person noch nicht vorhanden, wird eine neue Person in der THS angelegt, ein entsprechendes Pseudonym generiert und das Pseudonym an das Studienzentrum zurück übermittelt. In diesem Fall kann im Studienzentrum unter Angabe des Pseudonyms mit der Erfassung der medizinischen Daten begonnen werden.

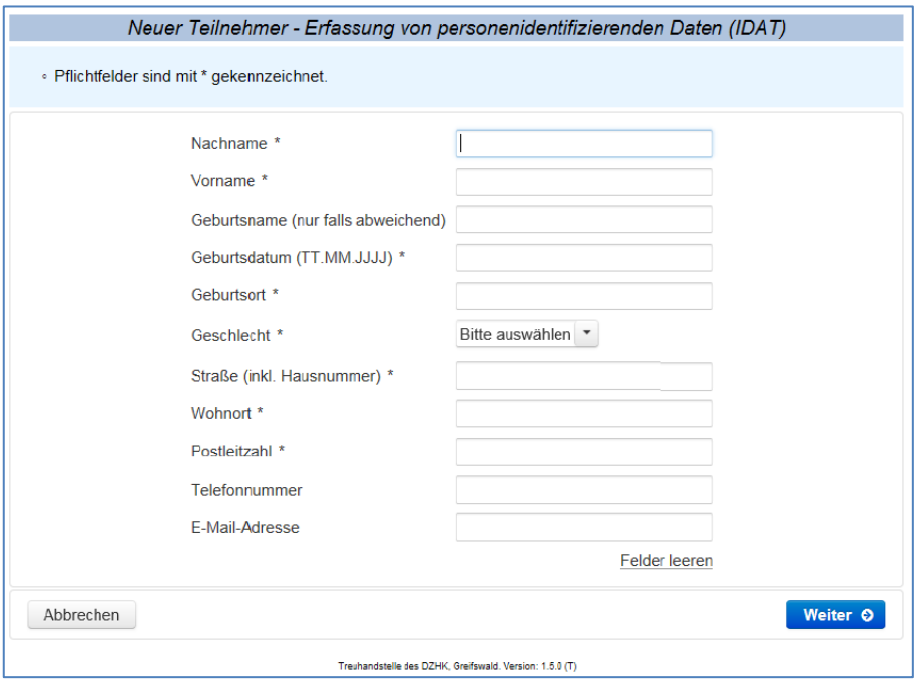


Abbildung 6 Erfassung der personenidentifizierenden Daten mittels THS-Formular

Gleichermaßen stellt die Treuhandstelle Web-Formulare zur Eingabe der Einwilligung bereit, um die im Studienzentrum in Papierform vorliegenden ICs auf einfache Weise an die Treuhandstelle übertragen zu können. Zur Qualitätsprüfung wird ergänzend ein Scan des Papier-basierten IC an die THS übermittelt (vgl. Abbildung 7). Dies ist technisch auch im Nachgang möglich.

Jegliche Kommunikation mit der Treuhandstelle wird mittels verschlüsselter Verbindungen sowie durch Client-Zertifikate und/oder Basic-Authentication, welche den Studienzentren durch die Treuhandstelle zur Verfügung gestellt werden, abgesichert.

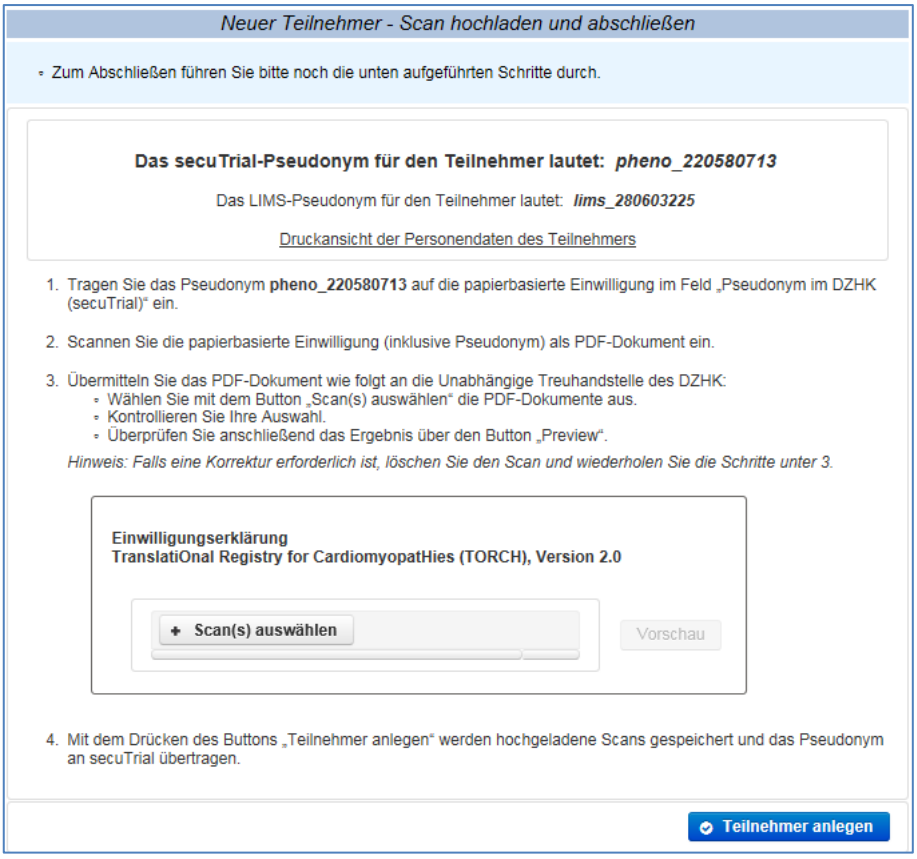


Abbildung 7 Nach Erfassung der digitalen Einwilligung (IC) wird ein Scan der Papiervariante durch das Studienzentrum direkt an die THS übermittelt und der:die Studienteilnehmer:in abschließend angelegt.

Studienteilnehmer:innen aktualisieren

Die Änderung von Personendaten wird grundsätzlich in zwei Bereiche unterschieden: Sollen IDAT einer Person aktualisiert werden (z.B. Namensänderung), wird die notwendige Änderung des Datenbestands innerhalb der Treuhandstelle vorgenommen. Sollen dagegen MDAT angepasst oder ergänzt werden, erfolgt die Änderung in der Datenhaltung. Im Kooperationsvertrag ist geregelt, dass die zur Änderung notwendigen eCRF jeweils durch die datenspeichernde Stelle bereitgestellt werden.

Voraussetzung für die Änderung einer Person ist, dass die Person bereits angelegt wurde und demzufolge das entsprechende Pseudonym bekannt ist. Der Nutzer im Studienzentrum ruft, unter Angabe des Pseudonyms der zu ändernden Person, das entsprechende eCRF in secuTrial® auf. Zur Bearbeitung von IDAT und MDAT werden jeweils getrennte Formulare bereitgestellt.

Im Fall einer IDAT-Aktualisierung kontaktiert das Studienzentrum die Treuhandstelle und übermittelt die anzupassenden Daten. Die THS-Mitarbeiter:innen bearbeiten in den internen Verwaltungssystemen die IDAT. Bevor die aktualisierten IDAT gespeichert werden, durchlaufen sie erneut den Matching-Prozess. Sind die neuen IDAT eindeutig, wird der Datenbestand bei gleichbleibendem Pseudonym in der Treuhandstelle aktualisiert. Führt der Matching-Prozess zu einem unsicheren Match, wird der:die Nutzer:in darüber informiert und weitere Schritte müssen manuell ggf. mit dem Studienzentrum geklärt werden (vgl. Verwaltung von Identitäten und Dopplerausschluss, Kapitel 3.6.1 im Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2]).

Die Änderung von MDAT erfolgt direkt in den eCRFs von secuTrial®. Mithilfe des Pseudonyms wird das entsprechende eCRF von der Datenhaltung angefordert, die medizinischen Daten werden aktualisiert

und zur Speicherung an die Datenhaltung in Göttingen übermittelt. Abbildung 20 IC anlegen (Technische Sicht) und Abbildung 21 IDAT ändern (Technische Sicht) im Anhang veranschaulichen den beschriebenen Workflow.

Informed Consent aktualisieren

Voraussetzung für die Aktualisierung eines Informed Consent ist, dass die zugehörige Person bereits angelegt wurde, das entsprechende Pseudonym bekannt ist und dieser Person bereits ein IC zugeordnet wurde. Der Nutzer im Studienzentrum ruft, unter Angabe des Pseudonyms, die jeweilige Person in secuTrial® auf. Unter der Funktion „Stammdaten und IC bearbeiten" können ein oder mehrere Informed Consent nacherfasst werden. Dieses Formular wird durch die Treuhandstelle mittels IFrame-Einbettung zur Verfügung gestellt.

Bei der Aktualisierung eines Informed Consent wird ein neuer IC der Studienteilnehmer:in gemäß der DZHK-SOP „*Erfassung von IDATs und des ICs*" durch das Studienzentrum erfasst, wodurch ein bereits vorhandener IC ab dem Einwilligungsdatum des neuen IC seine Gültigkeit verliert. Der aktuellste IC ist stets Entscheidungsgrundlage für die Zulässigkeit der einzelnen Prozesse der Datenverarbeitung und bildet die dann aktuellen Aspekte der Einwilligung von Studienteilnehmer:innen ab.

Gleichzeitig gilt, dass bis zu diesem Zeitpunkt erfasste Daten weiterhin zu den Bedingungen der zum Erhebungszeitpunkt gegebenen Einwilligung verarbeitet (gespeichert, verwendet) werden können. Die zukünftige Datenerfassung richtet sich jedoch nach den Bestimmungen des neuen IC.

Erfassung von Widerrufen / Studienausschluss

Der Widerruf erfolgt jeweils für eine ausgewählte Studie und sollte im Regelfall direkt an das Studienzentrum adressiert werden. Der Widerruf kann z.B. durch erneute Einwilligung zurückgenommen werden. Zusätzlich kann jederzeit eine Einwilligung von Studienteilnehmer:innen für eine andere Studie vom Studienpersonal eingeholt werden.

Das Studienzentrum ist verpflichtet, den Widerruf der Teilnehmer:innen bei der Treuhandstelle der Universitätsmedizin Greifswald schriftlich in Form des Widerrufsformulars zu melden. Die DZHK-SOP-P-05 (siehe Anlagen I.5) regelt die Erfassung des Widerrufs durch das Studienzentrum.

Nach Übermittlung des Widerrufs an die THS erfolgt die Umsetzung des Widerrufs seitens der THS, der DH, LIMS und BDMS gemäß „*SOP THS_12 Widerruf intern"*. Die THS prüft den Widerruf auf implizite Widerrufe (z. B. bedeutet der Widerruf der Teilnahme in Studie VAD implizit den Widerruf der Teilnahme an der VAD Biomaterialsammlung). Anschließend wird der Widerruf innerhalb der THS digital in das Einwilligungsmanagementsystem eingepflegt (vgl. Verwaltung von Einwilligungen und Widerrufen mittels Einwilligungsmanagement gICS®, Kapitel 3.6.3 im Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2]). Durch die THS wird die vormals gültige Einwilligung der Studienteilnehmer:in geschwärzt und in das Einwilligungsmanagementsystem der THS hochgeladen. Ausnahmen gelten hierbei für AMG-Studien (nachzulesen in Anlagen I.6: *SOP THS_12 Widerruf intern*). Die THS leitet den Widerruf an die DH und das LIMS sowie das BDMS weiter. Innerhalb der DH und des BDMS werden zugehörige medizinische Daten der Teilnehmer:in je nach Studie für die weitere Verarbeitung gesperrt oder in ein spezifisches Widerrufszentrum verschoben.[16] Die DH oder das LIMS

[16] Dies und die Prüfung tagesaktueller ICs vor Herausgabe der Daten durch die Transferstelle, gewährleisten den Ausschluss gesperrter oder widerrufener Daten von der weiteren Verwendung.

senden die Aufforderungen zur Biomaterialvernichtung weiter an die entsprechenden Ansprechpartner in den Studienzentren. Existierende Bioproben werden vernichtet oder für die Weitergabe gesperrt (nur Studienmaterial, Basismaterial wird immer vernichtet) und Biomaterialdaten des vernichteten Materials im zentralen LIMS des DZHK gelöscht. In der THS wird die Zuordnung zwischen Pseudonymen und IDAT gelöscht und eine Bestätigung des erfolgreich umgesetzten Widerrufs an das Studienzentrum übermittelt. Abbildung 22 Widerruf (Technische Sicht) im Anhang veranschaulicht den beschriebenen Workflow aus technischer Sicht.

Der beschriebene Vorgang gilt nicht für Studien nach AMG, da bei unerwünschten Ereignissen, die bis zu 15 Jahren nach Teilnahme an der Studie auftreten können, eine gesetzliche Nachverfolgbarkeit zur Studienteilnehmer:in gewährleistet sein muss. Sonderregelungen finden sich in den SOPs zum Widerruf und Studienausschluss.

Nach Dokumentation des Widerrufsvorgangs innerhalb der THS (eine Auflistung der gespeicherten Daten ist in *SOP THS 12* zu finden) ist der Widerrufsprozess abgeschlossen. Seit Start des DZHK wurden in der THS insgesamt 66 Widerrufe (Stand: 18.01.2018) auf diese Weise dokumentiert.

Jede:r Verantwortliche der beteiligten Projekte sorgt dafür, dass ein eingehender Widerruf (nach dem Rechtsgedanken Art. 26 Abs. 3 DS-GVO) an die THS weitergeleitet wird.

Zusätzlich steht den Studienmitarbeiter:innen die Durchführung eines Studienabbruches vor Rekrutierung und technischem Anlegen von Studienteilnehmer:innen in der THS offen, der nur geringfügige Nachfolgeprozesse in der Treuhandstelle hervorruft.

Qualitätssicherung von Einwilligungen

Neben den typischen Quartals- und Jahresberichten für Geschäftsstelle und Fördermittelmanagement erstellt und versendet die Treuhandstelle monatliche Feedback-Reports an alle Studienzentren. Diese geben u.a. Aufschluss über aktuelle Zahlen der angelegten Studienteilnehmer:innen, sowie Widerrufe der DZHK-Studien in der Klinischen Forschungsplattform.

In IC-Prüfberichten informiert die THS über noch offene Punkte und Probleme bei der Verwaltung der Einverständniserklärungen. Je Studie und Studienzentrum werden Auffälligkeiten innerhalb der Einwilligungen gemeldet und Hinweise zu deren Behebung gegeben.

Darüberhinaus erfolgt ein Datenmonitoring der IDAT auf THS-Seite und der MDAT auf Datenhaltungsseite und es werden im Bedarfsfall Korrekturen angefordert. Beispielsweise ist in der Studie „TORCH“ jedes Zentrum verpflichtet den Daten einen „Review-Status“ zu geben, um so die Möglichkeit für qualitativ hochwertige Datenherausgaben zu schaffen.

Einbindung der THS in die Prozesse des BDMS und LIMS

Die THS stellt für die verschiedenen Prozesse (Bilddatenupload, BDMS-integrierte Bildanalyse, Export von Bilddaten, Biomaterial analysieren, Genanalysen, etc.) Studienteilnehmer-spezifische Events. Damit ist es grundsätzlich möglich die Einwilligung auf Prozessebene zu modellieren. Die tagesaktuelle Synchronisierung dieser Events führt zu einer sehr zeitnahen Umsetzung von Widerrufen (siehe auch Abschnitt F1.5).

Die THS stellt für den Datentransfer zwischen dem BDMS und DH einen Service bereit, damit die Systeme Daten zu einem:einer Studienteilnehmer:in austauschen können. Dieses basiert auf einem temporären Token, der kurzzeitig für eine:n Studienteilnehmer:in identifiziert, so dass die

Informationstrennung (siehe Tabelle 3 Datenverteilungsmatrix erhalten bleibt. Details finden sich im Abschnitt Aufruf des Patientenvisitenplans; in Abbildung 28, in Abbildung 29).

2.5 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 und gleichzeitig den Ansprüchen des Datenschutzes genügen.

Die identifizierenden Daten (IDAT) bestehen aus Vornamen, Nachnamen, Geburtsnamen (falls abweichend), Geschlecht, Geburtsdatum, Geburtsort, Anschrift und auch Kontaktdaten wie Telefon, Fax und Mail (siehe Tabelle 4). 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 spezifisch erhobene medizinische Daten (MDAT) der eingeschlossenen Personen bekannt. Durch die Teilnahme an einer Studie können jedoch auch in der Treuhandstelle ggf. Gesundheitsdaten wie beispielsweise eine vorliegende Erkrankung, die erst zur Studienteilnahme berechtigt, abgeleitet werden. Die konkreten Anforderungen an die IDAT sind jedoch abhängig vom jeweiligen Studiendesign. Lediglich die Items Geburtsdatum und Geschlecht einer Person werden sowohl für eine fehlerfreie Zuordnung pseudonymisierter Daten als auch im Rahmen wissenschaftlicher Auswertungen verwendet. Adressdaten und Kontaktinformationen dienen in aller Regel einer späteren (eingewilligten) Kontaktaufnahme.

Im Einzelfall ist auch die Speicherung weiterer personenbezogener Daten, wie beispielsweise Fall-, Laborauftrags- und Bildnummern möglich. Diese unterliegen den genannten Regelungen für identifizierende Daten.

Die Dauer der Datenspeicherung für medizinische Forschungsvorhaben zur Prävention, Diagnostik und Behandlung von Krankheiten, insbesondere solcher des Herz-Kreislauf-Systems ist in der Regel unbegrenzt - spezialgesetzliche Regelungen, wie etwa Aufbewahrungspflichten (AMG, MPG, Vorgaben von Journals, Strahlenschutzgesetz), sind zu beachten.

Tabelle 4 Übersicht der in der THS gespeicherten personenbezogenen Daten

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
Fall-,Laborauftrags- und Bild-nummern	Eindeutige Zuordnung des Materials zur Person
Elektronisch auswertbare Einwilligung der teilnehmenden Person	Grundvoraussetzung zur Speicherung und Abruf der IDAT innerhalb der Treuhandstelle
Informationen zur/zum Daten erhebenden Projekt/Studie/Register	Qualitätssicherung Re-Kontaktierung
Identifizierende Daten des Erfassers: Name, Vorname, Titel, Abteilung	Qualitätssicherung Re-Kontaktierung

3 Technische Maßnahmen

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

3.1 Gesicherte Dokumentenübertragung mit T*ckets

Um Dokumente mit personenidentifizierenden Daten, wie beispielsweise Widerufsformulare oder nachträglich zu übermittelnde Einwilligungen sicher, zugriffsbeschränkt und möglichst automatisch vom Studienstandort in die Treuhandstelle übertragen zu können, wird im DZHK das von der Universitätsmedizin Greifswald (Institut für Community Medicine) entwickelte System „T*ckets“ verwendet.

Dieses rein Token-basierte Ticketsystem stellt einmalig nutzbare Zugänge für den Upload oder Download von Dateien bereit und gestattet so einen geschützten bidirektionalen Austausch von digitalen Dokumenten. Um beispielsweise einen Einwilligungsscan an die THS zu übermitteln, erfragt das Studienzentrum per Mail ein gültiges Zugangsticket bei der THS. Dieses Ticket wird automatisch durch die THS erstellt. Um dieses Ticket nutzen zu können, wird gleichzeitig eine PIN generiert und an den Anfragenden per Mail versandt. Das Ticket kann anschließend mit Hilfe der PIN vom Studienzentrum eingelöst werden. Hierbei wird der Einwilligungsscan an die THS übermittelt und AES-verschlüsselt (256-bit) in der entsprechenden T*ckets-Datenbank abgelegt. Die THS-Mitarbeiter:innen werden per E-Mail informiert, wenn ein Ticket eingelöst wurde und können anschließend die hochgeladenen Dokumente weiter verarbeiten.

So wie bei der Einbettung von Treuhandstellen Webformularen u. a. in secuTrial®, ist zum Aufrufen des Ticketsystems ebenfalls die Installation eines Client Zertifikats im Browser notwendig.

Die THS nutzt dieses Secure-File-Transfer Ticket-System aber auch um beispielsweise Berichte der Qualitätsmängel von ICs Studienzentren zum Download bereitzustellen. In diesem Fall kann das Studienzentrum beim Einlösen des Tickets mit der PIN die von der THS für das Zentrum hinterlegten Dokumente herunterladen.

3.2 Dokumentation wiederkehrender Arbeitsabläufe mittels JIRA

Jira ist eine Java-basierte Webanwendung und kann u. a. sowohl zum operativen Projektmanagement als auch zum Aufgabenmanagement eingesetzt werden.

In der THS des DZHK werden wiederkehrende Abläufe und Arbeiten, wie beipielsweise die Planung und Vorbereitung neuer Studien, aber auch die Umsetzung von Widerrufen (vgl. Anlagen I.6: *SOP-THS-12_Widerruf_intern*) mittels JIRA dokumentiert. Insbesondere Letzteres soll die technische Umsetzung des Widerspruchsrechts gemäß Art. 21 DS-GVO unterstützen. U. a. wird Folgendes dokumentiert:

- Datum des Eingangs des Widerrufs
- Datum des Versendens der Eingangsbestätigung des Widerrufs an das Studienzentrum
- Zeitpunkt der Rückmeldung des Widerrufs an angeschlossene Systeme
- Vollständigkeit und Korrektheit des Widerrufs
- Status der Widerrufsumsetzung in THS, Studienzentrum, Datenhaltung, …
- Datum des Abschlusses der Widerrufsumsetzung

Auf diese Weise ist es möglich, trotz der Vielzahl von Studien im DZHK, den stets aktuellen Arbeitsstand der vielfältigen und meist parallelen Arbeitsprozesse im Blick zu behalten. Gleichzeitig werden notwendige Auswertungen erheblich vereinfacht. Identifizierende Daten einzelner Studienteilnehmer:inen werden nicht im Dokumentationssystem JIRA gespeichert. Die Dokumentation erfolgt zu allen Vorgängen ausschließlich mit Hilfe der vergebenen Pheno_Pseudonyme.

