Clinical Communication Platform (CCP-IT)

Datenschutzkonzept

Projekt	Clinical Communication Platform (CCP-IT) im Deutschen Konsortium für Translationale Krebsforschung (DKTK)
Autoren	Martin Lablans[1] und Esther Schmidt[1]
Mitwirkende	Azita Ahmadi, Stefan Bartels, Heidrun Binder, Martin Boeker, Daniel Brucker, Daniel Büttner, Corinna Eichelser, Mirko Esins, Achim Flender, Dietmar Keune, Frank Ressing, Hagen Schulz und Tomas Skripcak
Träger	Deutsches Krebsforschungszentrum Im Neuenheimer Feld 280 69120 Heidelberg
Version	23. November 2020 (Diese Version unterscheidet sich von der vorigen Version (28. Februar 2019) nur durch die Ergänzung einer Risikobeurteilung im Rahmen der Datenschutz-Folgenabschätzung.)

DEUTSCHES KREBSFORSCHUNGSZENTRUM
IN DER HELMHOLTZ-GEMEINSCHAFT

[1] Deutsches Krebsforschungszentrum
Verbundinformationssysteme
Im Neuenheimer Feld 280
69120 Heidelberg

Inhalt

1. Einleitung

1.1 Zielsetzung

Vor dem Hintergrund des Wissens um das komplexe Zusammenwirken von individueller genetischer Disposition, Lebensstil und Umweltfaktoren für die Entstehung und den Verlauf von Krebserkrankungen verlangt die heutige Krebsforschung die Beobachtung von Krankheitsverläufen, individuellen Lebensgewohnheiten, und Umwelt-bedingungen über lange Zeiträume. Nur durch die Forschung in standortübergreifenden Verbünden mit ausreichenden Fallzahlen kann auch die Ursächlichkeit individueller genetischer Dispositionen erforscht werden.

Das DKTK hat sich zur Aufgabe gemacht, durch den Aufbau von effizienten translationalen Forschungseinheiten für anwendungsnahe Krebsforschung an bundesweit vernetzten Partnerstandorten die Erforschung der Entstehungsmechanismen von Krebserkrankungen sowie die Entwicklung optimierter Instrumente für eine gezielte Behandlung und für eine frühzeitige Erkennung von Krebserkrankungen voranzutreiben.

Als „Betriebssystem“ für diesen vernetzten Kampf gegen Krebs stellt die CCP-IT[1] eine einheitliche IT-Infrastruktur zur Verfügung. Sie stellt dabei Funktionalitäten wie z.B. Authentifizierungs-, Pseudonymisierungs- oder Datenintegrationsprozesse bereit, die in diesem Datenschutzkonzept einheitlich beschrieben sind, und von mehreren Anwendungen im DKTK als Grundlage ihres institutionsübergreifenden Datenmanagements genutzt werden. Diese werden daher als „CCP-Anwendungen“ bezeichnet.

CCP-Anwendungen werden einerseits durch den Betreiber der CCP-IT selbst entwickelt. So erlaubt es die in diesem Datenschutzkonzept beschriebene Suchanwendung, Fallzahlen zu definierten Krankheitsbildern standortübergreifend zu ermitteln, aber auch Probanden für klinische Studien zu rekrutieren oder bereits vorliegende Daten für Forschungsfragestellungen zur Auswertung anzufordern. Dazu werden an den beteiligten Standorten Daten aus der klinischen Krebsdokumentation sowie zu dort vorhandenen Biomaterialproben erhoben und je nach Möglichkeit in einer zentralen Datensammlung oder lokal an den Standorten gesammelt. Um diese Daten für die Forschung nutzbar zu machen, stellt die CCP-IT eine zentrale Suchschnittstelle bereit, die es Forschern ermöglicht

- abzuschätzen, ob für ein Forschungsvorhaben im DKTK genügend Probanden mit den betrachteten Eigenschaften auffindbar sind,
- zu ermitteln, welche Institutionen passende Patienten behandeln oder behandelt haben und
- Anfragen zur Nutzung von medizinischen Daten und Biomaterialproben dieser Patienten für Forschungsvorhaben zu stellen.