3.3 Identitätsmanagement mittels E-PIX®

Gemäß Art. 25 Abs. 2 DS-GVO werden nur die für das Identitätsmanagement erforderlichen personenidentizierenden Daten eines:einer Teilnehmer:in im E-PIX® erfasst. Diese sind als Pflichtfelder in der entsprechenden Eingabemaske gekennzeichnet (vgl. Abbildung 6).

Details zur Verwaltung von Personen und Identitäten mittels E-PIX® sind dem Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2] Abschnitt 5.2.4 zu entnehmen.

3.4 Pseudonymverwaltung mittels gPAS®

Gemäß Art. 32 Abs. 1 lit.a DS-GVO unterstützt die Verwendung von Pseudonymen dabei, ein angemessenes Schutzniveau der Datenverarbeitung zu gewährleisten.

Das Webservice-basierte Werkzeug gPAS® dient der Generierung und Verwaltung von Pseudonymen innerhalb der THS des DZHK. Es werden unterschiedliche Pseudonyme je Datentyp und Arbeitsprozess

generiert (vgl. Abbildung 3). Details zur Generierung und zum Zuordnungsprozess sind dem Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2] Abschnitt 5.2.5 zu entnehmen.

3.5 Verwaltung von Einwilligungen und Widerrufen mittels gICS®

Die Erhebung, Verarbeitung und Nutzung von medizinischen Forschungsdaten erfordert im Regelfall eine zweckbezogene, freiwillige und informierte Einwilligung der:s Betroffenen, den sogenannten Informed Consent (IC) (vgl. Art. 6-9 DS-GVO). Gleichzeitig wird eine organisorische (vgl. Abschnitt 1.3) und technische Umsetzung des Widerspruchrechts von Teilnehmer:innen durch Art. 21 DS-GVO gefordert.

Die THS des DZHK ist gemäß Definition der DS-GVO datenverarbeitende Stelle für personenidentifizierende Daten und somit verpflichtet, alle datenverarbeitenden Vorgänge nachvollziehbar darzustellen. Diese Nachweispflicht gegenüber den Aufsichtsbehörden ist gleichzeitig Grundlage zur Wahrung der Betroffenenrechte nach Auskunft, Korrektur und Löschung. Nur durch lückenlose Dokumentation sämtlicher Vorgänge, und insbesondere durch die zentrale Verwaltung aller Einwilligungen und Widerrufe innerhalb der THS, kann diese Nachweispflicht durch die THS erfolgreich erfüllt werden.

In der THS des DZHK dient das webservice-basierte Werkzeug gICS® der Verwaltung von Einwilligungen und Widerrufen. Details zum modularen Einwilligungsansatz und zur Verwaltung der Einwilligungen und Widerrufe sind dem Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2] Abschnitt 5.2.6 zu entnehmen.

3.6 Service-orientierte Architektur der Treuhandstelle

Ziel der im DZHK verwendeten Treuhandstellenarchitektur ist es, das Konzept des Datenschutzes durch Technikgestaltung (und durch datenschutzfreundliche Voreinstellungen) gemäß Art. 25 DS-GVO umzusetzen.

Arbeitsabläufe innerhalb der Treuhandstelle sollen möglichst automatisiert werden können und dafür notwendige Kommunikation zwischen ID-Management, Pseudonymverwaltung und Einwilligungsmanagement auf ein Mindestmaß manueller Intervention reduziert werden. Aus diesem Grund wird im Rahmen der THS des DZHK ein workflow-basierter Dispatcher-Ansatz verwendet. Details zum Ansatz und der zugrundeliegenden Service-orientierten Architektur sind publiziert [3] und können ergänzend dem Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2] Abschnitt 5.2.3 entnommen werden.

3.7 Einbindung des eCRF-Systems secuTrial®

Für die Erfassung der Daten setzt das Teilprojekt Datenhaltung elektronische Fragebögen (sog. eCRF) ein. Zu deren Realisierung wird das kommerzielle EDC-System secuTrial® genutzt. secuTrial® ist vollständig webbasiert und unterstützt typische Funktionen, wie Audit-Trail, ein Rollen- und

Rechtekonzept und eine elektronische Signatur. Die Einhaltung gängiger Sicherheitsstandards gemäß 21 CFR Part 11[17] wurde offiziell bestätigt. [6]

4 Organisatorische Maßnahmen

Einrichtung der Treuhandstelle an der Universitätsmedizin Greifswald und Rolle des Instituts für Community Medicine

Wie in A1.3 beschrieben, ist die Treuhandstelle rechtlich Teil der **Universitätsmedizin Greifswald** (Körperschaft des öffentlichen Rechts) und an das Institut für Community Medicine, Abteilung Versorgungsepidemiologie und Community Health (ICM-VC) angegliedert, jedoch in organisatorischer Hinsicht unabhängig. Alle technischen Systeme sind in die bestehenden Infrastrukturen der Abteilung ICM-VC integriert und werden nach den Standards der Universitätsmedizin und der Abteilung ICM-VC betreut. (weitere Details im Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2] Abschnitt 1.4). Durch geeignete technische Maßnahmen ist sichergestellt, dass jeder Zugriff auf Daten der Treuhandstelle durch die Abteilung ICM-VC ausgeschlossen ist.

Übersicht der organisatorischen Maßnahmen

Sämtliche getroffene organisatorische Maßnahmen, die für die Etablierung der THS erforderlich waren, sind detailliiert im Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2] dokumentiert. Nachfolgende Tabelle listet getroffene Maßnahmen und jeweilige Entsprechungen mit weiterführenden Informationen.

Tabelle 5: Übersicht der organisatorischen Maßnahmen und Verweise auf weiterführende Informationen im Datenschutzkonzept der THS der Universitätsmedizin Greifswald [2]

Maßnahme	Kapitel mit Detailinformationen im Datenschutzkonzept der THS der Universitätsmedizin Greifswald
Räumliche Trennung	Kapitel 5.1.2
Netzwerkstruktur und -schutz	Kapitel 5.1.3
Personelle Maßnahmen: Leiter und Mitarbeiter der THS	Kapitel 5.4.1
Rollen und Rechte	Kapitel 5.5

[17] http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11

Verschlüsselung von Systemen	Kapitel 5.5.2
Passwortdokumentation und -sicherheit	Kapitel 5.5.3
Audit Trail	Kapitel 5.8
Datenübertragung	Kapitel 5.9
Datensicherungskonzept	Kapitel 5.11
Ausfallschutz	Kapitel 5.12

D Datenhaltung (DH)

1 Prozesse der Datenhaltung

Die Datenhaltung arbeitet intern mit Standard Operating Procedures (SOPs), welche das Anlegen von Nutzer:innen, einen kontrollierten Updateprozess der Software sowie weitere, für einen sicheren Betrieb der Applikation notwendige Punkte adressieren. Derzeit kommen folgende SOPs in ihrer jeweils aktuellen Version zum Einsatz:

Tabelle 6: Übersicht über die verwendeten SOPs der Datenhaltung

Nr.	Interne Benennung	Beschreibung
1.	MI-sT01_SOP_Struktur Erstellung Änderung	Beschreibung der Struktur der SOPs, sowie das Vorgehen bei Änderungen (Master-SOP)
2.	MI-sT02_ Systemverwaltung	Anweisungen zur Verwaltung und zum Betrieb der in der MI betriebenen IT-Infrastruktur
3.	MI-sT03_SOP_eCRF-Erstellung	Vorgehen bei eCRF-Erstellung, Durchführung von Benutzertest und Systemtest
4.	MI-sT04_SOP_PID-Erstellung und Verwaltung	PID-Erstellung und Verwaltung bei der Pseudonymisierung von Forschungsdaten
5.	MI-sT05_SOP_ Benutzerverwaltung	Anlegen, Ändern, Deaktivieren und Löschen von Nutzerzugängen
6.	MI-sT06_SOP_ Export und Audit-Trail	Berechtigung, Dokumentation und Speicherung von Exporten
7.	MI-sT07_SOP_ Datenbank sperren und wiedereröffnen	Sperrung und ggf. Wiedereröffnung einer Datenbank nach Abschluss der Studie
8.	DM08_SOP_ Systemversionierung	Anweisungen bei Systemversionierung
9.	MI-sT09_SOP_ Langzeitarchivierung	Langzeitarchivierung von Daten nach Abschluss der Studie Sicherung von Daten nach Projektablauf Archivierung von Daten und Abschalten der Mandanten
10.	MI-sT10_SOP_ IT-Fehlermanagement	Beschreibung der Vorgänge zur Vermeidung von Fehlern und Reaktion auf Fehler beim Auftreten
11.	MI-sT11_SOP_Validierungen im laufenden Betrieb	Ablauf des Datenintegritätstests und der Validierung bei Softwareupdate und Produktivsetzung

12.	MI-sT12_SOP_ Dokumentenmanagement	Auflistung der notwendigen Dokumente des Datenmanagements, Dokumentation von Entscheidungen in Softwaresystemen für Projekte
13.	WI01_Systemsicherung und Notfallmanagement	Backupverfahren, Notfall- und Havariemanagement
14.	MI-sT13_Schulungen	Schulung neuer SOP-Inhalte und Nutzerschulung
15.	MI-sT14_SOP_Löschen von Patientendaten	Löschen von Patientendaten/Rückzug der Einwilligungserklärung

Mit einheitlichen SOPs gibt sich die Datenhaltung ein notwendiges und bindendes Regelwerk vor. Die Forderung nach der Existenz von SOPs ist Bestandteil der International Conference on Harmonisation (ICH) Harmonised Tripartite Guideline of Good Clinical Practice (GCP), Kapitel 5.1. Gegenstand der SOPs sind Abläufe innerhalb des elektronischen Datenmanagements von klinischen Studien innerhalb der Datenhaltung, welche aufgrund ihrer Komplexität oder Sicherheitsrelevanz einer Standardisierung und schriftlichen Fixierung bedürfen. Die SOPs berücksichtigen die Anforderungen an das Datenmanagement und die Erhebung von elektronischen Fallsammlungen aus Kapitel 5.5, International Conference on Harmonisation (ICH) Harmonised Tripartite Guideline of Good Clinical Practice (GCP).

2 Arbeitsabläufe und Datenflüsse

Die am Institut für Medizinische Informatik der Universitätsmedizin Göttingen verortete datenhaltende Stelle (Datenhaltung, DH) der Klinischen Forschungsplattform hat die Aufgabe, Methoden, Prozesse und Werkzeuge für die Verarbeitung personenbezogener Daten zu entwickeln und bereitzustellen. Diese Aufgabe teilt sich im wesentlichen in zwei Hauptprozesse: Die Bereitstellung von elektronischen Erfassungsbögen (eCRF, electronic Case Report Forms) für die Dateneingabe sowie den Datenexport und die Herausgabe dieser Exporte für die nachgelagerte Auswertung.

Weitere flankierende Aufgaben, wie die fachliche Beratung bei der Konzeptionierung und Erstellung der eCRF, die Schulung und Hilfestellung zu der eingesetzten Software secuTrial® sowie der Aufbau einer Reporting-Komponente für Qualitätssicherungs- und Controllingbelange des DZHK Vorstands und der Geschäftsstelle. Gemäß der generischen Konzepte zum Datenschutz, welche durch die TMF veröffentlicht wurden, übernimmt die Datenhaltung die Verarbeitung der bereits pseudonymisierten medizinischen Daten (MDAT) sowie den Betrieb der Forschungsdatenbank [4]. Identifizierende Daten (IDAT) sind zu keinem Zeitpunkt den Softwaresystemen oder den Mitarbeiter:innen der DH bekannt.

Zu den typischen Aufgaben der Datenhaltung zählen:

- Bereitstellung und Betrieb der Studiendatenbank secuTrial® auf geeigneten Servern
- Umsetzung aller im DZHK für die Datenerhebung benötigten eCRFs (Basisdatensatz und studienspezifische Module)
- Verarbeitung der über secuTrial® erfassten medizinischen Daten (MDAT) unter den durch die Treuhandstelle generierten Pseudonymen

- Erstellung von Reports und Statistiken zur Unterstützung von Qualitätsmanagement- und Controllingprozessen
- Export von Daten aus der Studiendatenbank zur Weitergabe an die für die Studienauswertung zuständige Stelle oder zur Weitergabe an die Transferstelle im Rahmen von Nutzungsordnungsprozessen

Innerhalb der folgenden Kapitel wird auf das Electronic-Data-Capture Werkzeug secuTrial® der Firma iAS / interActive Systems GmbH[18] eingegangen. Dieses wird für die Erfassung, Verarbeitung und Speicherung von Studiendaten verwendet. Zusätzlich ist ein bedarfsgerechter Datentransfer zwischen den Komponenten der Infrastruktur umgesetzt (z. B. das Einblenden klinischer Daten wie die Information „Raucher: ja/nein“ bei der Befundung eines Bilddatensatzes im BDMS). Dies wird mittels Kommunikation zwischen secuTrial® und dem BDMS ermöglicht. Für eine Auswertung der Bilddaten besteht daher zwischen der Softwarekomponente DH und BDMS ein Austausch von medizinischen Daten. Je nach studienspezifischen Erfordernissen werden Daten aus secuTrial® an das BDMS weitergeleitet und auch die aus den Bilddaten bestimmten Daten an das secuTrial® übertragen.

2.1 Datenerhebung

Die Datenerhebung geschieht in den für die jeweilige Studie zuständigen Zentren. Die erhebenden Zentren haben aufgrund ihres Behandlungszusammenhangs das Recht auf Kenntnis der identifizierenden und der medizinischen Daten (vgl. Tabelle 3). Die erhebenden Personen haben direkten Kontakt mit den Studienteilnehmer:innen. Die Erhebung der Daten erfolgt üblicherweise durch speziell für die Studien geschulte Personen; bspw. durch eine Studynurse oder durch eine:n Studienarzt:ärztin. Die gemäß Art. 6 DS-GVO geforderte Einwilligung der Studienteilnehmer:in zur Speicherung, Veränderung und Nutzung der zu erhebenden Daten wird durch das datenerhebende Personal abgefragt und dokumentiert. Die Speicherung dieser Einwilligungsinformation erfolgt in der Treuhandstelle (vgl. Studienteilnehmer:innen und Informed Consent anlegen S. 30, sowie Informed Consent aktualisieren S. 32).

2.2 Datenerfassung

Die Datenerfassung mit Hilfe der Software secuTrial® erfolgt durch Eingabe der in der Erhebung abgefragten Items in durch die DH erstellten und bereitgestellten eCRFs (siehe Abbildung 8). Die Erfassung der während der Untersuchung erhobenen Daten erfolgt in den meisten Fällen durch eine Studynurse. Der Zugriff auf die Studiendatenbank secuTrial® sowie deren technische Absicherung wird in Abschnitt 3.1 beschrieben.

[18] http://www.secutrial.com

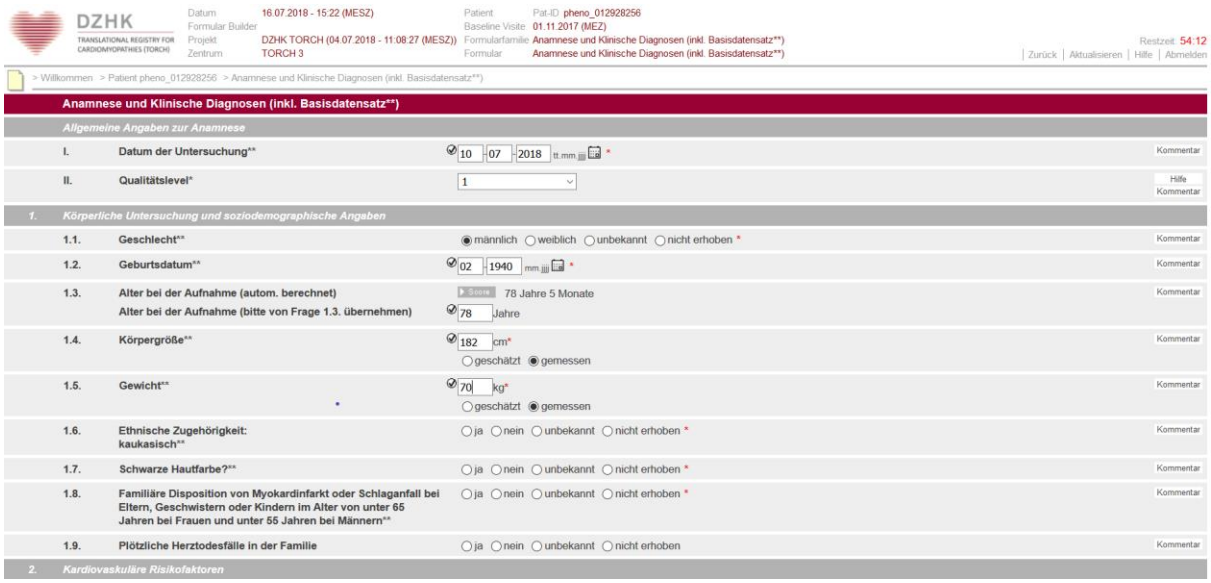


Abbildung 8 Beispiel mit Testdaten für die Eingabe medizinischer Daten über die Dokumentationsmaske in secuTrial®.

Im Vorfeld der Datenerhebung werden die MDAT von den IDAT abgespalten. Dies geschieht durch Einbindung einer IDAT-Eingabemaske der THS, bevor die eigentliche MDAT-Dateneingabe erfolgt. Die Eingabe der IDAT findet direkt auf den Servern der THS statt. Diese getunnelte Realisierung stellt sicher, dass IDAT niemals im secuTrial®-System bekannt werden. Dies veranschaulicht Abbildung 5.

Über secuTrial® wird ebenfalls der für die Qualitätssicherung und das Monitoring relevante Prozess des Query-Managements abgebildet. Queries sind ein Hilfsmittel für Monitore und andere autorisierte Nutzer:innen, um Rückfragen zu unklaren oder unplausiblen Einträgen zu stellen. Studienärzt:innen und Studynurses können Queries lesen und beantworten. Auch dieser Prozess ist ausschließlich für im System hinterlegte Nutzer:innen zugänglich.

2.3 Datenspeicherung und Datenverwaltung

Eine Kernaufgabe der Klinischen Forschungsplattform ist, neben der Bereitstellung geeigneter Erfassungswerkzeuge, die langfristige Speicherung und Verwaltung der erhobenen Daten. Bereits bei der Datenerfassung wird für den entsprechenden Datensatz ein nicht umgehbarer Audit-Trail, angelegt (siehe Abbildung 9). Dieser speichert, welche Person (Login-Information in secuTrial®) mit welcher Rolle (aus der Login-Information abgeleitet) welche Operation zu welcher Uhrzeit/Datum an welchem Datensatz durchgeführt hat. Somit ist eine lückenlose Versionierung und Nachvollziehbarkei aller Änderungen gewährleistet. Auch das oben erwähnte Query-Management wird vollständig in den Audit-Trail aufgenommen. Der Audit-Trail bietet einen Überblick aller Änderungen, die an den Daten im aktuellen Formular vorgenommen und gespeichert wurden. Er kann nach erstmaligem Speichern eines Formulars aufgerufen werden. Direkte Änderungen an der Datenbank der Software sind im Regelbetrieb nicht vorgesehen und durch organisatorische Maßnahmen unterbunden. Bei der Durchführung von Wartungsarbeiten (bspw. Software-Aktualisierungen) werden unvermeindliche Änderungen an der Datenbank gemäß SOP durchgeführt und dokumentiert; U. a. wird durch Datenintegritätstest sichergestellt, dass Studiendaten und Audit-Trail nach der Maßnahme unverändert sind.

Das Eingeben und Speichern von Kommentaren, das Stellen und Beantworten von Queries, sowie ggf. das Durchführen einer SDV[19], von Reviews und Formular-sperren-Aktionen und das Beenden der Datenerfassung stellen allesamt Speichervorgänge am jeweiligen Formular dar. Daher werden all diese Aktionen in der Speicherhistorie im oberen Abschnitt des Audit-Trail abgebildet (siehe Abbildung 9). Jeder Speichervorgang dokumentiert die aktuelle Projektversion, so dass auch hier Änderungen am Projekt-Setup nachvollzogen werden können. Zudem wird angezeigt, ob eine E-Signatur für die Speicherung verwendet wurde und ob diese nach wie vor gültig ist.