Eine Besonderheit gegenüber anderen Forschungsverbünden besteht darin, dass auch Bestandsdaten, die vor der Einrichtung des DKTK im Behandlungskontext erhoben wurden, für die Forschung nutzbar gemacht werden sollen. Dieser Nutzung von Bestandsdaten sind enge datenschutzrechtliche Grenzen gesetzt, wenn sie nicht durch eine Patienteneinwilligung gedeckt ist. Andererseits könnte dadurch die sonst nötige Wartezeit zwischen Beginn der Datenerhebung und dem Erreichen eines für Forschungszwecke hinreichend großen Datenbestandes erheblich reduziert werden. Darüber hinaus ermöglicht der Einbezug von Bestandsdaten die Evaluation von Therapiefortschritten. Das Ziel dieses Datenschutzkonzepts ist, in dieser Situation, in der Anforderungen bezüglich des Datenschutzes besonders stark mit Wünschen hinsichtlich der Nutzbarmachung für die medizinische Forschung konkurrieren, einen wirksamen und den rechtlichen Anforderungen genügenden Datenschutz sicherzustellen.

1.2 Nutzung der CCP-IT durch CCP-Anwendungen von Partnern

Andererseits werden CCP-Anwendungen durch Partner im DKTK entwickelt:

[1] IT der Clinical Communication Platform

Die Joint Imaging Platform (JIP) wird innerhalb des DKTK eine einheitliche IT-Infrastruktur für Bildanalyse anhand maschinellen Lernens an den DKTK-Standorten aufbauen. Ziel ist es, die Anwendung von Analysemethoden zu erleichtern, indem diese automatisiert und standardisiert auf Patientenkohorten in den verschiedenen Zentren angewendet werden können. Hierdurch können für die medizinische Bildverarbeitung bisher unerreichte Kohortengrößen ermöglicht werden, um quantitative bildbasierte Biomarker erfolgreich zu validieren.

Die RadiationDosePlan-Image/Biomarker-Outcome Plattform (RadPlanBio) stellt eine radiotherapie-spezifische IT-Infrastruktur für multizentrische Studien bereit. Sie integriert die Dokumentation mittels klinischer Fragebögen, von Bild- und Bestrahlungsplanungsdaten sowie die Verlinkung von Informationen aus Biobanksystemen und Labor-Datensätzen in einer Plattform. Das Hauptziel dieser Infrastruktur ist die Durchführung elektronisch erfasster klinischer und präklinischer Studien nach der Good Clinical Data Management Practice (GCDMP).

Dieses Datenschutzkonzept beschreibt die von den CCP-Anwendungen genutzten Prozesse und Funktionalitäten der CCP-IT. Darüber hinausgehende Prozesse der CCP-Anwendungen werden in separaten Dokumenten behandelt und sind nicht Bestandteil dieses Datenschutzkonzepts.

1.3 Überblick über die Datenverarbeitung

In der CCP-IT werden Daten von Tumorpatienten, die an den teilnehmenden Kliniken (auch als „Standorte“ bezeichnet) behandelt werden, erhoben und verarbeitet. Sie werden zum größten Teil aus vorhandenen Datenverarbeitungssystemen (z.B. Krankenhausinformationssysteme und Software zur Tumordokumentation), in die zentralen Komponenten der CCP-IT eingebracht. Darüber hinaus erlaubt die Komponente „Lokales Datenmanagement“ (siehe Abschnitt 2.1) die manuelle Eingabe von Daten zu Biomaterialproben.

Grundsätzlich teilen sich die erhobenen datenschutzrelevanten Daten in medizinische und identifizierende Daten auf, die im Folgenden in Anlehnung an die TMF[2]-Datenschutzkonzepte als MDAT und IDAT bezeichnet werden. Die erhobenen MDAT umfassen klinische Daten sowie Daten zu Biomaterialproben und sind in den Abschnitten (2.1 „Brückenkopf“ und 2.3 „Zentrale MDS-Datenbank“) näher beschrieben.

Weiterhin ist vermerkt, an welchen Studien des DKTK und dessen Kooperationspartner der Patient[3] teilnimmt, sowie welche Experimente mit seinen Biomaterialproben bereits durchgeführt wurden.[4] Die IDAT enthalten demografische Daten, die eine eindeutige Identifikation des Patienten erlauben. Genauere Informationen zum Umfang dieser Daten finden sich in den Darstellungen der folgenden Abschnitte (insbesondere Kapitel 2.2, Abschnitt „Kontrollnummern-Erzeuger“), sowie im Anhang.

1.4 Rechtsgrundlage

In Hinblick auf die Rechtsgrundlage sowie die Prozesse der Datenverarbeitung ist zwischen folgenden zwei Patientengruppen zu unterscheiden:

1. Patienten, die der Verwendung ihrer Daten und/oder Biomaterialproben im DKTK explizit zugestimmt haben (im Folgenden *explizit eingewilligte Patienten*). Die dafür vorgesehene Einwilligung (siehe Anlage 1) deckt neben der Weitergabe von Daten an die zentrale Suche auch die Weitergabe von IDAT zur Erzeugung eines zentralen Pseudonyms ab (Kapitel 2.2, Abschnitt „Kontrollnummern-Erzeuger“). Rechtsgrundlage ist hier also die genannte informierte Einwilligung des Patienten (siehe Abschnitt 6.1). Auf der Grundlage die-

[2] Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.

[3] „Patient“, „Arzt“ und ähnliche Begriffe bezeichnen in diesem Dokument Funktionsrollen und meinen Personen jeglichen Geschlechts. Auf eine gendergerechte Formulierung wurde aus Gründen der Lesbarkeit verzichtet.

[4] Letzteres dient dazu, die mehrfache Erhebung von Daten zu vermeiden.

ser Einwilligung können MDAT in eine zentrale Komponente (die sogenannte *MDS-Datenbank*) in pseudonymisierter Form exportiert werden und können dort über die *zentrale Suche* von DKTK-Forschern durchsucht werden.

2. Patienten, die der Verwendung ihrer Daten im DKTK nicht explizit zugestimmt haben (im Folgenden *nicht explizit eingewilligte Patienten*). Dieser Fall liegt insbesondere bei Bestandsdaten vor, die aus der Zeit vor Errichtung des DKTK stammen und damit wesentlich zahlreicher als Daten von *explizit eingewilligten Patienten* sind. Rechtsgrundlage sind hier die am Standort anwendbaren landes- und bundesrechtlichen Datenschutzbestimmungen sowie die lokale Einwilligung in die Verwendung und Weitergabe klinischer Daten und/oder Biomaterialproben für standortübergreifende Forschungsprojekte in anonymisierter bzw. pseudonymisierter Form (vgl. Abschnitt 6.2).
   In Hinblick auf die Rechtsgrundlage für den Export von Daten in die MDS-Datenbank ist zu erwähnen, dass für diesen Zweck keine IDAT den Standort verlassen, sondern nur ein festgelegter, sparsamer Satz an MDAT; weiteres siehe Abschnitt 6.2 und Anlage 0.

Die MDAT beider Patientengruppen werden in eine lokale Komponente, den *Brückenkopf*, in pseudonymisierter Form importiert und dort gespeichert. Der Brückenkopf steht unter lokaler Kontrolle der behandelnden Einheit des jeweiligen Standorts, und auch nur dort kann mithilfe des Pseudonyms auf die Identität des Patienten geschlossen werden. Auf diesen lokal verbleibenden MDAT können zwar im Rahmen einer sogenannten *dezentralen Suche* Suchanfragen von außerhalb des Standorts durchgeführt werden, die Ergebnisse dieser Suchanfragen sind aber im Rahmen der CCP-IT nur nach manueller Freigabe durch den Standort, der die Daten besitzt, für den Anfragenden sichtbar. Rechtsgrundlage sind hier die am Standort anwendbaren landes- und bundesrechtlichen Datenschutzbestimmungen. (vgl. Abschnitt 6.2).

Nutzer bzw. Empfänger von Daten sind Forscher des DKTK und dessen Kooperationspartner[5]. Aus deren Sicht gibt es zwei verschiedene Zugriffswege (eine detaillierte Beschreibung der Komponenten und Prozesse wird in den folgenden Abschnitten gegeben):