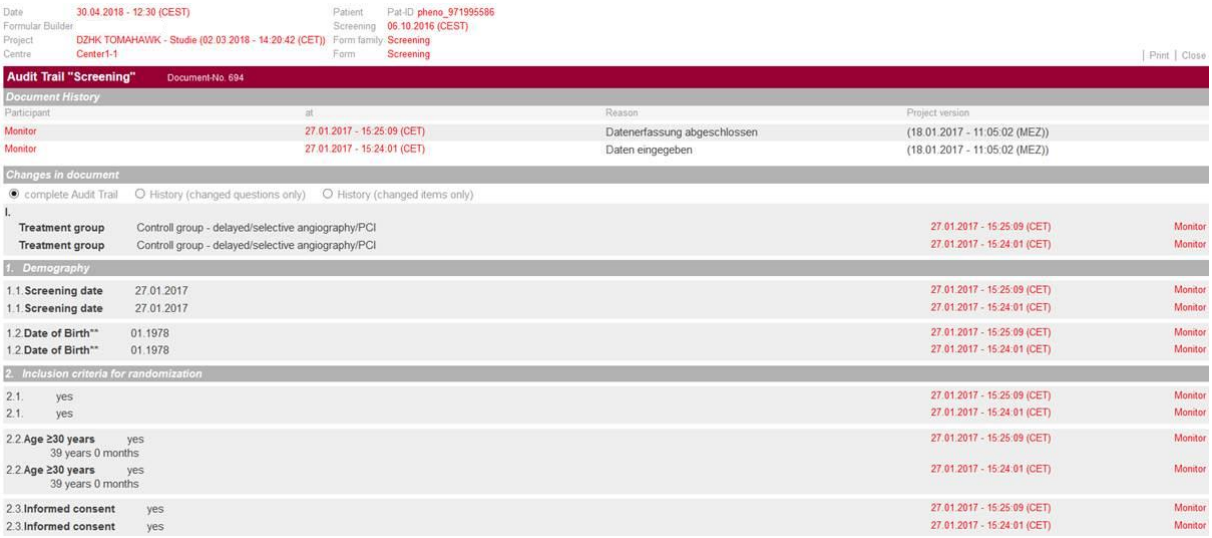


Abbildung 9: Beispiel mit Testdaten für einen Audit-Trail innerhalb von secuTrial®. Sämtliche Eingaben, Änderungen und Löschungen werden protokolliert.

2.4 Transferstelle: Datenaufbereitung und Datentransfer

Das durch die DH betriebene System secuTrial® dient vorrangig der Dokumentation und Speicherung von Studiendaten. Zwar können auch gefilterte Exporte dieser Datenbank durchgeführt werden, jedoch ist das System selbst nicht für die Durchführung statistischer Analysen oder für ein vollständiges Qualitätsmanagement der Daten vorgesehen. Hierfür werden nachgelagerte Systeme verwendet, welche ihrerseits jedoch auch ausschließlich mit pseudonymisierten Daten arbeiten. Die Daten werden hierfür über die Transferstelle, welche ebenfalls durch das Institut für Medizinische Informatik der Universitätsmedizin Göttingen entwickelt und betrieben wird, bereitgestellt. Die Datenaufbereitung beinhaltet folgende Schritte:

- Austausch der systemspezifischen Pseudonyme (Pheno-PSN, LIMS-PSN, BDMS-PSN) durch ein weiteres durch die THS generiertes Pseudonym (Transfer-PSN; siehe Abbildung 25);
- Entfernen von anderen systemspezifischen Identifikatoren
- Ggf. Angleichung von Kodierungen

[19]Source Data Verification (SDV) kann als zusätzlicher Schritt der Datenqualitätssicherung konfiguriert werden. Dann kann der Vergleich der Studiendaten mit den Originaldaten (vgl. Schritte „Datenerhebung“ und „Datenerfassung“)in secuTrial protokolliert werden. Die Überprüfung ist grundsätzlich für jedes Item, aber auch summarisch oder stichprobenhaft für Formulare, Visiten und den gesamten Studienteilnehmer möglich.

Innerhalb des Transferstellen-Datenspeichers können spezifische Suchanfragen auf die pseudonymisierten Daten gestellt werden. Diese Suchanfragen werden gemäß des Dokumentes „*Nutzungsordnung des DZHK e.V. zur Nutzung von Daten und Probenmaterial des DZHK: Use and Access Policy*“[20] durch die Transferstelle bearbeitet. Das heißt, dass sämtliche Anfragen – auch wenn sie später verworfen oder abgelehnt werden – gespeichert werden. Die durch die Transferstelle herausgegebenen Daten werden ebenfalls mit ihrer konkreten Ausprägung (welche Daten wurden wann an welche Person übergeben) gespeichert. Die herausgegebenen Daten werden vor der Herausgabe durch die Transferstelle mit Export-Pseudonymen versehen.

Für die Transferstelle sind alle Datenherausgaben stets rückverfolgbar. Sofern keine Interessenkonflikte vorliegen, speichert die Transferstelle schon während der Abwicklung von Datenherausgaben alle Informationen, welche an Dritte zugestellt wurden. Dies umfasst die betroffenen Daten (Trivialformate mit Stand zum Zeitpunkt der Herausgabe), die Dokumentation des Herausgabeprozesses, sowie die Zuordnung der herausgegeben Datensätze zu den Identitäten der Betroffenen in der Infrastruktur. Die Zuordnung reicht nicht auf die oberste Pseudonymebene oder zu direkt identifizierenden Informationen, da diese nur über die Treuhandstelle hergestellt werden kann. Zusätzlich archiviert die Transferstelle alle während der Anfrage eingesetzten Algorithmen und Zwischenergebnisse. Dies stellt die Nachvollziehbarkeit der Entscheidungen, welche letztendlich zur Datenherausgabe geführt haben, sicher und gewährleistet die Reproduzierbarkeit der Herausgabekohorten, die Integrierbarkeit externer Forschungsergebnisse in die Infrastruktur, sowie ggf. notwendig werdende Risikoanalysen. Während der Datenaufbereitung und der Vorbereitung des Datentransfers wird von Beginn an zwischen zwei Szenarien der Datennutzung differenziert. Erstes Anwendungsszenario ist die Nachnutzung der Daten für die Forschung, das zweite Anwendunsszenario ist die Nutzung der Daten für das Qualitätsmanagement und das Controlling.

Nutzung der Daten für die Forschung

Das erste Anwendungsszenario unterteilt sich noch einmal in zwei Unterszenarien. Das erste ist die Nutzung der Forschungsdaten durch die:den datengenerierende:n Forscher:in in einer über die ursprüngliche Beantragung hinausgehenden Form. Für dieses Szenario definiert die Nutzungsordnung das Verfahren „Nutzungsanzeige“. Die Nutzungsanzeige wird an das Use&Access-Committee[21] des DZHKs (vgl. §5 der Nutzungsordnung) gerichtet und muss von diesem genehmigt werden.

Das zweite Unterszenario ist die Nutzung von Forschungsdaten durch Personen, die nicht an der ursprünglichen Datengenerierung beteiligt waren. Für dieses Szenario definiert die Nutzungsordnung das Verfahren „Nutzungsantrag“. Der Nutzungsantrag wird an das Use&Access-Committee des DZHKs (vgl. §5 der Nutzungsordnung) gerichtet und muss von diesem genehmigt werden.

In beiden Fällen ist für eine Herausgabe von Daten und Biomaterialien ein positives Ethik-Votum der für den:die Antragsteller:in zuständigen Ethikkommission vorzuweisen. Die Nutzung von aggregierten Daten durch Mitarbeiter:innen der Klinischen Forschungsplattform oder des Use&Access-Committees zu Zwecken des Qualitätsmangements, des Controllings oder der Beurteilung von Nutzungsanzeigen und Nutzungsanaträgen ist von diesem Vorgehen ausgenommen.

[20] Kann bei Bedarf bei der Gst. des DZHK erfragt werden.

[21] Die jeweils aktuelle Besetzung des Use&Access-Committees kann auf der DZHK-Website eingesehen werden: https://dzhk.de/das-dzhk/struktur-und-gremien/wissenschaftliche-gremien/

Vor der Herausgabe von Daten an Antragsteller:innen wird eine Umpseudonymisierung vorgenommen, damit die exportierten Daten ein für sie individuelles Pseudonym erhalten. Durch diese zweistufige Pseudonymisierung werden die durch den Treuhänder bereitgestellten Pseudonyme auf die Systeme der Klinischen Forschungsplattform beschränkt. Die Zuordnung zwischen Transfer-PSN und dem Export-Pseudonym wird von der Transferstelle archiviert. Abbildung 23 im Anhang veranschaulicht den beschriebenen Workflow aus technischer Sicht.

Qualitätsmanagement und Controlling

Das zweite Anwendungsszenario ist die Nutzung der Daten zum internen Qualitätsmanagement innerhalb der DH und zum Reporting an das Controlling des DZHK (Vorstand und Geschäftsstelle) und die Studienleitungen. Im Gegensatz zu den zuvor genannten Forschungsexporten werden bei diesem Schritt keine Primärdaten durch die Klinische Forschungsplattform herausgegeben. Mit dem QM beauftragte Personen können zu diesem Zweck Kennzahlen an die DH melden, welche dort mit ihren jeweiligen Bildungsvorschriften registriert werden. Diese Registrierung wird zwischen QM und DH abgestimmt. Dieser Prozess ist in Abbildung 26 dargestellt. Modellierung von Abfragen an die datenhaltenden Quellsysteme sowie das nachgelagerte Datenintegrationszenrutm werden durch die DH durchgeführt, so dass die Kennzahlen durch die Systeme der Klinischen Forschungsplattform berechnet und in einem Speicher hinterlegt werden. Während des Berechnungsprozesse ist je nach Art der Kennzahl eine temporäre Zusammenführung von gespeicherten Daten notwendig; nach der Generierung der Kennzahlen wird die Zusammenführung wieder verworfen. Bei den Kennzahlen handelt es sich größtenteils um Querschnittsinformationen, welche keinen direkten Personenbezug haben. Dieser Prozess ist in Abbildung 24 dargestellt.

Architektur der Transferstelle

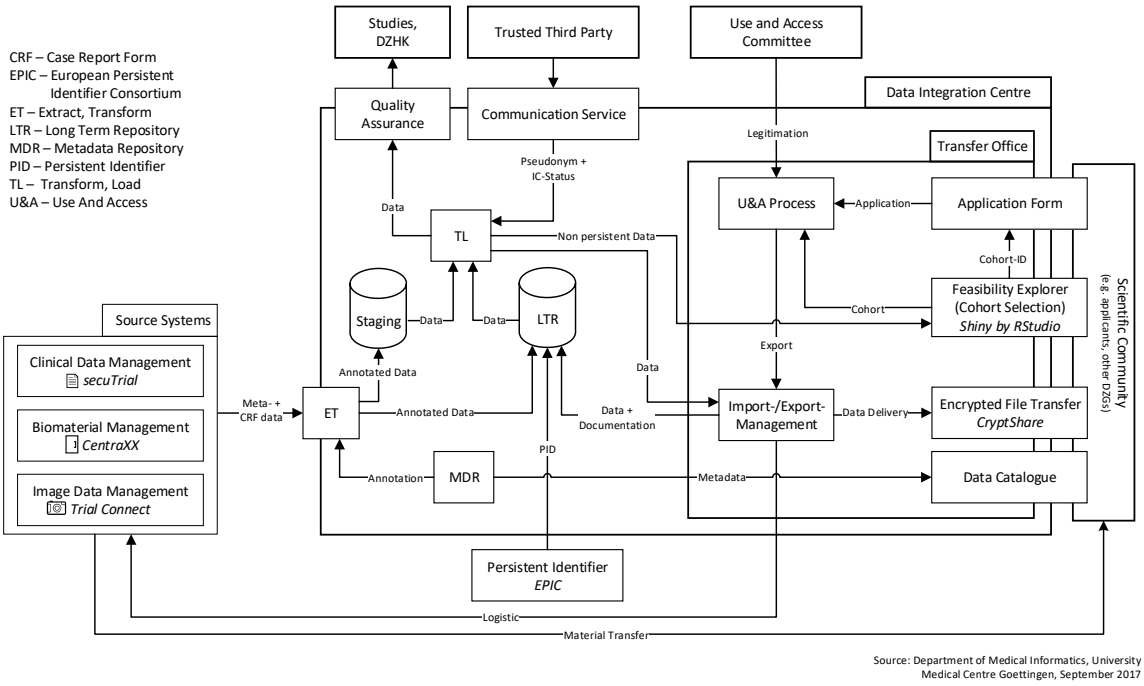
Das zentrale Informationssystem zur Umsetzung der beiden Anwendungsszenarien ist ein modulares Datenintegrationszentrum, welches parallel zu den datenerfassenden Systemen die Aufbereitung und Komposition der zu exportierenden Daten übernimmt. Die Datenverarbeitung innerhalb des Datenintegrationszentrums folgt dem ETL-Muster, also einer sequenziellen **E**xtraktion, **T**ransformation und dem abschliessenden **L**aden der Daten. Dieses Muster wird iterativ je nach Anwendungsfall individuell angepasst und durchgeführt. Aus den verschiedenen Quellsystemen werden die Daten mittels angepasster Exportfilter zunächst exrahiert und zusammengefasst. Hier findet bereits früh im Prozess eine Umpseudonymisierung statt. Die Pseudonyme der Quellsysteme werden an den Treuhänder gesendet und durch die Pseudonyme der Warehouse-Domäne ersetzt. Gleichzeitig werden bereits erste Kennzahlen berechnet. Während des Imports werden die Daten nach Aspekten der Qualitätssicherung von Artefakten bereinigt und harmonisiert. Innerhalb des Datenintegrationszentrums liegen die Datensätze in einem personenzentrierten Schema vor, verteilen sich jedoch auf unterschiedliche Pseudonyme. Auch nach dem Import in das Datenintegrationszentrum liegen die Daten in nicht zusammengeführter Form vor.

Damit die Informationen des Datenintegrationszentrums den Forschenden zugänglich gemacht werden können, müssen die Daten bei Bedarf zusammenführbar sein. Hierzu wird zusammen mit der Treuhandstelle ein Record Linkage durchgeführt. Hierbei werden die Pseudonyme für den Export zusammengestellt und zusammen mit einer formalisierten Beschreibung des Nutzungsvorhabens an den Treuhänder geschickt. Dieser prüft pro Pseudonym, ob die Nutzung durch einen Informed Consent abgedeckt wird und der Datensatz in beabsichtigter Weise verwendet werden darf. Im Anschluss

sendet die Treuhandstelle zu den positiv geprüften Pseudonymen die zugehörigen Linkage-Pseudonyme und sendet diese zurück an die Transferstelle. Die Nutzung der zusammengeführten Daten teilt sich nun nach Einsatzszenario in zwei unterschiedliche Vorgehensweise auf:

1) Im Falle eines Exports für ein Forschungsvorhaben benötigt ein Forscher einen zusammengeführten Export. Ist durch den Treuhänder sichergestellt, dass der:die Studienteilnehmer:in einem solchen Export zugestimmt hat und diese Zustimmung weiterhin gültig ist, so werden die Daten des Datenintegrationszentrums mittels des Record Linkage des Treuhänders zusammengeführt. Für jeden Export werden individuelle Exportpseudonyme erstellt, welche die Pseudonyme aus Datenintegrationszentrum und Record Linkage ersetzen. Dieser Prozess ist in Abbildung 25 dargestellt.

2) Für das Controlling bestimmte Daten werden nun nach den Bildungsvorschriften der registrierten Kennzahlen aufbereitet. Hierfür werden die Daten nur so lange in zusammengeführter Form vorgehalten, wie es für die Berechnung der Kennzahlen notwendig ist. Abschliessend werden die Ergebnisse in eine für analytische Auswertung geeignete Form gebracht. Die Weitergabe wird im Audit-Trail des Datenintegrationszentrums mit Empfänger dokumentiert und es verbleiben keine weiteren Spuren der zusammengeführten Daten aus den verschiedenen Quellsystemen im Datenintegrationszentrum.



Source: Department of Medical Informatics, University Medical Centre Goettingen, September 2017

Abbildung 10: Architektur des Datenintegrationszentrums und der Transferstelle. Innerhalb des Datenintegrationszentrums werden Daten nur temporär zusammengeführt. Die einzige Ausnahme bildet das Long Term Repository, in dem Exporte, die im Rahmen von Nutzungsordnungsprozessen herausgegeben wurden, aufgehoben werden.

2.5 Beteiligte Personengruppen

Folgende Personengruppen der Universitätsmedizin Göttingen sind am Aufbau und bei dem Betrieb der Datenhaltung tätig:

- Mitarbeiter:innen des Geschäftsbereichs Informationstechnologie sind für den reibungslosen Betrieb, die Wartung und die Administration der eingesetzten Infrastruktur (Hard- und Software) verantwortlich
- Mitarbeiter:innen des Instituts für Medizinische Informatik sind für die Entwicklung, Umsetzung und inhaltliche Betreuung des DH-Gesamtkonzeptes sowie seiner Teile zuständig

Keine dieser Personengruppen hat Zugang zu den identifizierenden Daten der gespeicherten Datensätze oder ist in der Lage, diesen Zugang zu erlangen.

3 Technische Systeme

3.1 secuTrial®

Die Bereitstellung eines für den Nutzer komfortabel zu bedienenden aber dennoch allen datenschutzrechtlichen Bedingungen genügenden Datenerfassungswerkzeuges ist die Kernaufgabe der DH. Hierfür wird das Werkzeug secuTrial® verwendet. Mit secuTrial® können multizentrische, klinische Studien und Anwendungsbeobachtungen durchgeführt werden. secuTrial® ermöglicht die direkte, dezentrale elektronische Erfassung von Studiendaten (remote data entry) in eine zentrale Datenbank.

Die Bedienung von secuTrial® ist vollständig browserbasiert, so dass weder für die Administration noch für die Datenerfassung eine Software installiert werden muss. Von jedem internetfähigen PC können von autorisierten Benutzer:innen das Studiensetup definiert, die Teilnehmer:innen verwaltet und die Daten exportiert sowie die Studienteilnehmerdaten eingeben werden.

Innerhalb der Anwendung existiert sowohl ein separater Testbereich, als auch ein produktiver Bereich. So können vor Beginn der eigentlichen Studie oder bei der Implementierung von Änderungen nach der Produktivstellung alle Funktionen getestet werden, bevor sie für die Anwender freigeschaltet werden. Das getestete Studiensetup kann nach erfolgreichen Tests in den Produktivbereich übertragen werden. Alle Änderungen werden stets mitversioniert.

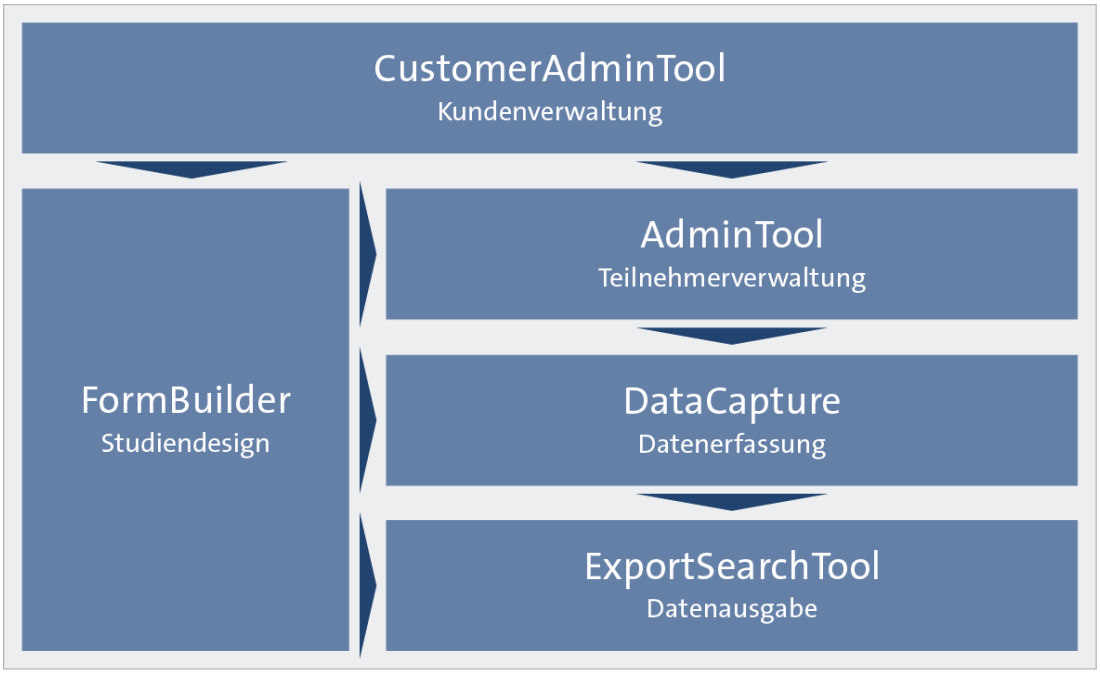


Abbildung 11: Modularer Aufbau von secuTrial®

secuTrial® erfüllt alle regulatorischen Standards und weist alle FDA-konformen Funktionen wie Audit Trail, Rollen- und Rechtekonzept und Elektronische Signatur auf. Zugleich wurde secuTrial® mehrfach unabhängigen Benchmarking-Audits unterzogen und die vollständige Compliance mit 21 CFR Part 11 und den darauf basierenden Bestimmungen attestiert.