- Datensätze, die in der zentralen MDS-Datenbank gespeichert sind, können von Forschern nach vorgegebenen Kriterien direkt durchsucht werden (*Zentrale Suche*, vgl. Abschnitt 3.4). Hier wird direkt ein Ergebnis in Form eines zusammenfassenden Überblicks über die gefundenen Datensätze zurückgeliefert. Die zentrale Suche erlaubt also mit ihrer Abfrage eine erste Einschätzung von im DKTK und bei dessen Kooperationspartnern vorliegenden Daten und Biomaterialproben. Die Datensätze werden aus der MDS-Datenbank nicht weitergegeben, sondern die Anzahl geeigneter Patienten und/oder Proben aufgrund der ausgewählten Suchkriterien angezeigt.
- Nur lokal (d.h. im Brückenkopf) gespeicherte Datensätze können über die *Dezentrale Suche* angefragt werden (vgl. Abschnitt 3.5). Dabei wird keine zentrale Datenbank durchsucht, sondern die Suchkriterien werden an die Standorte übermittelt. Der Anfragende sieht zunächst kein Suchergebnis, sondern die auf die Suchkriterien passenden Datensätze werden nur dem Dateneigentümer am Standort (ggfls. vertreten durch von ihm beauftragte Personen) angezeigt. Am Standort wird die Anfrage auf inhaltliche Kriterien und rechtliche Zulässigkeit geprüft und, falls beides positiv ausfällt, manuell durch den Dateneigentümer beantwortet. Diese Art der Suche kommt am ehesten einer klassischen schriftlichen Anfrage gleich, nur dass ihre Begutachtung und Beantwortung durch technische Hilfsmittel unterstützt werden.

Dieses Datenschutzkonzept beschreibt ausschließlich die Prozesse zur übergreifenden Vernetzung der teilnehmenden Standorte im Rahmen der CCP-IT. Lokale Prozesse werden in diesem Datenschutzkonzept nicht behandelt. Es obliegt den teilnehmenden Standorten, die Rechte der Betroffenen gemäß Kapitel 3 DSGVO, insbesondere Artikel

[5] Siehe Abschnitt 4.2, „Teilnehmende Forscher“, für die genaue Bestimmung dieses Personenkreises.

15 bis 21, zu berücksichtigen und durch Umsetzung entsprechender Maßnahmen den daraus resultierenden Pflichten nachzukommen, ggfls. in Abstimmung mit den anderen Standorten und den Betreibern der zentralen Komponenten. Weiterhin unterliegen die teilnehmenden Standorte der Nachweispflicht in Bezug auf das Vorliegen einer relevanten Patienteneinwilligung für Prozesse, die sie erfordern, bzw. die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz. Dies gilt entsprechend auch für CCP-Anwendungen, die Funktionalitäten der CCP-IT nutzen.

1.5 Träger und Joint Controlling

Träger des Vorhabens ist das Deutsche Krebsforschungszentrum (DKFZ), Heidelberg.

Die Aufteilung der Verantwortlichkeiten im Sinne des Joint Controlling (Artikel 26 DSGVO) sind in der Anlage 0 „Checkliste Joint Controllership“ zusammengefasst.

2. Datenverarbeitende Komponenten

2.1 Brückenkopf

Kernstück der CCP-IT ist der Brückenkopf. Er wird durch jeden teilnehmenden Standort unter Hoheit seiner eigenen Systemadministratoren installiert und betrieben und dient dem Anschluss des Standorts an die CCP-IT. Dies umfasst

- einerseits das Vorhalten der Daten des Standorts in einem DKTK-kompatiblen Format, das von den anderen IT-Komponenten und Anwendungen der CCP verstanden wird. Seine Art der Datenhaltung erlaubt dabei dem Standort eine Teilnahme an der CCP-IT auch ohne „Upload auf Verdacht“ seiner patientenbezogenen Daten an eine externe Stelle, was Datenschutz und Datenhoheit fördert,
- und andererseits die Bereitstellung von Funktionalitäten in nachnutzbarer Form als Grundlage für ein standortübergreifendes Datenmanagement durch CCP-Anwendungen (z.B. Pseudonymisierung oder Authentifizierung; vgl. 3.2 und 5.1).

Der Brückenkopf besteht aus den folgenden, lokal in der Klinik installierten, Softwarekomponenten:

- *Lokales Datenmanagement*: Bereitet die in den lokalen Primärsystemen prinzipiell vorliegenden, aber unterschiedlich strukturierten Datenbestände für eine Nutzung im DKTK auf. Bietet für Biomaterialbanken an den Standorten eine rudimentäre Proben- und Materialverwaltung samt Nutzer- und Gruppenverwaltung und Formularhandling. Diese Komponente entspricht funktional und technisch weitgehend einem Clinical Data Warehouse.
- *Teiler*: Leistet eine kontrollierte Freigabe der Datenbestände des lokalen Datenmanagements zur Nutzung durch Projekte des DKTK und dessen Kooperationspartner. Dabei kommen zwei sich ergänzende „Teilmethoden“ zum Einsatz: Eine zentrale Suche gibt sofort erste Ergebnisse aus, dann folgt eine langsamere, aber dafür umfassendere dezentrale Suche.
- *Lokales Identitätsmanagement*, bestehend aus lokalem ID-Manager und lokaler Patientenliste. Stellt für die Pseudonymisierung sowohl von *explizit eingewilligten* als auch von *nicht explizit eingewilligten Patienten* eine einheitliche Schnittstelle bereit. Die lokale Patientenliste vergibt für IDAT eines Patienten ein lokales Pseudonym ($BK_{\#}L$-ID, s.u.) und speichert dieses zusammen mit den IDAT. Die rein lokale Speicherung der IDAT ist notwendig, um zum Beispiel im Falle des Widerrufs oder eines Antrags auf Auskunft oder Löschung der Daten durch den Patienten, oder auch zu Überprüfungszwecken durch den Datenschützer, eine Zuordnung der Klarnamen zu den erzeugten Pseudonymen zu ermöglichen. Optional können für CCP-Anwendungen weitere Pseudonyme desselben Patienten erstellt und gespeichert werden. Falls nötig, kann ein Standort die lokale Patientenliste auf einem vom Brückenkopf getrennten Server ausführen und somit auch lokal eine Trennung von IDAT und MDAT umsetzen. Im Folgenden wird jedoch von einem Betrieb innerhalb des Brückenkopfes ausgegangen.

- *Authentifizierung*: Überprüft die Berechtigungen zugreifender Nutzer/APIs entweder lokal innerhalb des Standorts oder durch Anfrage an einen zentralen Authentifizierungsdienst.

Die im Brückenkopf gespeicherten MDAT können prinzipiell alle Elemente des einheitlichen onkologischen Basisdatensatzes der Arbeitsgemeinschaft Deutscher Tumorzentren[6] sowie Daten zu Biomaterialproben umfassen. Außerdem können darüber hinausgehende Daten, die in DKTK-assoziierten Verbundstudien erhoben werden, gespeichert werden.

Diese Komponenten stehen unter Kontrolle des jeweiligen Zentrums, das heißt, die in diesen Komponenten gespeicherten Daten stehen weiter unter der Hoheit der Institution, in der sie erhoben wurden. Gegebenenfalls ist der Zugriff auf die behandelnde Einheit, z.B. die Fachabteilung, einzuschränken (vgl. auch Abschnitt 7).

2.2 Identitätsmanagement

Pseudonymisierung ist ein zur Aufrechterhaltung eines hohen Datenschutzniveaus notwendiger Schritt, um den Patienten vor Rückidentifizierung zu schützen. Anstelle seiner identifizierenden Daten (IDAT) treten Pseudonyme.

Um eine unerlaubte Zusammenführung von Daten zu verhindern, erhalten Anwendungen und CCP-Komponenten, aber auch jeder Standort, für denselben Patienten verschiedene Pseudonyme, die nur durch einen kontrollierten Prozess einander zuordenbar sind. In der CCP-IT werden Pseudonyme nach folgender Systematik erstellt (vgl. Abbildung 1):