Interne Struktur der Anwendung

Innerhalb von secuTrial® gibt es fünf verschiedene Tools, welche gewährleisten, dass spezifische Adminstrationsaufgaben vollständig von operativen Aufgaben der Datenerfasser abgekapselt sind. Diesen modularen Aufbau verdeutlicht Abbildung 11. Das Gesamtsystem besteht aus folgenden einzelnen Modulen:

1. *CustomerAdminTool*
- Funktion: Verwaltung von Kund:innen und Administrator:innen, Anlage von Projekt-Schemata (DB-Bereiche), Generierung der Statistiken, gebündelter Nachrichtenversand, Kontrolle Dateisystem (verwaiste Bilder, temporäre Dateien), Archivierung und Löschung, DB-Dokumenation
- Zugangsprüfung: User in Passwortdatei

2. *FormBuilder*
- Funktion: Anlage und Konfiguration von Projekten, Anlage der Formulare, Projekt-Versionierung, interne Anpassung Datenbank
- Zugangsprüfung: Teilnehmer:innen aus AdminTool-Verwaltung

3. *AdminTool*
- Funktion: Teilnehmer:innen- und Patient:innenverwaltung, Rollen- und Rechteverwaltung, Design-Anpassung, Kundenspezifische Benutzerführung
- Zugangsprüfung: Administrator aus CustomerAdminTool-Verwaltung

4. *DataCapture*

- Funktion: Anlage von Patient:innen, Datenerfassung, Datenübersicht (Reports und Statistiken), Querymanagement, Datenimport
- Zugangsprüfung: Teilnehmer:innen oder Patient:innen (nur bei genutzter Patientenselbst-dokumentation) aus AdminTool-Verwaltung

5. *ExportSearchTool*

- Funktion: Suche nach Studienteilnehmer:innen, Export von Daten
- Zugangsprüfung: Teilnehmer:innen aus AdminTool-Verwaltung

Um den Datenaustausch zwischen secuTrial und weiteren Systemen der Infrastruktur zu ermöglichen, stellt secuTrial® Web-basierte Schnittstellen bereit, um Informationen über das SOAP-Protokoll aus secuTrial® abzurufen bzw. an secuTrial® zu übermitteln. Abrufbare Informationen beziehen sich auf das Studiendesign (bspw. teilnehmende Zentren), Studienteilnehmer:innen und Visitenpläne, sowie Informationen, welche in den eCRF erfasst werden. Da die Systeme der Infrastruktur aufgrund der Trennung in individuelle Pseudonymkreise nicht direkt mit secuTrial kommunizieren können, wurde ein ID-Proxy entwickelt, welcher gemäß der generischen Lösungen der TMF eine Dreieckskommunikation zwischen secuTrial®, Treuhandstelle und einem weiteren System ermöglicht. Bei dieser Methode werden System-spezifische Pseudonyme durch die Treuhandstelle in temporäre Pseudonyme übersetzt, so dass die kommunizierenden Systeme nicht die Pseudonyme des jeweils anderen Systems lernen können. Dieser ID-Proxy ist den secuTrial®-Schnittstellen vorgeschaltet und wird durch die Transferstelle entwickelt und betrieben.

3.2 Warehousing

Das Zusammenführen der verschiedenen Datenquellen wird über eine individuelle Warehouse-Lösung realisiert, bestehend aus einem Datenbankverbund, welcher in einem geschützen Netzsegment des klinischen Rechenzentrums betrieben wird. Das Exportieren der heterogenen Datenbestände aus den jeweiligen Quellsystemen wird in Form von individuell entwickelten ETLStrecken realisiert. Dabei kommen etablierte Integrationswerkzeuge wie Talend Open Studio und R zum Einsatz. Innerhalb des Datenbankverbundes befinden sich somit verschiedene separate und durch technische Maßnahmen wie Verschlüsselung sowie abgestufte Berechtigungsmodelle geschützte relationale Datenbanken. Je nach Anwendungsfall werden die jeweils betroffenen Bestände unter Nutzung einer gesicherten Verbindung zur Treuhandstelle ad hoc verknüpft, indem die entsprechenden Einwilligungsmodule geprüft und die verschiedenen Pseudonyme der Primärsysteme in ein gemeinsames Transferstellenpseudonym übersetzt werden. Die Zusammenführung erfolgt über eine durch die Treuhandstelle bereitgestellte Schnittstelle. Zu Controlling-Zwecken werden so system- und Studienteilnehmer-übergreifende Daten aggregiert und in Form generierter Dokumente und Grafiken der Geschäftstelle zur Verfügung gestellt. Darüber hinaus werden die gemäß Nutzungsordnung beantragbaren Datenbestände des DZHK katalogisiert und auf der offiziellen Webseite ohne Personenbezug zur Übersicht und Filterung dargestellt[22], was es Forschenden ermöglicht eine Machbarkeitsanalyse durchzuführen sowie ein Probandenkollektiv zu spezifizieren und formal zur Nachnutzung gemäß des Use & Access Prozesses zu beantragen. Zu diesem Zweck werden die Daten

[22] DZHK Ressource, Data Catalogue, https://dzhk.de/ressourcen/data-catalogue/

aus der Datenbank heraus in eine eigens entwickelte R-Shiny Anwendung „Feasibility Explorer“[23] geladen, die die Visualisierung in Form einer interaktiven Webseite ermöglicht.

4 Technische und organisatorische Maßnahmen

4.1 Verwendete IT-Infrastruktur

Die für den Betrieb der Systeme benötigten Komponenten (Datenbanksysteme und Anwendungssoftware) befinden sich auf virtuellen Maschinen auf Servern im zugangsgesicherten Serverraum des Geschäftsbereichs Informationstechnologie (G3-7) der Universitätsmedizin Göttingen. Die beschriebenen Systeme (darunter secuTrial®) befinden sich Netzsegment 134er-WissLAN[24] (vgl. Abbildung 12).

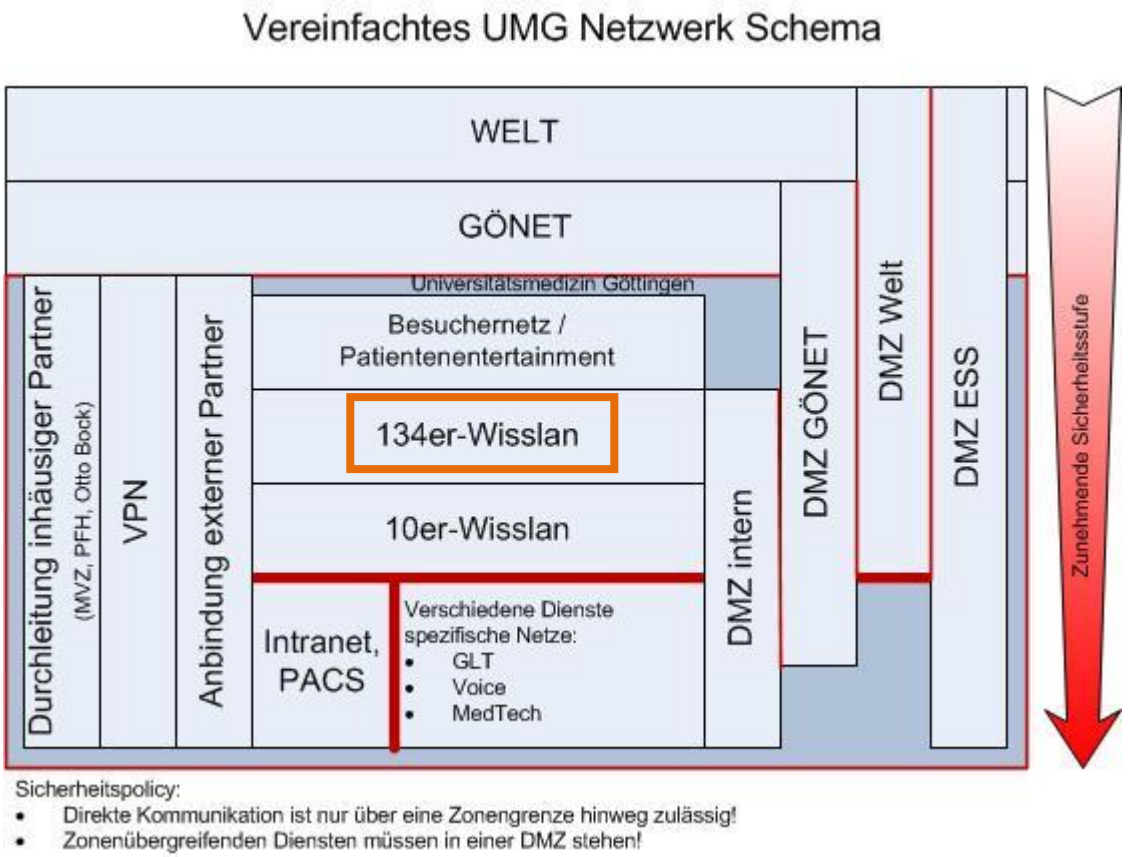


Abbildung 12: Darstellung des derzeitigen Stands der Netzwerkinfrastruktur an der Universitätsmedizin Göttingen: Die Trennung des inneren Segments für die Patientenversorgung (hier Intranet, PACS) von den übrigen Netzsegmenten hat sich bewährt und wird aus Sicherheitsgründen konsequent durchgeführt. Die Infrastruktur der Medizinischen Informatik befindet sich im Netzsegment 134er-WissLAN.

[23] DZHK Ressource, Feasibility Explorer, https://dzhk.de/dzhk-heart-bank/antragstellung/verfuegbarkeitscheck-feasibility-explorer/

[24] Das WissLAN ist ein dediziert für wissenschaftliche Zwecke eingerichtetes Netzsegment innerhalb der Universitätsmedizin Göttingen. Es grenzt sich insbesondere zum PatLAN ab, welches ausschließlich für die Patientenversorgung genutzt wird.

Innerhalb des WissLANs existiert eine dedizierte Forschungsinfrastruktur des Instituts für Medizinische Informatik. Diese ist durch eine zweistufige Firewall vom öffentlichen Teil des WissLANs getrennt und erfüllt damit die Anforderungen des IT-Grundschutzes gemäß BSI-Empfehlung [5]. Die BSI-Maßname *M 4.223 Integration von Proxy-Servern in das Sicherheitsgateway* [7] wurde umgesetzt. Die dedizierte Forschungsinfrastruktur implementiert das Konstrukt des *Reverse-Proxys* der BSI-Maßname *M 4.223,* welche somit Anwendung findet. Die Kommunikation innerhalb des geschützten Netzwerkes findet unverschlüsselt statt. Die äußere Firewall ist als Paketfilter konfiguriert. Der Reverseproxy verschlüsselt die gesamte Kommunikation mit allen öffentlichen Netzen. Die Architektur ist in Abbildung 13 in dargestellt.

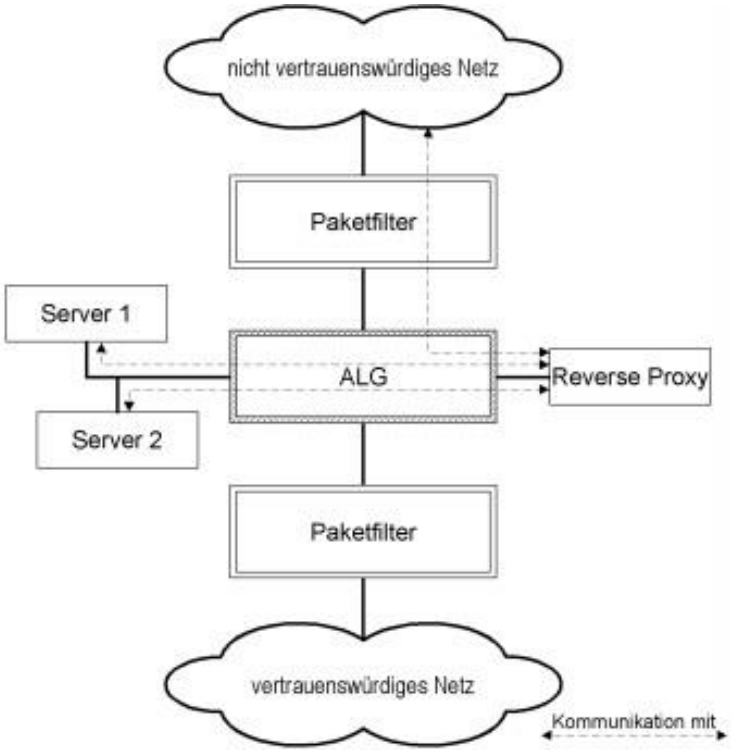


Abbildung 13: Schematische Darstellung der dedizierten Forschungsinfrastruktur. Die Architektur folgt der BSI-Maßname M 4.223 [7].

4.2 Servervirtualisierung

Innerhalb des dedizierten Forschungsnetzes kommen Servervirtualisierungstechnologien zum Einsatz. Diese entsprechen den Empfehlungen des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder [8].

4.3 Schutzbedarfsfeststellung, Datenschutz-Folgeabschätzung

Der für die Datenhaltung und die Transferstelle nötige Schutzbedarf wurde entsprechend den Empfehlungen des BSI und auf Grundlage möglicher Schadensszenarien festgestellt. Grundsätzlich hängt dieser von den Anwendungsfällen, von Datenumfang und Dauer der Datenspeicherung ab.

Innerhalb der Datenhaltung und der Transferstelle werden ausschließlich pseudonymisierte medizinische Daten verarbeitet. Vor diesem Hintergrund wurde eine Risikoanalyse durchgeführt, eine

Datenschutzfolgeabschätzung erstellt und mit dem Datenschutzbeauftragten der Universitätsmedizin Göttingen abgestimmt. Siehe hierzu auch A2.1.

E Labor-Inform.-Management-System (LIMS)

1 Arbeitsabläufe und Datenflüsse

Das vom Bereich Informationstechnologie (IT) der Universitätsmedizin Greifswald betriebene Labor-Informations-Management-System (LIMS) wird im Rahmen von klinischen Forschungsprojekten des DZHK zur Steuerung und Dokumentation der Gewinnung, Verarbeitung, Lagerung und Ausgabe von Bioproben (Bioproben-Management) von Studienteilnehmer:innen verwendet. Als technisches System wird für das LIMS die Software CentraXX der Kairos GmbH verwendet. Zu den typischen Aufgaben des LIMS-Betreibers zählen:

- Bereitstellung und Betrieb des CentraXX-Systems auf geeigneten Servern
- Einbringen von Studien- und Standort-spezifischen Anpassungen und Ergänzungen für die Prozesse des Bioproben-Managements
- Verarbeitung der über CentraXX erfassten Daten unter den durch die Treuhandstelle generierten Pseudonymen

Gemäß der generischen Konzepte zum Datenschutz, welche durch die TMF veröffentlicht wurden, übernimmt der LIMS-Betreiber die Verarbeitung der pseudonymisierten Daten von Bioproben (MDAT) sowie den Betrieb einer dazugehörigen Datenbank [4]. Identifizierende Daten (IDAT) sind zu keinem Zeitpunkt den Softwaresystemen oder den Mitarbeiter:innen des LIMS-Betreibers bekannt.

1.1 Einbindung des LIMS in die Klinische Forschungsplattform des DZHK

Das LIMS ist Teil der Forschungsinfrastruktur des DZHK. Insbesondere die Systeme der Treuhandstelle (THS) und der Datenhaltung (inkl. Transferstelle) sind für die pseudonymisierte Verarbeitung und die Bereitstellung der Daten für die Forschung an das LIMS anzubinden. Durch automatisierte Schnittstellen kann dann ein regelmäßiger Datenaustausch zwischen den Systemen erfolgen.

Anbindung an die THS

Die Anbindung der THS erfolgt über eine automatisierte Server-Schnittstelle. Über diese Schnittstelle werden von der Treuhandstelle Informationen zu Pseudonymen und Informed Consents (Einwilligung, Änderung, Widerruf) an das LIMS gesendet. Das LIMS sendet im Falle eines Consent-Widerrufs eine Information über die vollständige Bearbeitung an die Treuhandstelle.

Die Kommunikation erfolgt über REST-Schnittstellen. In die Kommunikation ist ein Kommunikations-Server der IT der Universitätsmedizin-Greifswald eingebunden. Die Kommunikation zwischen allen beteiligten Systemen erfolgt über TLS 1.2 gesicherte Verbindungen.

Anbindung an die DH (Transferstelle)

Die Anbindung an die DH erfolgt über eine automatisierte Server-Schnittstelle. Über diese Schnittstelle werden von der DH Auslagerungs- und Versand-Aufträge an das LIMS gesendet. Zudem fordert die DH regelmäßig Exporte zu verfügbaren Proben und ggf. Analyse-Ergebnissen an (inkrementelle Änderungen).

Die Kommunikation erfolgt über REST-Schnittstellen. Die Kommunikation zwischen allen beteiligten Systemen erfolgt über TLS 1.2 gesicherte Verbindungen.

1.2 Datenerhebung, -speicherung und -verwaltung

Die Datenerhebung geschieht in den für die jeweilige Studie zuständigen Zentren, welche sowohl in den jeweiligen Förderanträgen als auch in den Studiendesigns benannt sind. Ein Teil der erhebenden Personen hat direkten Kontakt mit den Studienteilnehmer:innen. Die Erhebung der Daten erfolgt üblicherweise durch speziell für die Studien geschulte Personen, z. B. eine Studynurse oder Medizinisch-technischer Laboratoriumsassistent:innen (MTLA). Die Einwilligung von Studienteilnehmer:innen zur Speicherung, Veränderung und Nutzung der zu erhebenden Daten wird im Vorfeld abgefragt und dokumentiert; die Speicherung dieser Einwilligungsinformation erfolgt in der Treuhandstelle (vgl. Studienteilnehmer:innen und Informed Consent anlegen, sowie Informed Consent aktualisieren, Verfahrenbeschreibung und Datenschutzkonzept).

Die Datenerfassung mit Hilfe der Software CentraXX erfolgt durch Eingabe der in der Erhebung abgefragten Items in Eingabemasken (siehe Abbildung 14). In den meisten Fällen wird der Prozess der Datenerhebung parallel mit dem der Datenerfassung durchgeführt. Dies ist jedoch aus technischer Sicht nicht zwingend notwendig. Die erhobenen Daten können auch zunächst auf ausgedruckten Bögen „zwischengespeichert“ sein. Die Erfassung der erhobenen Daten in den bereitgestellten Eingabemasken erfolgt in den meisten Fällen durch eine:n MTLA oder eine:n Studienmitarbeiteri:n (Studynurse). Der Zugriff auf CentraXX sowie deren technische Absicherung wird im Abschnitt Technische und organisatorische Maßnahmen beschrieben. Die auf der Webseite des DZHK-LIMS[25] verfügbaren Kurzanleitungen sowie das entsprechende Schulungsvideo zeigen die Datenerfassung aus Anwendersicht.

[25] https://service4studies.dzhk.de/studienzentren/biobanking/

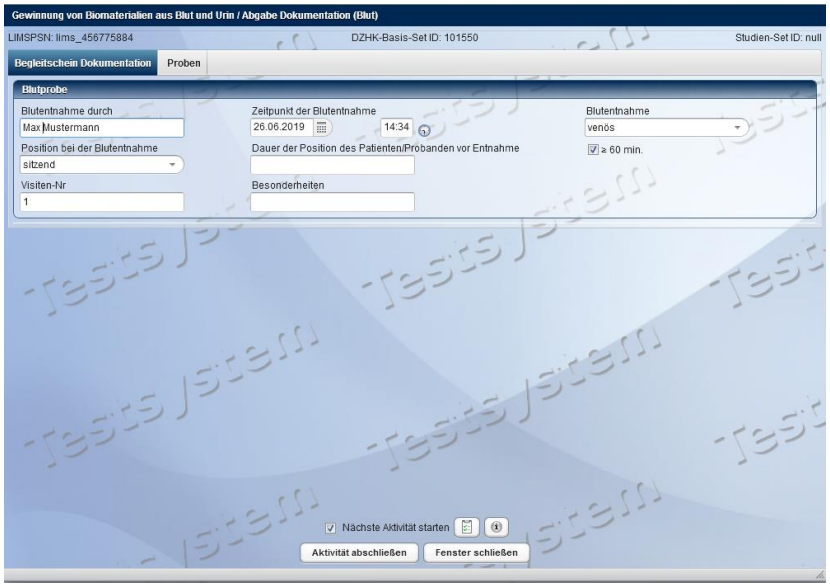


Abbildung 14 Beispiel mit Testdaten für die Eingabe einer Biomaterial-Entnahme über die Dokumentationsmaske in CentraXX

Neben der Bereitstellung geeigneter Erfassungswerkzeuge ist eine Kernaufgabe der Klinischen Forschungsplattform die langfristige Speicherung und Verwaltung der erhobenen Daten. Bereits bei der Datenerfassung wird für den entsprechenden Datensatz ein nicht umgehbarer Audit-Trail in der Datenbank angelegt. Dieser speichert, welche Person (Login-Information in CentraXX) welche Änderung zu welcher Uhrzeit/Datum an welchem Datensatz durchgeführt hat. Somit ist eine lückenlose Versionierung und Nachvollziehbarkeit aller Änderungen gewährleistet.

Eine Einsicht in den Audit-Trail ist für die Systemadministratoren zur Fehlersuche oder -Wiederherstellung notwendig und zulässig. Eine Weitergabe der Audit-Trail-Daten oder daraus abgeleiteter Informationen erfolgt nur mit Zustimmung der betroffenen Personen oder auf richterliche Anordnung hin.

1.3 Benutzer-Verwaltung

Für die Beantragung von Benutzer-Zugängen wird ein Formular verwendet, das alle Systeme der Forschungsinfrastruktur umfasst. Die Einrichtung von Nutzer:innen im DZHK-LIMS erfolgt entsprechend der *SOP-DZHK-LIMS-03*[26] - Informationen zu den Berechtigungen der Nutzer:innen finden sich im Abschnitt 3.4.

1.4 Widerrufs-Abarbeitung

In Abhängigkeit von den Anforderungen der Studie werden zu einer Studienteilnehmer:in im LIMS gespeicherten Daten entweder anonymisiert, gesperrt oder vollständig gelöscht. Die zugehörigen Bioproben werden vor diesem Schritt durch das jeweils lagernde Studienzentrum vernichtet, wenn nicht andere rechtliche Anforderungen vorliegen.

[26] Kann bei Bedarf beim DZHK-LIMS Betreiber angefragt werden.

1.5 Beteiligte Personengruppen

Folgende Personengruppen sind am Aufbau und am Betrieb des LIMS tätig:

- Mitarbeiter:innen des Bereichs Informationstechnologie (IT) der Universitätsmedizin Greifswald sind für folgende Bereiche verantwortlich:
  - ⇨ Betrieb, Wartung und Administration der eingesetzten Infrastruktur (Soft- und Hardware)
  - ⇨ Betrieb, Wartung und Administration der eingesetzten LIMS-Software
- Mitarbeiter:innen der DZHK-Geschäftsstelle sind in folgenden Bereichen tätig:
  - ⇨ Administration der eingesetzten LIMS-Software
  - ⇨ Schulung von Mitarbeiter:innen der Studienzentren (Systembenutzer:innen)

2 Technische Systeme

Das CentraXX-System der Kairos GmbH ist eine Webanwendung zum Studien- und Biobank-Management. Die Anforderungen des DZHK werden durch CentraXX in Form von Systemmodulen, individueller Systemparametrisierung und kundenspezifischer Implementierung abgebildet.

Der modulare Aufbau des CentraXX-Systems umfasst neben den System-Schnittstellen:

- *Biobanking-Modul*: Zur Verwaltung der Daten von Bioproben (Prozessierung, Lagerung, etc.)
- *Messdatenverwaltungs-Modul*: Zur Verwaltung von Messergebnissen, welche aus Bioproben gewonnen wurden
- *Workflow-Engine*: Zur Steuerung von Prozessen der Probengewinnung, Verarbeitung und Lagerung
- *Pseudonymisierte Patientenregistrierung*: Für den Fall eines Ausfalls der Treuhandstelle/ Treuhandstellenanbindung können hierrüber Pseudonyme im LIMS angelegt werden, um eine Arbeitsfähigkeit zu gewährleisten
- *Reporting Modul*: Zur automatisierten Erstellung von Statistiken und Auswertungen der Systemdaten
- *Benutzer- Rechte- und Rollenverwaltung:* Zur feingranularen Steuerung der Zugriffsrechte der einzelnen Personen sowie deren Authentifizierung

2.1 Schutzbedarf

Im LIMS werden ausschließlich pseudonymisierte Daten zu Bioproben von Studienteilnehmer:innen verarbeitet. Bei diesen Daten handelt es sich um Prozessierungs- und Lagerinformationen, sowie ggf. aus den Bioproben gewonnene Analyse-Ergebnisse. Für die Verarbeitung der Daten liegt in der Treuhandstelle ein Informed Consent der Studienteilnehmer:in vor. Siehe hierzu auch A2.1.

2.2 Verzeichnis der Verarbeitungstätigkeiten

Ein Verzeichnis wurde erstellt und kann zur Verfügung gestellt werden.

3 Technische und organisatorische Maßnahmen

Die nachfolgend beschriebenen Maßnahmen dienen der Umsetzung von Datensicherheit und Datenschutz innerhalb der für den Betrieb des LIMS genutzten Räumlichkeiten. Da das LIMS zentral für die Studienzentren des DZHK betrieben wird, erfolgt der Zugriff auf das System von Computern der jeweiligen Studienzentren aus. Für diese Computer und die Nutzer:innen sind innerhalb der Studienzentren, durch die Studien oder durch das DZHK entsprechende Maßnahmen zu treffen, um auch auf der Anwenderseite entsprechenden Datenschutz und Datensicherheit gewährleisten zu können.

3.1 Netzwerkschutz

Der Zugriff auf die CentraXX-Webanwendung in den Studienzentren erfolgt über eine TLS1.2 gesicherte HTTPS-Verbindung. Zusätzlich sind die Studienzentren durch einen VPN-Tunnel mit der Universitätsmedizin Greifswald verbunden. Hierüber wird die Kommunikation zwischen dem CentraXX-Anwendungsserver und einem Rackscanner-System im jeweiligen Studienzentrum ermöglicht und abgesichert.

Die CentraXX-Webanwendung und die zugehörige Datenbank werden auf getrennten Servern in separaten Netzen der Universitätsmedizin Greifswald betrieben. Diese Netze sind sowohl nach außen als auch untereinander über restriktiv konfigurierte Firewalls mit Deep Packet Inspection voneinander getrennt. Zudem wird der Datenverkehr zwischen den Systemen durch Intrusion Detection Systeme auf ungewöhnliche Kommunikationsmuster geprüft.

3.2 Zutrittskontrolle

Der Zutritt zu den Server- und Arbeitsräumen der Universitätsmedizin Greifwald ist durch ein kartenbasiertes Zutrittskontrollsystem gesichert. Die Karten sind personalisiert und dienen gleichzeitig als Mitarbeiterausweis. Das Zutrittskontrollsystem wird zentral durch das Dezernat Technik der Universitätsmedizin Greifwald verwaltet. Für die Öffnungsvorgänge werden digitale Protokolle geführt, die in Abstimmung mit der datenschutzbeauftragten Person der Universitätsmedizin Greifswald ggf. ausgewertet werden können.

3.3 Netzwerk- und IT-Infrastruktur

Der Betrieb der für das LIMS verwendeten Software-Systeme erfolgt auf redundant ausgelegten Hardware-Systemen in einer Virtualisierungsumgebung. Dabei sind die physikalischen Rechner auf zwei Serverräume in unterschiedlichen Brandabschnitten aufgeteilt. Die primäre Datenspeicherung erfolgt auf einem Hochverfügbarkeits-SAN (HP 3Par). Zudem werden Backups auf einem SAN-System in einem dritten Serverraum gespeichert. Nachfolgend erfolgt zudem eine regelmäßige Bandsicherung.

Zwischen den Systemen bestehen redundante Netzwerkverbindungen. Durch diese Hardware-Architektur wird eine hohe Ausfallsicherheit bei Hardware-Defekten gewährleistet.

Der Betrieb der Software-Systeme erfolgt in unterschiedlich zugreifbaren Netzwerksegmenten, die untereinander durch Firewalls abgetrennt sind.

Der Betrieb der Software-Systeme, Hardware-Systeme, Netzwerkkompenenten, sowie die Verfügbarkeit und das korrekte Verhalten einzelner Software-Komponenten werden über einen zentralen Monitoring-Server überwacht. Dieser Monitoring-Server ist nur aus dem internen Netz der Universitätsmedizin Greifswald erreichbar.

3.4 Rollen- und studienbasierte Zugriffsrechte

Für die Nutzung des LIMS ist eine Authentifizierung mit Benutzername und Passwort erforderlich. Jeder Benutzer:in können studien- und standortabhängig Rollen zugewiesen werden. Diese Rollen ermöglichen den Zugriff auf die vom jeweiligen Benutzer benötigten Funktionen des Systems. Zusätzlich zu den operativen Rollen Studynurse und MTLA gibt es eine Administratoren-Rolle.

Die Berechtigungen wurden in Zusammenarbeit mit Expert:innen des Systemherstellers erstellt, um eine bestmögliche Abbildung der benötigten Funktionalität bei gleichzeitiger weitestgehender Einschränkung zu erhalten.

3.5 Protokollierung von Zugriffen und Änderungen (Audit-Trail)

Die Zugriffe und Änderungen der Daten werden detailliert in einem Audit-Trail des CentraXX-Systems gespeichert. Ein Zugriff auf diese Daten ist nur für Systemadministrator:innen möglich, die besonders auf den Datenschutz dieser personenbezogenen Mitarbeiterdaten verpflichtet sind. Eine Verwendung dieser Daten ist nur zu Zwecken der Analyse in Fehlerfällen oder bei Vorliegen einer richterlichen Anordnung zulässig.

Eine Löschung der Audit-Trail Informationen wird aufgrund der Anforderungen an die Nachverfolgbarkeit in klinischen Studien nicht vorgenommen.

3.6 Personelle Maßnahmen

Die Mitarbeiter:innen des Bereichs IT der Universitätsmedizin Greifswald werden bei Einstellung und in regelmäßigen Abständen mündlich und schriftlich auf die Vorschriften des Datenschutzes im Rahmen ihrer Tätigkeit belehrt.

F Bilddatenmanagement (BDMS)

1 Arbeitsabläufe und Datenflüsse

Das BDMS besteht aus einem Betreiber und zwei vom DZHK beauftragte Stellen: Die eine beauftragte Stelle ist am Institut für kardiovaskuläre computer-assistierte Medizin an der Charité – Universitätsmedizin Berlin angesiedelt und verantwortet die technische Koordination (TK) zwischen dem Betreiber, den anderen Infrastrukturteilen (THS, DH, Transferstelle) und den Studienzentren. Die zweite Stelle ist an der Klinik und Poliklinik für Radiologie der Ludwig Maximilian Universität in München verortet und überwacht die Datenqualität im BDMS (QM) und übernimmt die Nutzerverwaltung und -schulung.

Das BDMS stellt einen Service für klinische DZHK-Studien bereit und steht für notwendige Prozesse im Austausch mit anderen Infrastruktursystemen (siehe Abbildung 15). Der Service dient zum einen den Studien als Service, aber gleichzeitig auch als Datenverwaltung für eine Datennachnutzung im Rahmen des Use-and-Access-Prozesses (siehe Abschnitt D2.4).

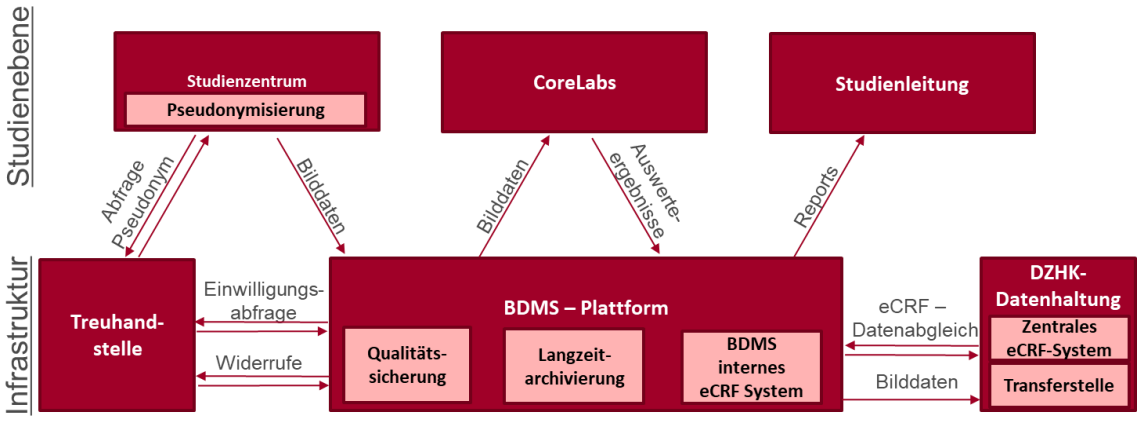


Abbildung 15 Einbindung des BDMS in die Studien und Infrastruktur. Der Austausch der Informationen zwischen den Stellen erfolgt ausschließlich über verschlüsselte Verbindungen mittels Token oder IDs der THS für die Datenzuordnung. Ein tokenbasierter Datentransfer erfolgt mit der Datenhaltung, welche die Token über die THS auflöst. Für die Datenherausgabe über die Transferstelle werden die Bilddaten vor Bereitstellung bereits im BDMS mit bereitgestellten Transfer-PSN zweitpseudonymisiert.

Zu den Aufgaben des Betreibers gehören:

- Bereitstellung und Betrieb der Bilddatenbank Trialconnect auf geeigneten Servern
- Verarbeitung der über Trialconnect erfassten Bilddaten und bilddatenbezogenen medizinischen Daten unter den durch die Treuhandstelle generierten Pseudonymen für das BDMS

Weitere unterstützende Maßnahmen werden von den beiden beauftragten Stellen übernommen:

- Überwachung des Betreibers (TK)
- Koordination BDMS spezifische Anpassungen des eCRF mit der Datenhaltung und Studienkonfiguration im BDMS (TK)
- First Level Support für technische Fragen der Studien (TK)

- Durchführen von Nutzerschulungen (QM)
- Erstellung von Reports und Statistiken zur Unterstützung von Qualitätsmanagement- und Controllingprozessen (QM)
- Export von Daten aus der Studiendatenbank zur Weitergabe an die für die Studienauswertung zuständige Stelle oder zur Weitergabe an die Transferstelle im Rahmen von Nutzungsordnungsprozessen (TK)

Gemäß der generischen Konzepte zum Datenschutz, welche durch die TMF veröffentlicht wurden, übernimmt das BDMS die Verarbeitung der bereits pseudonymisierten Bilddaten (BDAT) und einem Minimalsatz bildbezogenen medizinischen Daten (MDAT) [4]. Identifizierende Daten (IDAT) sind zu keinem Zeitpunkt dem Betreiber oder den beauftragten Stellen im BDMS bekannt.

Ausgangspunkt der Prozessdarstellung ist eine Visite einer Studienteilnehmer:in bei der Daten erhoben werden. Je nach Datentyp werden diese in die Systeme der Infrastruktur eingespielt. Ins BDMS werden die Bilddaten vom Studienzentrum eingespielt (siehe Abschnitt F1.2). Anschließend werden die Bilddaten von der Qualitätssicherung der jeweiligen Studie zur Auswertung freigegeben (siehe Abschnitt F1.3). Die Auswertung erfolgt in dezentralen studienspezifischen CoreLabs, die aus den Bilddaten weitere Messwerte ermitteln (siehe Abschnitt F1.3). Dabei ist es mitunter erforderlich, Daten aus dem Datenhaltungssystem über das BDMS dem CoreLab zur Verfügung zu stellen, um Parameter aus den Messdaten und den MDATs zu bilden. Alle von den CoreLabs berechneten Werte werden in eCRFs im BDMS erfasst und an die Datenhaltung als eCRF-führendes System weitergeleitet. Diese Studienprozesse werden durch Hintergrundprozesse unterstützt, welche die Informelle Trennung der Pseudonyme für die Studien sicherstellen und die Verarbeitungsrechte im Studienplan des:der Studienteilnehmer:in entsprechend dem aktuellen Consent der THS (siehe Abschnitt F1.1) ermöglichen.

1.1 Aufruf des Patientenvisitenplans

Die BDMS-Nutzer:innen arbeiten im BDMS-Pseudonymkreis des:der jeweiligen Studienteilnehmer:in, die von der THS vergeben werden. Die Nutzer:innen wählen einzelne Studienteilnehmer:innen entweder über die Kenntnis des Pseudonyms aus (siehe Abbildung 16 links) oder oder alternativ über deren identifizierende Daten. Für den Weg über identifizierende Daten wird ein eingebettetes iFrame der THS (siehe Abbildung 16 rechts) eingeblendet und von dem:der Benutzer:in ausgefüllt. Nach Abschluss übermittelt die THS die dazugehörige BDMS-ID ans BDMS und dem:der Nutzer:in wird der Visitenplan dargestellt. Die eingegebenen Daten werden über eine getunnelte Verbindung zwischen Rechnern des:der Nutzer:in und der THS verschlüsselt ausgetauscht, sodass das BDMS keinen Zugriff auf die Informationen hat.

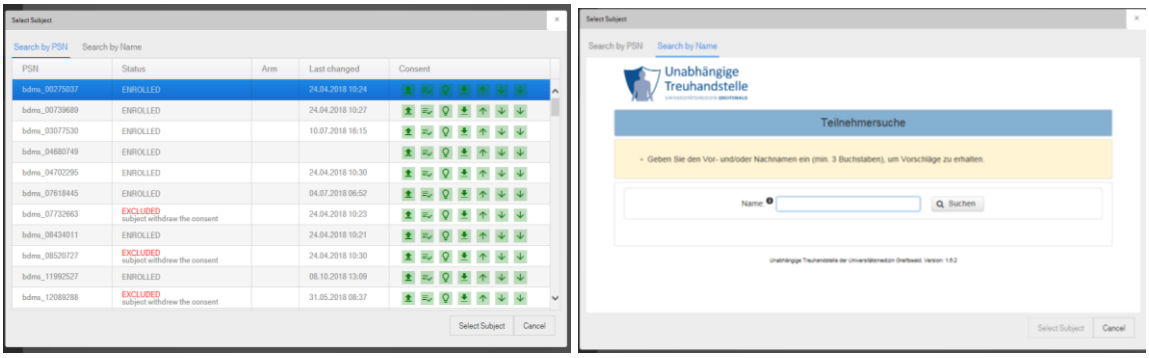


Abbildung 16: Auswahl einer:s Studienteilnehmer:in anhand eines Pseudonyms (Search by PSN) (links) oder über das Treuhandstellenformular (Search by Name) (rechts). In der Übersicht im linken Bild werden die Consent-Events (grüne Symbole) aller Studienteilnehmer:innen für die Nutzer:innen sichtbar. Diese Events werden mindestens einmal täglich aktualisiert und führen bei nicht gesetzten Event zur Einschränkung der Datennutzung im BDMS.

In der Übersicht (siehe Abbildung 16 links) wird durch Icons auch der Konsentstatus dargestellt, der sich aus der Einwilligung der Studienteilnehmer:innen ableitet. Die dazugehörigen modularen Policies – hier: Konsentstati - (bdat_upload, bdat_qs, bdat_analysis, bdat_download_only, mdat_uplad, mdat_download, mdat_download_principle_investigator) werden in der THS verwaltet und im BDMS den Nutzer:innen dargestellt. Die Konsentstati haben nicht nur informativen Charakter, sondern schränken auch die Funktionen im BDMS ein. So kann bei fehlendem Status bdat_upload kein Hochladen von DICOM-Daten erfolgen und beim fehlenden Status bdat_download_only können vorhandene Bilddaten nicht aus dem System heruntergeladen werden. Mit dem Status bdat_analysis ist es nur möglich, die Bilddaten innerhalb der Cloudlösung zu betrachten.

Sofern der Status mdat_download positiv ist, wird eine Synchronisation der für BDMS-Nutzer:innen relevanten medizinischen eCRFs aus der DH abgefragt und in den Formularen lesend dargestellt. Der Umfang der synchronisierten Daten wird durch Rechtevergabe im DH-System gesetzt und auf die notwendigen Informationen für die Erfüllung der Aufgaben im CoreLab und der notwendigen Studieninformationen (Studienzentren, Studienteilnehmer:in, Visitenplaninformationen) begrenzt, (siehe Abbildung 17).

Für einen Austauschvorgang wird eine Anfrage vom BDMS ans DH-System initiiert, indem zunächst von der THS ein Token[27] zum:zur Studienteilnehmer:in abgefragt wird. Dieser Token wird an das DH-System gesendet und dort über eine Auskunftsanfrage bei der THS in die entsprechende pheno-ID überführt und die Antwort unter Angabe des Tokens an das BDMS zurückgesendet. Der Datenfluss ist in Abbildung 27 dargestellt. Mit diesem ID-Austausch werden auch bildbezogene MDATs an das DH-System versendet.

[27] Token - Sitzungskennung, session ID

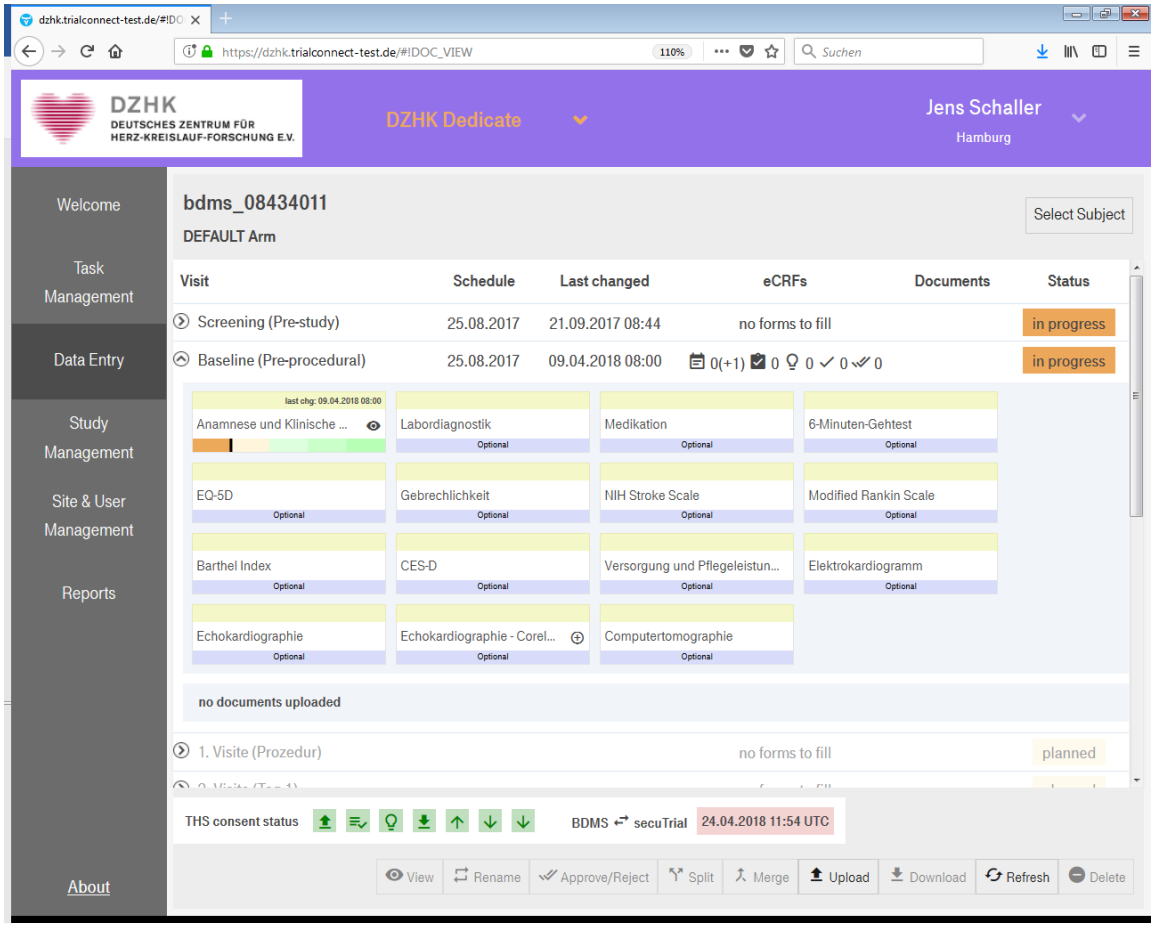


Abbildung 17: Geöffnetes Studiendesign mit den Rechten für Studienleitungen (erkennbar an der linken Navigationsleiste). Das Studiendesign ist im grauen Teil dargestellt und ist unterteilt in Visiten (Screening, Baseline, …) mit den symbolisierten eCRF Formularen. Im unteren Teil ist der Konsentstatus einer teilnehmenden Person dargestellt, der von der THS bei jedem Aufruf abgefragt wird.

1.2 Hochladen von DICOM-Daten

Das BDMS akzeptiert ausschließlich Dateien im DICOM-Format. In diesem Format werden neben den eigentlichen Daten (Bilddaten, EKG-Signale) noch Metainformationen in standardisierten (*Patientennamen, Geburtsdatum, Geschlecht, Aufnahmeeinstellungen, Klinikadressen, behandelnde:r Arzt:Ärztin*) und nicht-standardisierten Feldern (*Private Tags*) erfasst.

Nach Empfehlungen der NEMA[28] zu Pseudonymisierungsprofilen in klinischen Studien wurde ein DZHK Pseudonymisierungsprofil definiert. Das von der NEMA definierte Basic Profile [9] ist um weitere DICOM-TAGs zum DZHK-Profil anhand der Ergänzungsprofilvorschläge der NEMA ergänzt worden (siehe Anlagen: I.9). Maßgeblich für die Entscheidung waren dabei die durchführbaren Pseudonymisierungsautomatisierungen der Software (Ersetzen von DICOM Tags) und der Erhalt der unspezifischen Datenauswertbarkeit in nachgelagerten Prozessen. Identifizierende Daten in den eigentlichen Daten (Bilddaten) (z. B. als in den Rastergrafiken abgelegte „eingebrannte“ Informationen) werden mit diesem Profil nicht entfernt und müssen in Verantwortung der

[28] National Electrical Manufacturers Association (NEMA)

Studienzentren in vorgelagerten Prozessschritten entfernt werden, so wie es auch in nicht BDMS-unterstützten Studien praktiziert werden muss.

Während des Prozesses werden in den Metainformationen im Feld *Patientenname* das von der THS festgelegte Pseudonym eingetragen. Somit wird bereits beim Upload auf pseudonymisierte Daten systemseitig abgezielt (siehe Abbildung 18).

Es ist vorgesehen, dass einzelne Zentren einen Uploadserver innerhalb ihres gesicherten Bereiches betreiben, der sich als Upload-Puffer zwischen den Nutzer:innen und dem Zentralsystem befindet. Zum einen werden die Prozesse für Benutzer:innen schneller abgeschlossen. Zum anderen sollen standort- und gerätespezifische Profile in Verantwortung der Kliniken definiert werden. Die Schwärzung wird aber auch hier BDMS-seitig nicht unterstützt.

Die Datenflüsse sind in Abbildung 28 dargestellt.

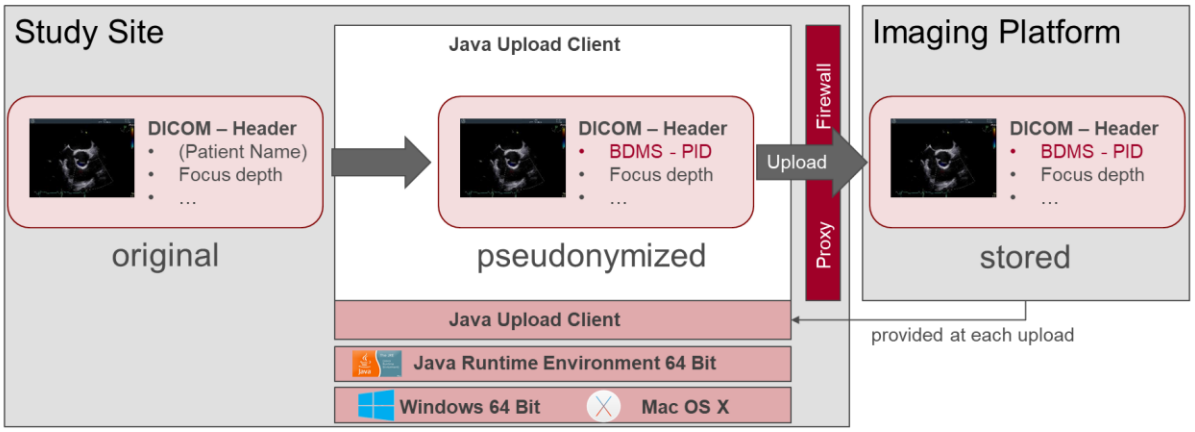


Abbildung 18 Schema des Pseudonymisierungsprozesses. Das DICOM-Object in der jeweils vorliegenden Version wird durch einen JAVA-Upload-Client anhand des BDMS-Profils pseudonymisiert bevor es aus dem Bereich des Studienzentrums durch den Client an die BDMS-Plattform geschickt wird.

Die Daten werden zunächst für die Weiterverarbeitung von einer Stelle der Studie geprüft und bei gegebener Qualität für die weitere Analyse als geeignet markiert, womit die Daten für Löschvorgänge durch Studiennutzer:innen gesperrt werden.

Die Analyse der Daten wird von zentralisierten Stellen der einzelnen Studien (CoreLabs) durchgeführt. Typischerweise werden dazu die DICOM-Daten heruntergeladen und temporär für die Zeit der Auswertung in Verantwortung der CoreLabs zwischengespeichert. Das BDMS bietet auch basale Online-Auswertemöglichkeiten, die derzeit die eingesetzten Analyseprogramme nicht vollständig ersetzen können. Die erhobenen Mess- und Kennwerte sind über das BDMS-Pseudonym den Studienteilnehmer:innen zugeordnet und werden daher in ein eCRF im BDMS erfasst. Sobald die Daten signiert wurden, werden sie auch in das MDAT-System der DH übertragen, damit für die Studien eine Gesamtanalyse der Daten in dem ID-Bereich der Datenhaltung möglich wird. Die Übertragung der Inhalte wird durch das BDMS initiiert; eine Darstellung der Datenflüsse ist in Abbildung 28 dargestellt.

1.3 Datenspeicherung und Datenverwaltung

Die Datenspeichung und Datenverwaltung erfolgt beim Betreiber. Sämtliche Änderungen am Datenbestand und Zugriffe werden im Audittrail analog den Spezifikationen der Datenhaltung (siehe

Abschnitt D2.3) erfasst. Dazu gehören auch die Dokumentation von Queries an den vorangegangenen Stellen der Prozesskette.

Die studienübergreifende Qualitätssicherung erfolgt nicht durch Studienmitarbeiter:innen, sondern durch den Qualitätsmanagenden des BDMS-Projektes. Dazu werden bei der Studienkonfiguration automatisierte Qualitätschecks erstellt, die beim Dateneingang angewandt werden. Grundsätzlich erfolgt die Qualitätsprüfung studienübergreifend an Einträgen des DICOM-Header.

Für die stichprobenhafte Untersuchung erfolgt auch der Download einzelner DICOM-Dateien, um Qualitätsdefizite manuell zu bewerten und Qualitätskriterien abzuleiten. Es ist geplant, weitere Qualitätsmethoden der eigentlichen Bild-Informationen einzuführen, sobald geeignete Verfahren vorhanden sind.

1.4 Datennachnutzung

Über eine Schnittstelle werden regelmäßig Daten des DICOM-Headers von der Transferstelle abgefragt, die für den Feasiblity-Explorer (siehe Seite 23) verwendet werden. Im Fall eines beantragten Use-and-Access-Prozesses wird an das BDMS eine Liste mit einem Exportauftrag mit Objekt-IDs geschickt, der dann als Prozess beim technischen Koordinator eingeht.

Je nach Anfragezweck wird die Pseudonymisierung weiter verschärft und die für die Datennachnutzung unnötigen Information (z.B. Zeitpunkt der Erfassung) aus den Bilddaten entfernt. Diese Pseudonymisierung und eine Zweitpseudonymisierung mit Transfer-PSN (siehe Abschnitt C1.2) erfolgt durch das BDMS. Die Bilddaten werden vor Herausgabe stichprobenartig auf eingebrannte Informationen geprüft. Sofern die zweitpseudonymisierten Daten herausgegeben werden können und positiv über die Herausgabe entschieden wurde, erhält die Transferstelle einen Link zum Downloadpaket. Im Fall von Nacharbeiten wird ein Datenträger mit den bereinigten Daten der Transferstelle oder den Nachnutzer:innen bereitgestellt.

1.5 Widerruf von Studienteilnehmer:innen

Der Widerruf von Studienteilnehmer:innen erzeugt einen elektronischen Auftrag durch die THS. Mit Eingang des Auftrags werden Zugriffe über die negativen Konsente für den Studienbetrieb unterbunden. Einzig der:die Studienkoordinator:in hat noch Zugriff auf die Daten, sofern es rechtlich notwendig ist. Der:die technische Koordintor:in prüft zeitnah, ob der Widerruf vom BDMS erfolgreich umgesetzt worden ist und bestätigt der THS schriftlich den erfolgten Widerruf. Die Dokumentation erfolgt gemäß der *SOP THS 12* (siehe Anlagen I.6) in der THS.

1.6 Beteiligte Personengruppen und Einrichtungen

Das BDMS wird durch einen Auftragsdatenverarbeiter (derzeit Deutsche Telekom Healtcare Service GmbH) betrieben, der eine kundenangepasste Variante der Software TrialConnect im Auftrag des DZHK e.V. als eine Software-As-A-Service (SAAS) betreibt. Die BDMS-Mitarbeiter:innen mit ihren jeweiligen Fachkenntnissen arbeiten an der Charité – Universitätsmedizin Berlin, Institut für Kardiovaskuläre Computer-assistierte Medizin und an der Ludwig-Maximilians-Universität München, Klinik und Poliklinik für Radiologie und verwalten das BDMS für das DZHK.

Folgende Personengruppen sind am Betrieb und der Weiterentwicklung des BDMS tätig:

Mitarbeiter:innen der Deutschen Telekom Healthcare Services GmbH (DTHS) sind für folgende Bereiche verantwortlich:

- Betrieb, Wartung und Administration der eingesetzten Infrastruktur (Soft- und Hardware)
- Anpassung, Aktualisierung und Wartung der eingesetzten BDMS-Software

IT-Mitarbeiter:innen in den Studienzentren

- Betrieb, Wartung und Administration der geplanten Gateways (Soft- und Hardware)
- Aktualisierung der Gateway-Software
- Erstellen und Einspielen der standortbezogene Pseudonymisierung

BDMS-Teilprojektmitarbeiter:innen sind in folgenden Bereichen tätig:

- Inhaltliche Administration
- Schulung von Mitarbeiter:innen der Studienzentren (Systembenutzer:innen)
- Koordination der Maßnahmen für den Betrieb durch den Betreiber
- Umsetzung BDMS-spezifischer studienvorbereitender Arbeiten
- Überprüfung des Auftragsdatenverarbeiters
- Regelmäßige und anlaßbezogene Prüfungen der Datenqualität

Die Mitarbeiter:innen des Auftragsdatenverarbeiters und die BDMS-Teilprojektmitarbeiter:innen haben keinen Zugang zu den identifizierenden Daten der gespeicherten Datensätze und sind auch nicht in der Lage, diesen Zugang auf legalem Wege zu erlangen. Alle beteiligten Personen am BDMS arbeiten nicht im adminstrativen Bereich der anderen Systeme.

2 Technische Systeme

Das BDMS wird von der Deutschen Telekom Healthcare Services GmbH (DTHS) als Software-As-A-Service (SAAS) betrieben, womit Software, Hardware und deren gemeinsamer Betrieb von der DTHS übernommen werden. Die Software ist eine für die DZHK-Bedarfe angepasste Variante der webbasierten Software TrialConnect.

Der Anbieter ist im Rahmen einer Auftragsdatenverarbeitung an die Anweisungen des DZHK gebunden. Der Betreiber prüft seine TOMs entsprechend dem aktuellen technischen Stand und prüft - wie auch das DZHK - auch auf aktuelle Eignung. Die Eignung der eingesetzten Rechenzentren werden durch gültige Zertifikate nach ISO 27001 regelmäßig nachgewiesen.

Sämtliche Datenübertragungen von personenbezogenen Daten erfolgen unter Nutzung von verschlüsselten Verbindungen dem Stand der Technik entsprechend zwischen den beteiligten Stellen.

3 Schutzbedarf

Im BDMS werden ausschließlich pseudonymisierte Daten zu Bilddaten von Studienteilnehmer:innen verarbeitet. Bei diesen Daten handelt es sich um Bilddaten von inneren Organen, sowie zusätzliche klinische Informationen und von ihnen abgeleitete Analyse-Ergebnisse. Für die Verarbeitung der Daten

liegt in der Treuhandstelle ein Informed Consent der Studienteilnehmer:innen vor. Siehe hierzu auch A2.1.

4 Technische und organisatorische Maßnahmen (TOMs)

Die DTHS setzt als Hardware für die Software die „Dynamic Services for Medium Enterprise Customers“ der T-Systems International GmbH ein. Für die Datensicherung werden die Daten in ein zweites unabhängiges Rechenzentrum regelmäßig übertragen. Sämtliche Services werden auf mindestens gleichwertige Rechenzentren innerhalb Deutschlands erbracht.

Die verwendeten Rechenzentren werden mit Ausrichtung des Kundenkreises der öffentlichen Verwaltung betrieben, der ein hohes Maß an Revisionspflicht im Anwendungskreis des deutschen Grundschutzkataloges des Bundesamts für Sicherheit und Informationstechnik (BSI) unterliegt.

Die Services unterliegen unter anderem Zertifizierungen nach

- ISO 9001 Qualitätsmanagementsysteme
- ISO 20000 Service Management
- ISO 27001 Informationssicherheit Management Systems

Die Rechenzentren sind nach Tier3+ mit einer Verfügbarkeit von 99.982% klassifiziert.

Der Betreiber ist rechtlich im Rahmen einer Auftragsdatenverarbeitung an das DZHK e.V. gebunden und unterliegt somit deren Anweisungen. Die ausführlichen TOMs des Betreibers können auf Anfrage bereitgestellt werden. Die BDMS-Mitarbeiter:innen prüfen regelmäßig die Gültigkeit der genannten Zertifikate des Betreibers und der Datenzentren.

4.1 Netzwerkschutz

Der Zugriff auf die BDMS-Webanwendung in den Studienzentren erfolgt über eine TLS1.2 gesicherte HTTPS-Verbindung, wie auch die Verbindungen zur THS und der Datenhaltung.

4.2 Rollen- und studienbasierte Zugriffsrechte

Für die Nutzung des BDMS ist eine Authentifizierung mit Benutzername und Passwort erforderlich. Allen Benutzer:innen können studien- und standortabhängig Rollen zugewiesen werden. Diese Rollen ermöglichen den Zugriff auf die von Benutzer:innen benötigten Funktionen des Systems. Zusätzlich zu den operativen Rollen *Study* gibt es mehrere Administratoren-Rollen (*Studienadministration, Systemadministration*).

4.3 Protokollierung von Zugriffen und Änderungen (Audit-Trail)

Die Zugriffe und Änderungen der Daten werden detailliert in einem Audit-Trail des TrialConnect-Systems gespeichert. Ein Zugriff auf diese Daten ist nur für Systemadministrator:innen möglich, die besonders auf den Datenschutz dieser personenbezogenen Mitarbeiterdaten verpflichtet sind. Eine Verwendung dieser Daten ist nur zu Zwecken der Analyse in Fehlerfällen oder bei Vorliegen einer richterlichen Anordnung zulässig.

G Anhang

1 Übersicht der in der Treuhandstelle etablierten SOPs und Formulare

Tabelle 7 Übersicht der THS-SOPs

Kennung	Titel	Kurzbeschreibung	DE	EN	Version	Arbeitsversion
Allgemeine DZHK SOPs						
DZHK-SOP-P-05_DE	Widerruf Studienauschluss Kontaktsperre	Verfahrensweise bei einem Widerruf bzw. Studienauschluss im DZHK aus Sicht des Studienzentrums	x		1.8	
DZHK-SOP-P-05_EN	Revocation Study exclusion Contact blocking	siehe DE Version		x		
DZHK-SOP-P-06_DE	Erfassung IDAT Informed Consent	Verfahren zur Erfassung von personen identifizeirenden Daten und Informed Consents in den Weboberflächen des DZHK	x		1.7	
DZHK-SOP-P-06_EN	Aquisition of person identifying data and the IC	siehe DE Version				
DZHK-SOP-P-07_DE	Ticketsystem (extern)	Verfahrensweise bei der Ticketanforderung durch das Studienzentrum	x		1.2	
DZHK-SOP-P-07_EN	Ticketsystem (extern)	siehe DE Version		x		
Kennung	Titel	Kurzbeschreibung	DE	EN	Version	Arbeitsversion
THS interne SOPs						
DZHK-SOP-THS-06_DE	Erstellung Client-Zertifikat	Erstellung eines Client-Zertifikats (THS intern)	x		2.0	
DZHK-SOP-THS-08_DE	Prüfung IC	Verfahrensweise bei der Qualitätsprüfung der angelegten Einweilligungen (THS intern)	x		2.3	
DZHK-SOP-THS-10_DE	Ticketsystem (intern)	Verfahrensweise bei der Ausstellung und Einlösung von Tickets über das Ticketsytem des DZHK (THS intern)	x		1.2	
DZHK-SOP-THS-12_DE	Widerruf (intern)	Verfahrensweise bei der Bearbeitung von Widerrufen innerhalb der DZHK Infrastruktur	x		1.0	x
DZHK-SOP-THS-15_DE	Dubletten IDAT bearbeiten	Verfahrensweise der Anwednungsfälle Dubletten auflösen und ändern von bereits erfassten personenidentifizierenden Daten (THS intern)	x		1.0	x
DZHK-SOP-THS-16	Studienausschluss (intern)	Verfahrensweise bei der Bearbeitung von Studienausschlüssen innerhalb der DZHK Infrastruktur	x		1.0	x
DZHK-SOP-THS-17	IP Filter und Basic Auth intern	Vorgehen bei der Freischaltung von IP Adressen oder aternativ dem Anlegen neuer Nutzer für die Basic Authentification	x		1.0	x

Tabelle 8 Übersicht der in der THS verwendeten Formulare

Kennung	Titel	Kurzbeschreibung	DE	EN	Version	Arbeitsversion	Verwaltung durch Geschäftsstelle
DZHK-FORM-THS-xx-DE	Anforderung Client-Zertifikat - Mobil	Formular für den Basic-Authentification-Login	x		3.3		
DZHK-FORM-THS-xx-DE	Anforderung Client-Zertifikat	Formular für die Anforderung eines Client-Zertifikates	x		3.2		
DZHK-FORM-THS-xx-EN	client certifikate	siehe DE Version (Anforderung Client-Zertifikat)		x	3.2		
DZHK-FORM-THS-xx-DE	Vermerk Einwilligung	Formular client dazu den eindeutigen Wille des Teilnehmers auf dem Informed Consent nicht festzuhalten	x		1.1		
DZHK-FORM-THS-xx-EN	file note to informed consent	siehe DE Version (Vermerk Einwilligung)		x	1.0		
DZHK-FORM-THS-xx-DE	Widerruf Studienzentrum	Formular zum Widerrufen eines Teilnehmers aus einer Studie. Wird vom Studienzentrum ausgefüllt.	x		1.7		
DZHK-FORM-THS-xx-EN	revocation	siehe DE Version (Widerruf Studienzentrum)		x	1.7		
DZHK-FORM-THS-xx-DE	Studienausschluss	Formular für einen Studienausschluss eines Teilnehmers. Wird vom Studienzentrum ausgefüllt.	x		1.1		
DZHK-FORM-THS-xx-EN	deviation	siehe DE Version (Studienausschluss)		x	1.1		
DZHK-FORM-THS-xx-DE	Widerruf/SA Biomaterial für DH	Formular Widerruf/Studienausschluss für Biomaterialen. Wird von der Datenhaltung ausgefüllt.	x		1.1		
DZHK-FORM-THS-xx-DE	Widerruf/SA DH	Formular Widerruf/Studienausschluss für medizinische Daten. Wird von der Datenhaltung ausgefüllt.	x		1.1		
DZHK-FORM-THS-xx-DE	Widerruf Biomaterial für LIMS	Formular Widerruf für Biomaterialen. Wird vom DZHK-LIMS ausgefüllt.	x		1.1		
DZHK-FORM-THS-xx-DE	Auflösung Dubletten	Formular zur Auflösung von mehrfachangelegten Personen im ZDM	x		1.2		
DZHK-FORM-THS-xx-DE	Dokumentation IDAT Änderungen	es wird dokumentiert wer wann welche IDATs in der THS geändert hat	x		1.0	x	
DZHK-FORM-THS-xx-DE	Übersicht WR SA	pro Studie wird dokumentiert wie viele Widerrufe und Studienausschlüsse für die Studienzentren	x		1.0	x	
DZHK-FORM-THS-xx-DE	Berechtigte Personen		x		1.1		x
DZHK-FORM-THS-xx-DE	Meldung zur Aktivierung	Formular zur Aktivierung eines Studienzentrums in der THS	x		1.3		x
DZHK-FORM-THS-xx-EN	Notification for activation	Form for activating a study center in the THS		x	1.3		x

Tabelle 9 Überschrift der THS Anträge und Abnahmeprotokolle

Kennung	Titel	Kurzbeschreibung	DE	EN	Version	Arbeitsversion
DZHK-Protokoll-THS-01-DE	Abnahmeprotokoll THS	Protokoll zum Test der für eine Studie umgesetzten Funktionalitäten, welches vor dem Prodivktivstart an die THS gesendet werden muss	x		1.6	
DZHK-Protokoll-THS-01-EN	System Verification Protocol TTP	siehe DE Version		x	1.6	
DZHK-Protokoll-THS-02-DE	Abnahmeprotokoll Basic Authentication	Protokoll (mit Basic-Authentification) welches vor dem Prodivktivstart an die THS gesendet werden muss	x		1.0	
	Funktionsprüfung secuTrial	THS internes Protokoll zur Funktionsprüfung der Schnittstelle zu secuTrial	x		2.0	
	Funktionsprüfung DZHK-LIMS	THS internes Protokoll zur Funktionsprüfung der Schnittstelle zu DZHK-LIMS	x		1.0	x
	Funktionsprüfung BDMS	THS internes Protokoll zur Funktionsprüfung der Schnittstelle zu BDMS	x		1.0	x

Tabelle 10 Übersicht der durch die THS bereitgestellten Anleitungen und Info-Blätter

Kennung	Titel	Kurzbeschreibung	DE	EN	Version	Arbeitsversion
DZHK-Anleitung-THS-01-DE	Informationsblatt für Client-Zertifikat und secuTrial	Informationsblatt zur Installation und Verwendung von Client-Zertifikaten	x		1.1	
DZHK-Anleitung-THS-01-EN	Information Sheet Client Certificate and secuTrial	siehe DE Version		x	1.1	
DZHK-Anleitung-THS-03-DE	Informationsblatt IC-Prüfung	Informationblatt für die Studienmitarbeiter, das die Bearbeitung des IC-Prüfberichtes erklärt	x		1.0	
DZHK-Anleitung-THS-03-EN	IC-Verification Information Sheet	siehe DE Version		x	1.1	
DZHK-Anleitung-THS-xx-DE	Suche im gICS, gPAS und EPIX	beschreibt Verfahrensweise der THS mit dem gICS, gPAS und E-PIX. (THS intern)	x		1.0	x
DZHK-Anleitung-THS-xx-DE	Handbuch TrackingSystem_Technik	beschreibt den rechnischen Umgang mit dem Tracking System (THS intern)	x		1.0	x
DZHK-Anleitung-THS-xx-DE	Handbuch QS IC	beschreibt die Qualitätssicherung der Informed Consents (THS intern)	x		1.0	
DZHK-Anleitung-THS-xx-DE	Informationsblatt Auflösung Dubletten	beschreibt die Auflösung von Dubletten für die Studienzentren	x		1.1	
DZHK-Anleitung-THS-xx-EN	clarification of multiple registered participants	siehe DE Version		x	1.0	x
DZHK-Anleitung-THS-xx-DE	Einführung Tracking System_Workflows	beschreibt den Umgang mit dem DZHK Trackingsystem (THS-intern)	x		1.0	x

2 Abbildungen

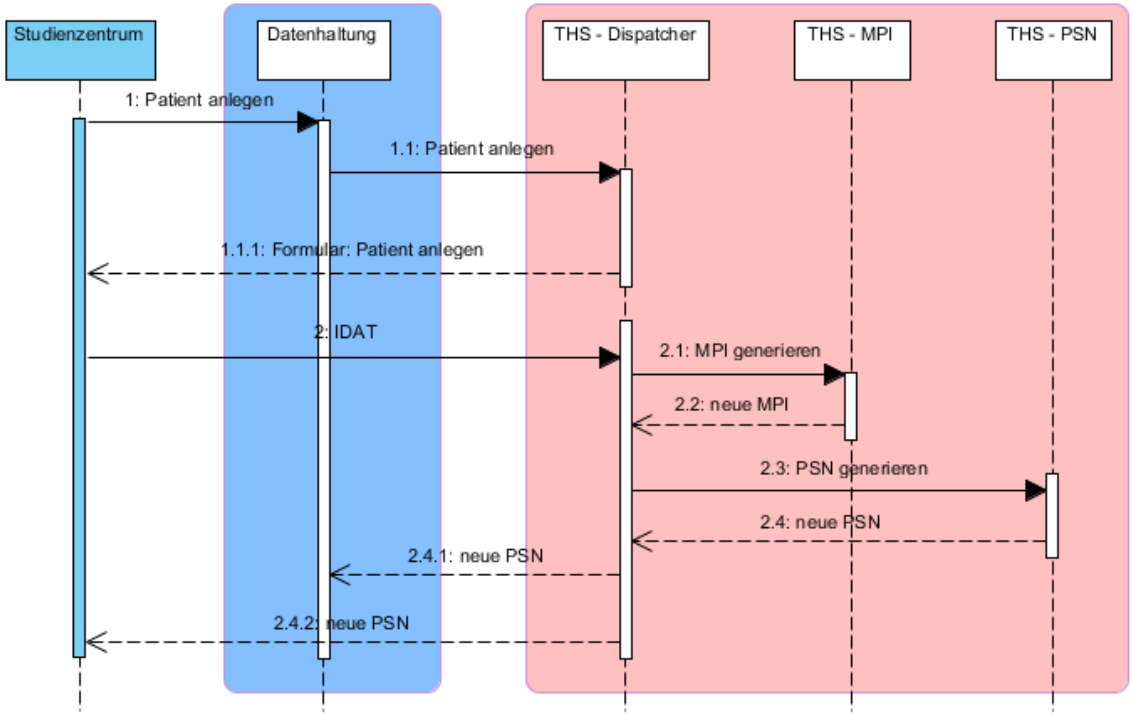


Abbildung 19 Studienteilnehmer anlegen (Technische Sicht)

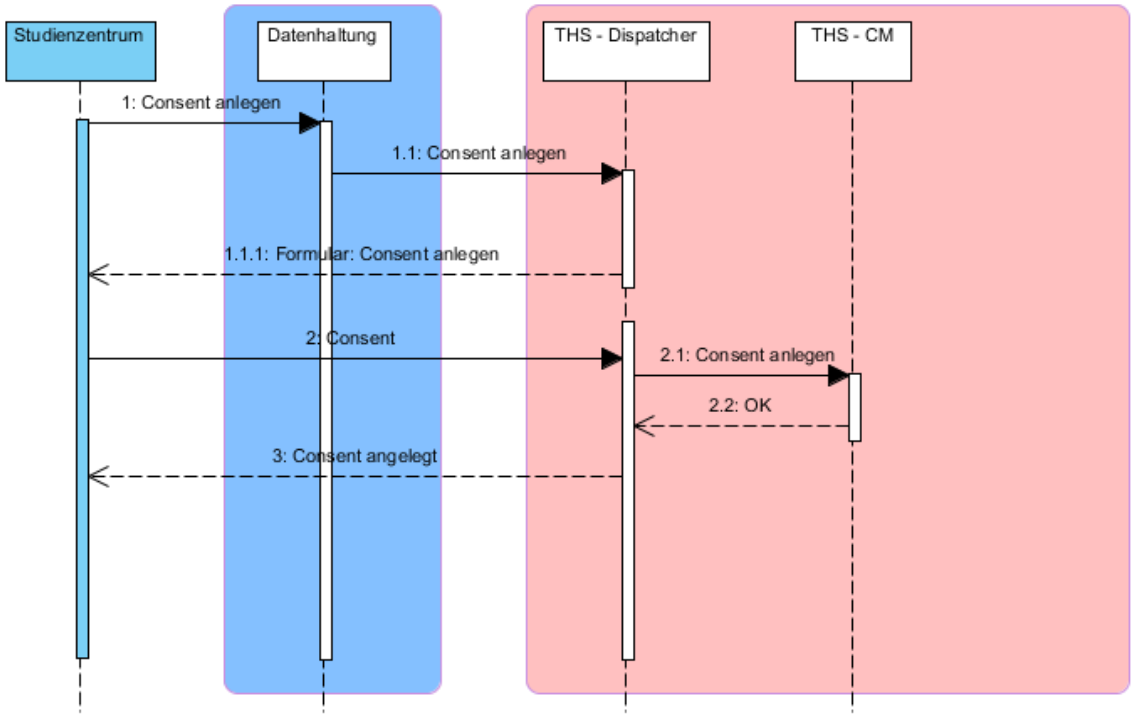


Abbildung 20 IC anlegen (Technische Sicht)

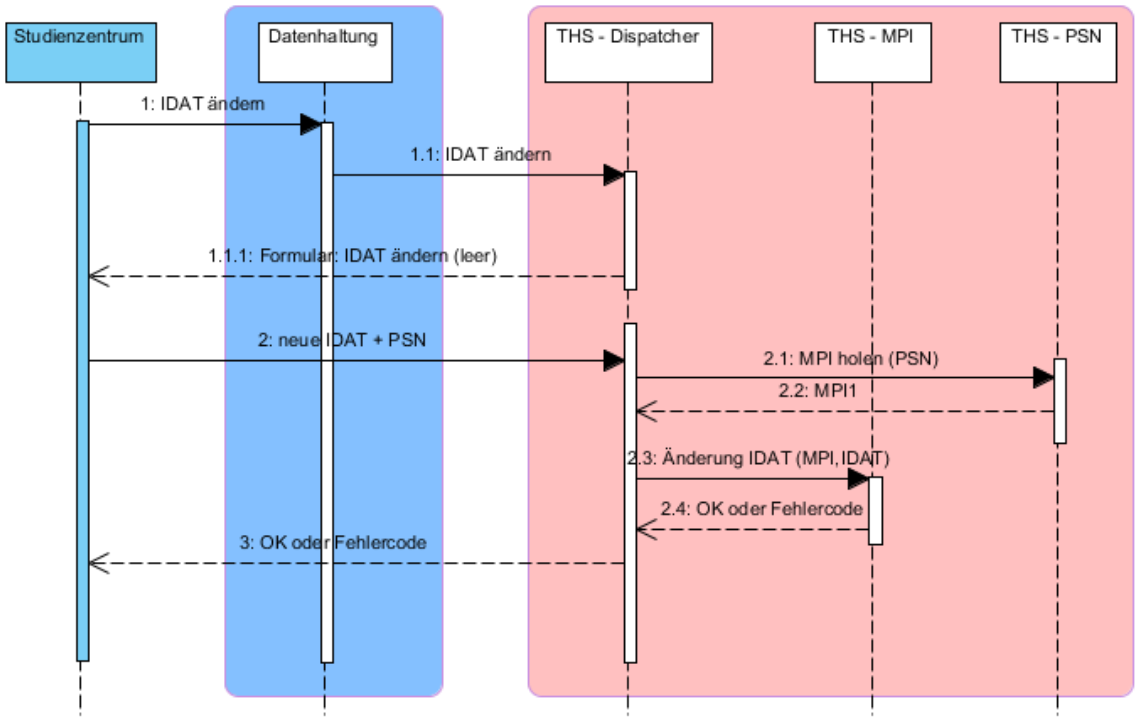


Abbildung 21 IDAT ändern (Technische Sicht)

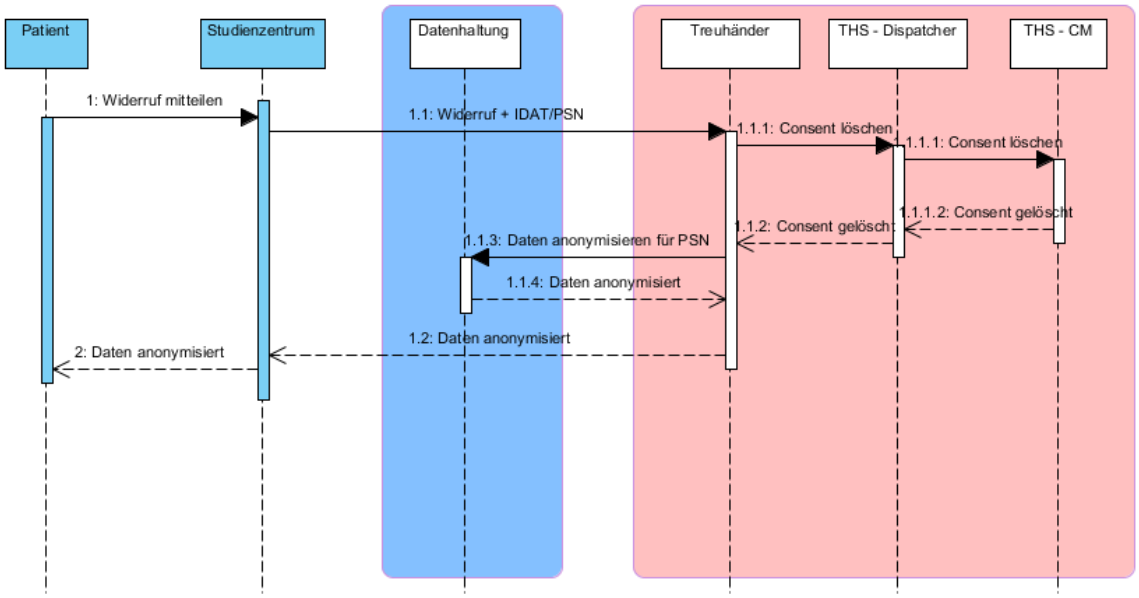


Abbildung 22 Widerruf (Technische Sicht)

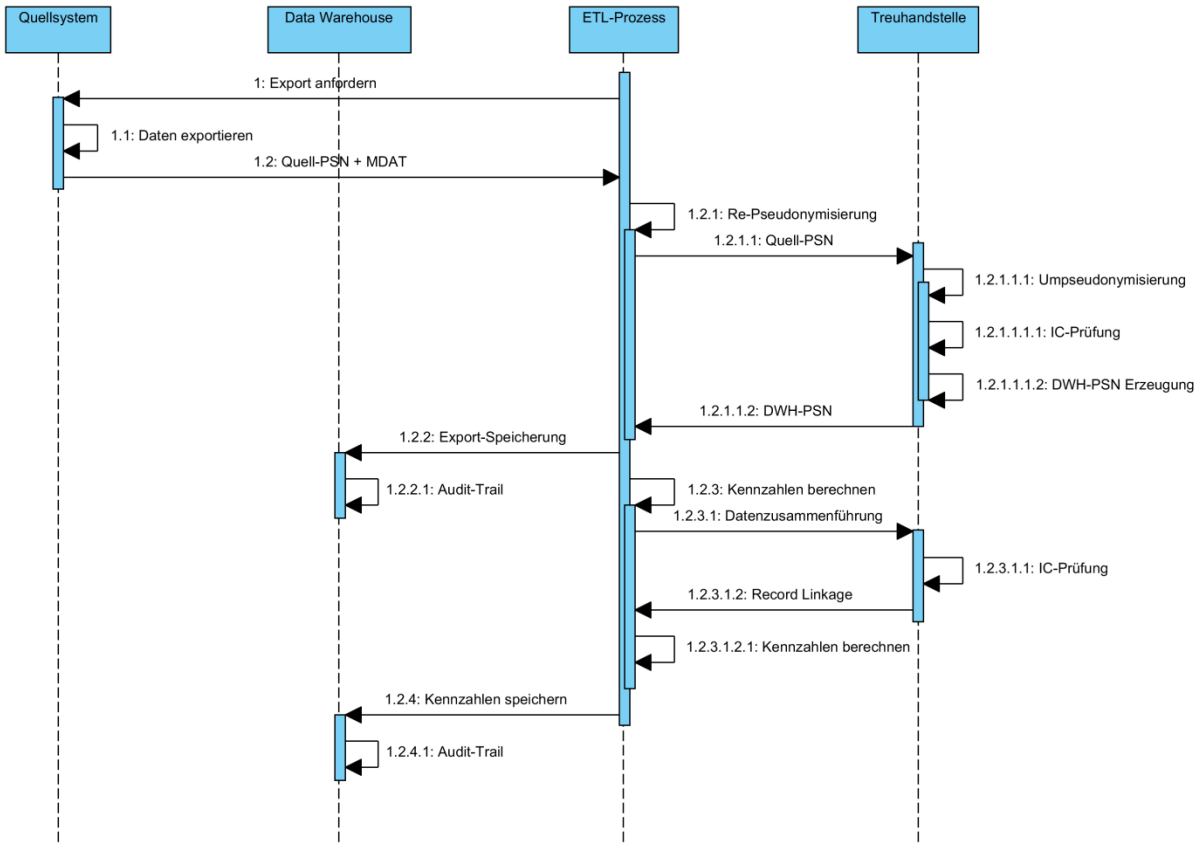


Abbildung 23: Technischer Ablauf des Exports und der Re-Pseudonymisierung medizinischer Daten aus einem Quellsystem (z.B. secuTrial®) mit angeschlossenem ETL-Prozess und Interaktion mit der Treuhandstelle.

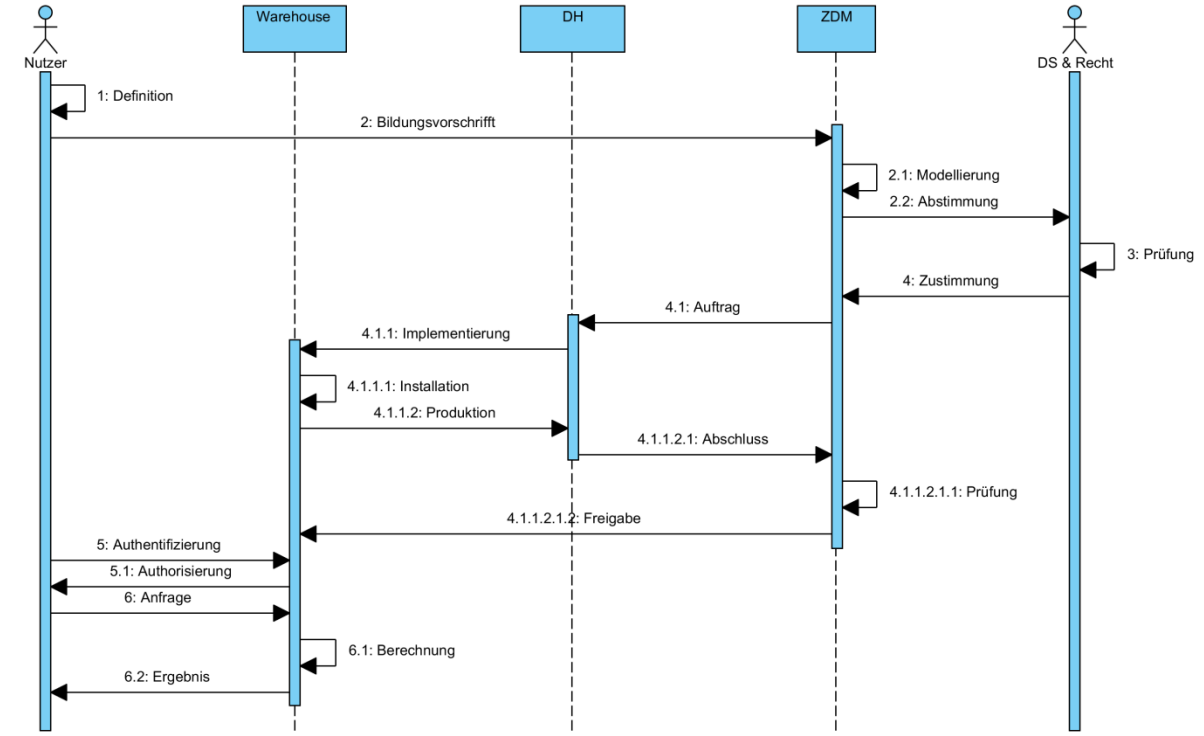


Abbildung 24: Organisatorischer Ablauf zur Registrierung und Nutzung von Qualitätsmanagement-Kennzahlen.

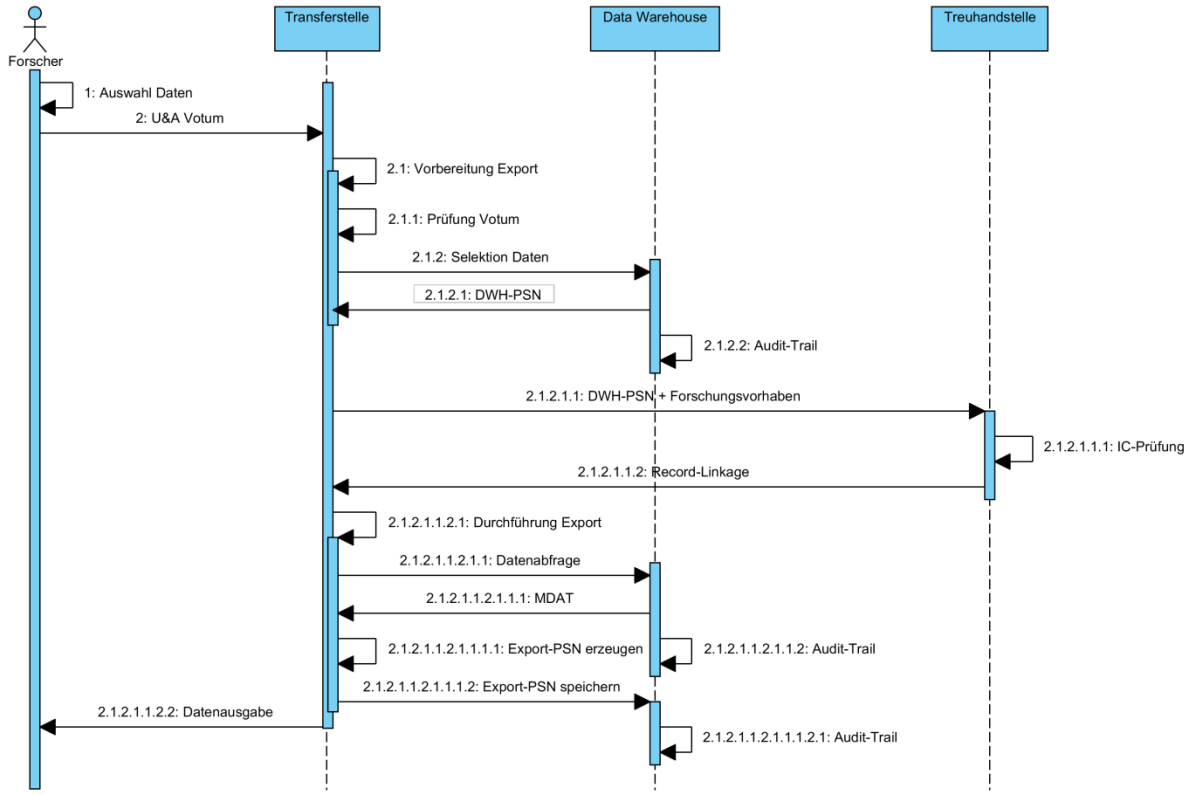


Abbildung 25: Technischer Ablauf zum Abrufen pseudonymisierter medizinischer Daten über die Transferstelle.

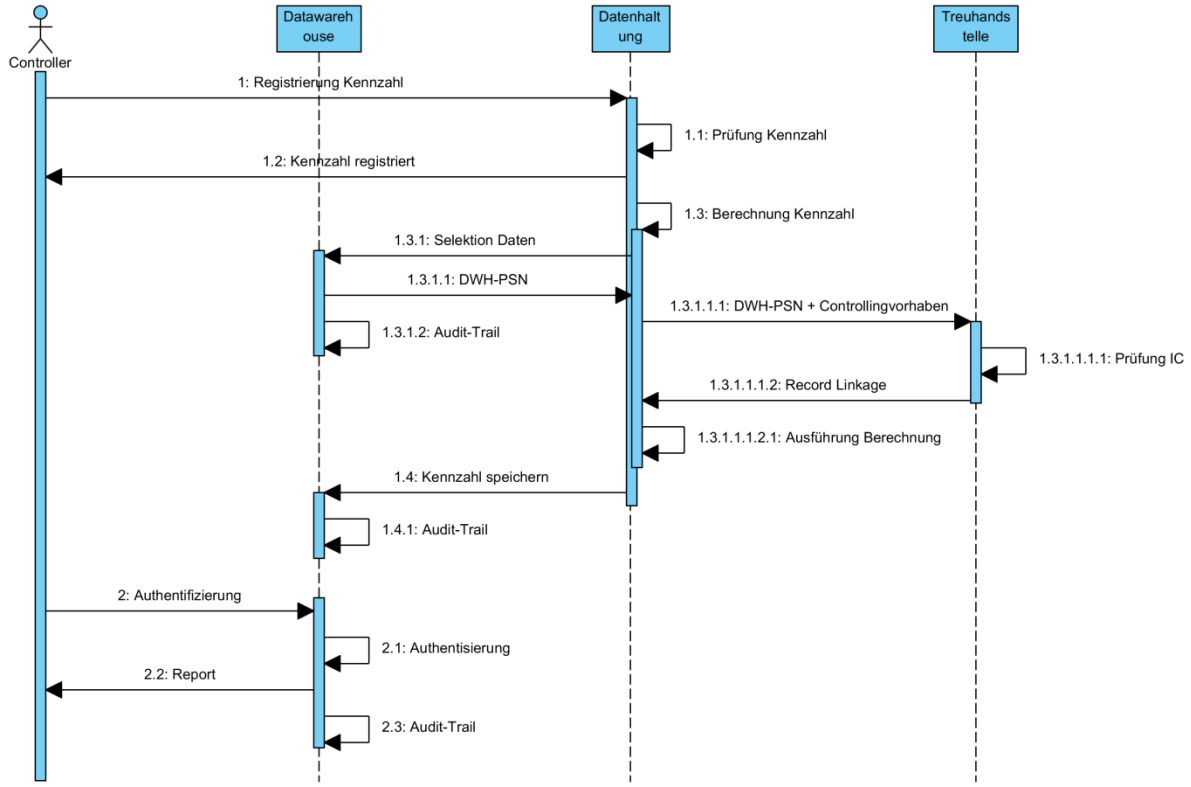


Abbildung 26: Technischer Ablauf zum Abrufen von Qualitätsmanagement-Berichten durch das Controlling.

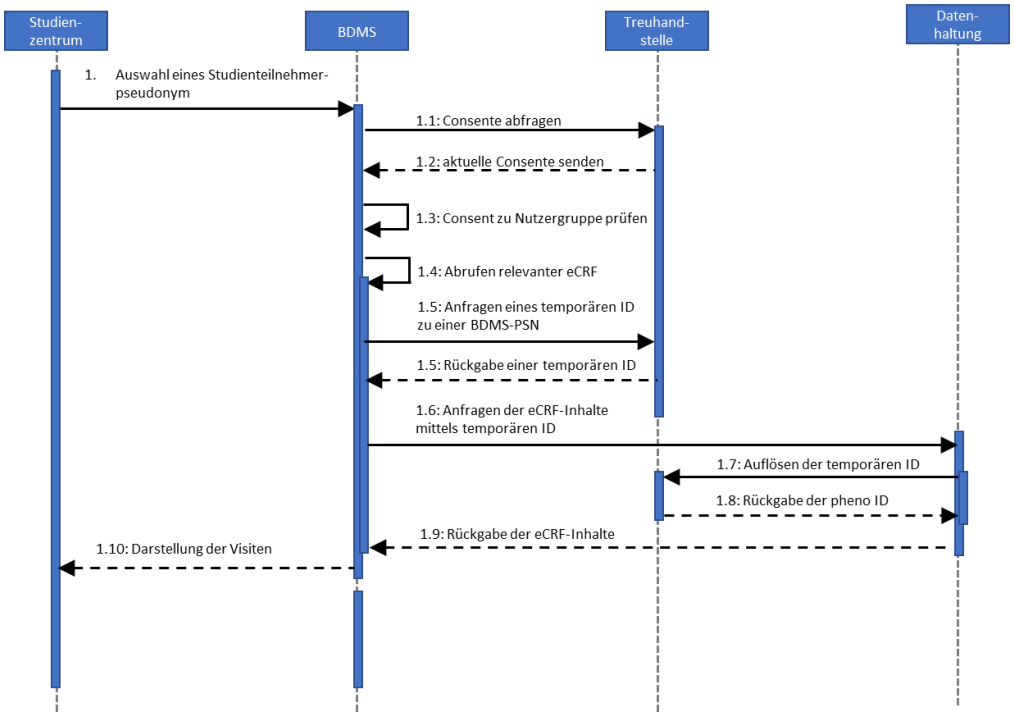


Abbildung 27: Datenflüsse beim Aufruf des Visitenplans im BDMS

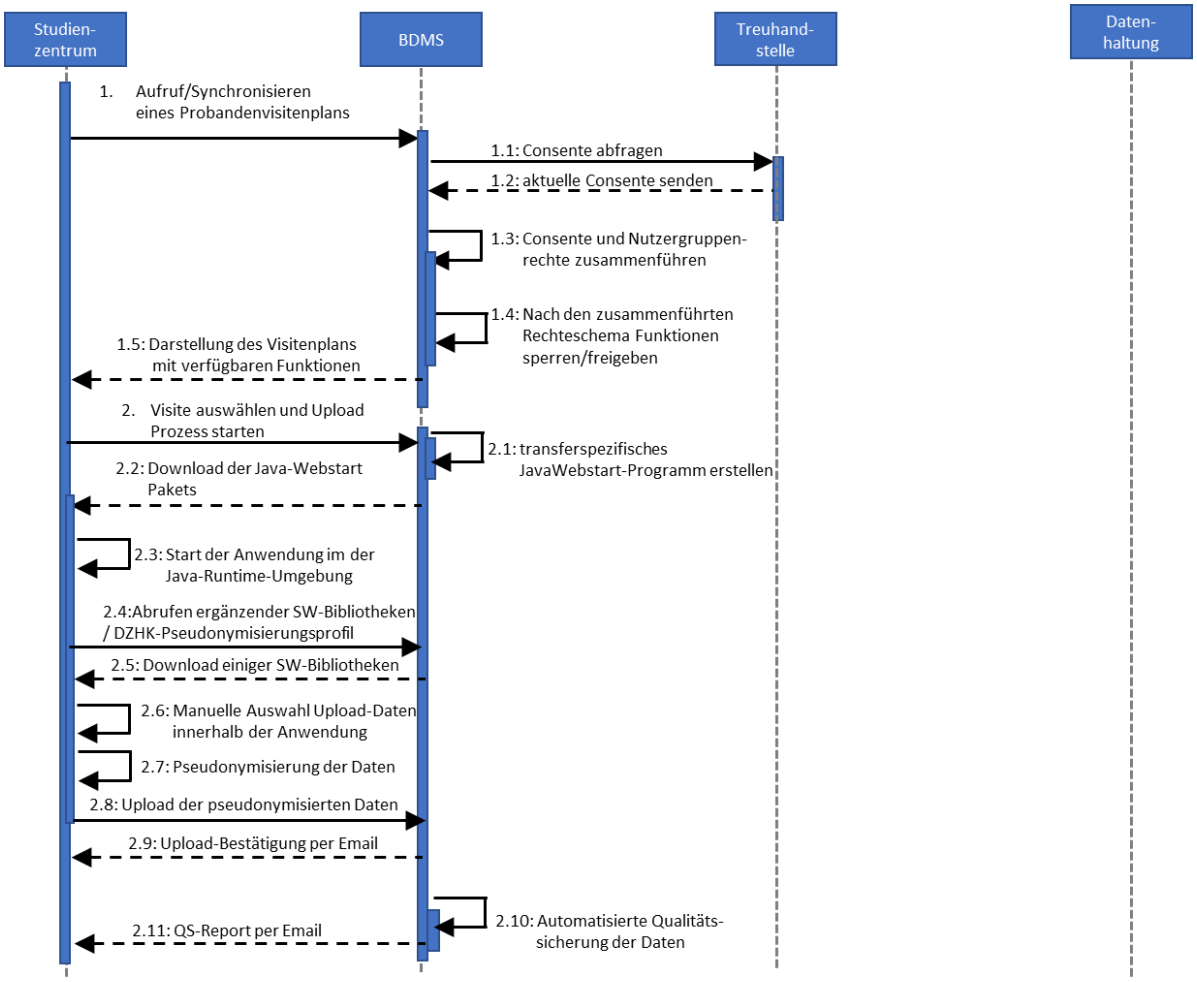


Abbildung 28: Datenflüsse beim Upload von DICOM-Daten (1. – Aufruf des Visitenplans und Umsetzen der teilnehmerspezifischen consertierten Funktionen; 2. – Prozess des Bilddatenuploads)

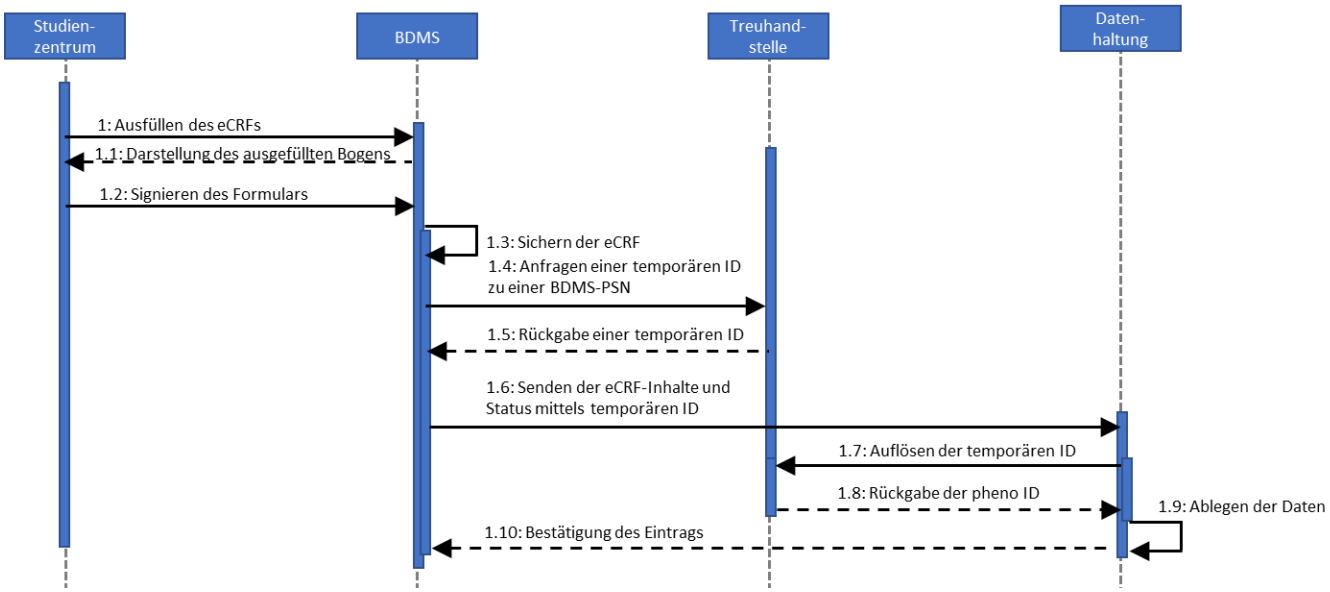


Abbildung 29: Datenflüsse beim Ändern von eCRFs im BDMS

3 Abkürzungsverzeichnis

AES – Advanced Encryption Standard

AMG – Arzneimittelgesetz

BlnDSG – Berliner Datenschutzgesetz

BDAT – Medizinische (Bild-)Daten, die über das BDMS erfasst wurden

BDSG – Bundesdatenschutzgesetz

BMBF – Bundesministerium für Bildung und Forschung

BSI – Bundesamt für Sicherheit in der Informationstechnik

CFR – Code of Federal Regulations

DE – Deutsch

DH – Datenhaltung

DICOM – Digital Imaging and Communications in Medicine

DSFA – Datenschutzfolgeabschätzung

DS-GVO – Datenschutzgrundverordnung

DSG M-V – Datenschutzgesetz Mecklenburg-Vorpommern

DSK – Datenschutzkonferenz

DTHS – Deutschen Telekom Healthcare and Security Solutions GmbH

DWH – data warehouse

DZHK – Deutsche Zentrum für Herz-Kreislauf-Forschung e. V.

DZHK-GSt. – Geschäftsstelle des DZHK e.V.

DZG – Deutsche Zentren der Gesundheitsforschung

EDC – Electronic Data Capture

eCRF – Electronic Case Report Form

EN – Englisch

ELSI – Ethical, Legal and Social Implications

EKG – Elektrokardiogramm

EP – Ethikprojekt

ErwGr – Erwägungsgrund

ETL - extract, transform, load

GCP –Guideline of Good Clinical Practice

GCP-V – GCP-Verordnung

HTTPS – Hypertext Transfer Protocol

IC – Informed Consent

ICH – International Conference on Harmonisation

ICM – Institut für Community Medicine

ICM-VC - Abteilung Versorgungsepidemiologie und Community Health des ICM

ID – Identifikator

IDAT *– Identifizierende Daten*

iFrame – Inlineframe

ISO – International Organization for Standardization

IP – Internet Protocol address

IT – Informationstechnologie

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

LIMS – Laborinformationssystem

MDAT – Medizinische Daten

MDR – EU-Medizinprodukte-Verordnung

MI – Institut für Medizinische Informatik

MPG – Medizinproduktegesetz

MPI – Master Person Index

MPI–ID – Master Person Index Identifier

MTLA – Medizinisch-technische/r Laboratoriumsassistent/in

NAKO – Nationale Kohorte

NDSG – Niedersächsisches Datenschutzgesetz

NEMA – National Electrical Manufacturers Association

NO – Nutzungsordnung des DZHK

OLAP – Online Analytical Processing

PACS – Picture archiving and communication system

PSN – Pseudonym

QM – Qualitätsmanagement

REST - REpresentational State Transfer

SAN – Storage area network

SaaS – Software-As-A-Service

SDV – Source Data Verification

SOAP – Simple Object Access Protocol

SOPs - Standard Operating Procedures

SW - Software

THS – Treuhandstelle

TK – technischer Koordinator

TLS – Transport Layer Security

TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.

TOMs – Technische und organisatorische MaßnahmenUMG – Universitätsmedizin Greifswald VPN – virtual private Network

4 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, [13])

Informed Consent – Informierte 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 zustehendes Recht im eigenen Namen auszuüben.

Einwilligung – Vereinbarung zwischen Studienteilnehmer und datenerhebender Stelle betreffs Erhebung und Verarbeitung personenbezogener Daten, sowie 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.

5 Literaturverzeichnis

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

[2] Unabhängige Treuhandstelle der Universitätsmedizin Greifswald, „Datenschutz- und IT-Sicherheitskonzept für die Unabhängige Treuhandstelle der Universitätsmedizin Greifswald, v.1.1.0 vom 25.01.2018," Greifswald, 2018.

[3] M. Bialke, P. Penndorf, T. Wegner, T. Bahls, C. Havemann, J. Piegsa und W. Hoffmann, „A workflow-driven approach to integrate generic software modules in a Trusted Third Party," *Journal of Translational Medicine,* Bd. 13, Nr. 176, 6 2015.

[4] K. Pommerening, J. Drepper, K. Helbing und T. Ganslandt, Guideline for Data Protection in Medical Research Projects: TMF's generic solutions 2.0, 1 Hrsg., Berlin, 2014.

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

[6] „Leitfaden Informationssicherheit," Bundesamt für Sicherheit in der Informationstechnik (BSI), 2012. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzUeberblick/LeitfadenInformationssicherheit/leitfaden_node.html. [Zugriff am 01 03 2014].

[7] „M 4.223 Integration von Proxy-Servern in das Sicherheitsgateway," Bundesamt für Sicherheit in der Informationstechnik - BSI, 2013. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/ m04223.html. [Zugriff am 01 03 2014].

[8] A. Technik, „Technische und organisatorische Anforderungen: Orientierungshilfe Mandantenfähigkeit," Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten, 2012.

[9] DICOM Standards Committee Working, Group 18 Clinical Trials, *Supplement 142: Clinical Trial Deidentification Profiles,* Rosslyn , Virginia 22209 USA,, 2011.

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

[11] „Gesetz über den Verkehr mit Arzneimitteln," Juris , 2013. [Online]. Available: http://www.gesetze-im-internet.de/amg_1976/index.html. [Zugriff am 01 03 2014].

[12] „Gesetz über Medizinprodukte," Juris, 2013. [Online]. Available: http://www.gesetze-im-internet.de/mpg/index.html. [Zugriff am 01 03 2014].

[13] „Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen," Juris, 2012. [Online]. [Zugriff am 01 03 2014].

[14] nds-voris.de, „Niedersächsische Vorschrifteninformationssystem," juris GmbH, 2012. [Online]. Available: http://www.nds-voris.de/jportal/portal/t/308u/page/bsvorisprod.psml. [Zugriff am 01 03 2013].

[15] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise," Bonn, 2008.

6 Anlagen

I.1 Datenschutzkonzept der Unabhängigen Treuhandstelle der Universitätsmedizin Greifswald, (v.2.0)

I.2 Rahmenkonzept Datenschutz und IT-Sicherheit für das ICM

I.3 Konzept für den sicheren internen und externen Zugriff auf Forschungsdienste

I.4 DZHK-SOP-P-06_DE „Erfassung IDAT Informed Consent“

I.5 DZHK-SOP-P-05_DE „Widerruf Studienausschluss Kontaktsperre“

I.6 DZHK-SOP-THS-12_DE Widerruf intern

I.7 Verfahrensverzeichnis der THS des DZHK der UMG, (v.1.0)

I.8 Ethik-Konzept des Bereichs Klinische Forschung des Deutschen Zentrums für Herz-Kreislauf-Forschung e.V. (DZHK)

I.9 BDMS Pseudonymisierungsprofil