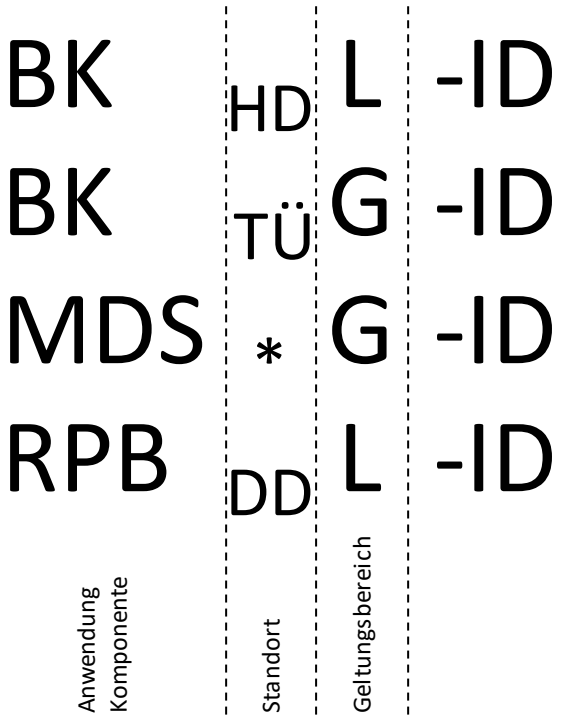

Abbildung 1 – Systematik zur Bezeichnung von Pseudonymen.

1. Der erste Teil des Pseudonyms gibt an, für welche CCP-Anwendung bzw. welche CCP-Komponente das Pseudonym erstellt wurde. „BK“ steht für den Brückenkopf, „MDS“ für die zentrale MDS-Datenbank (vgl. 2.3) und „RPB“ beispielsweise für die CCP-Anwendung RadPlanBio (vgl. 1.2).
2. Der zweite Teil des Pseudonyms gibt den Standort # an, für den das Pseudonym erzeugt wurde. Ist ein Pseudonym für alle Standorte gleich, kommt der Platzhalter * zum Einsatz.

[6] siehe http://www.tumorzentren.de/onkol-basisdatensatz.html

3. Aus dem dritten Teil des Pseudonyms geht sein Geltungsbereich hervor, also ob es sich um ein lokales Pseudonym (L) handelt, oder um ein standortübergreifend vergleichbares, globales Pseudonym (G).

In Abbildung 1 ist also das Pseudonym

- BK_{HD}L-I*D*: Ein Identifikator, der für einen Brückenkopf erzeugt wurde, nur für den Standort Heidelberg (HD) eindeutig ist und keine standortübergreifende Verknüpfung von Daten eines Patienten erlaubt (L). Dieser Identifikator wird in der CCP-IT immer erstellt.[7]
- $BK_{TÜ}$G-I*D*: Ein Identifikator, der für einen Brückenkopf erzeugt wurde und nur für den Standort Tübingen (TÜ) eindeutig ist. Im Gegensatz zum vorigen Pseudonym können $BK_{\#}$G-IDs, die an verschiedenen Standorten $\#_1$ und $\#_2$ zu einem Patienten existieren, in der zentralen Patientenliste einander zugeordnet werden.[8] Rechtsgrundlage zur Erzeugung der globalen $BK_{\#}$G-ID ist die informierte Einwilligung; daher wird sie nur für *explizit eingewilligte Patienten* erzeugt.
- MDS_{*}G-ID: Ein Identifikator, der für die zentrale MDS-Datenbank erzeugt wurde und keinen Standortbezug hat (*). In der zentralen Patientenliste kann er anderen Pseudonymen desselben Patienten zugeordnet werden.
- RPB_{DD}L-ID: Ein Identifikator, der für die CCP-Anwendung RadPlanBio (RPB) erzeugt wurde, nur für den Standort Dresden (DD) eindeutig ist und keine standortübergreifende Verknüpfung von Daten eines Patienten erlaubt (L).

Record Linkage

Das zentrale Identitätsmanagement ermöglicht eine datenschutzgerechte Zusammenführung („Record Linkage“) der von mehreren Standorten gesendeten patientenbeziehbaren Daten. Dafür werden IDAT oder daraus abgeleitete Werte durch eine Kombination dreier Methoden/Werkzeuge miteinander verglichen, vgl. folgende Unterabschnitte und Abbildung 2.

In den Record-Linkage-Prozess eingehende IDAT bestehen aus folgenden Attributen:

- Vorname
- Nachname
- Frühere Namen (z.B. Geburtsname bei Namensänderung durch Heirat)
- Geburtsdatum, aufgetrennt in die Komponenten Tag, Monat und Jahr
- Staatsangehörigkeit
- Geschlecht

[7] In den Datenschutzkonzepten bis einschließlich Version vom 30.06.2017 entspricht dieser Identifikator einer S_{HD}ID.
[8] In den Datenschutzkonzepten bis einschließlich Version vom 30.06.2017 entspricht dieser Identifikator einer $DKTK_{TÜ}$ID.

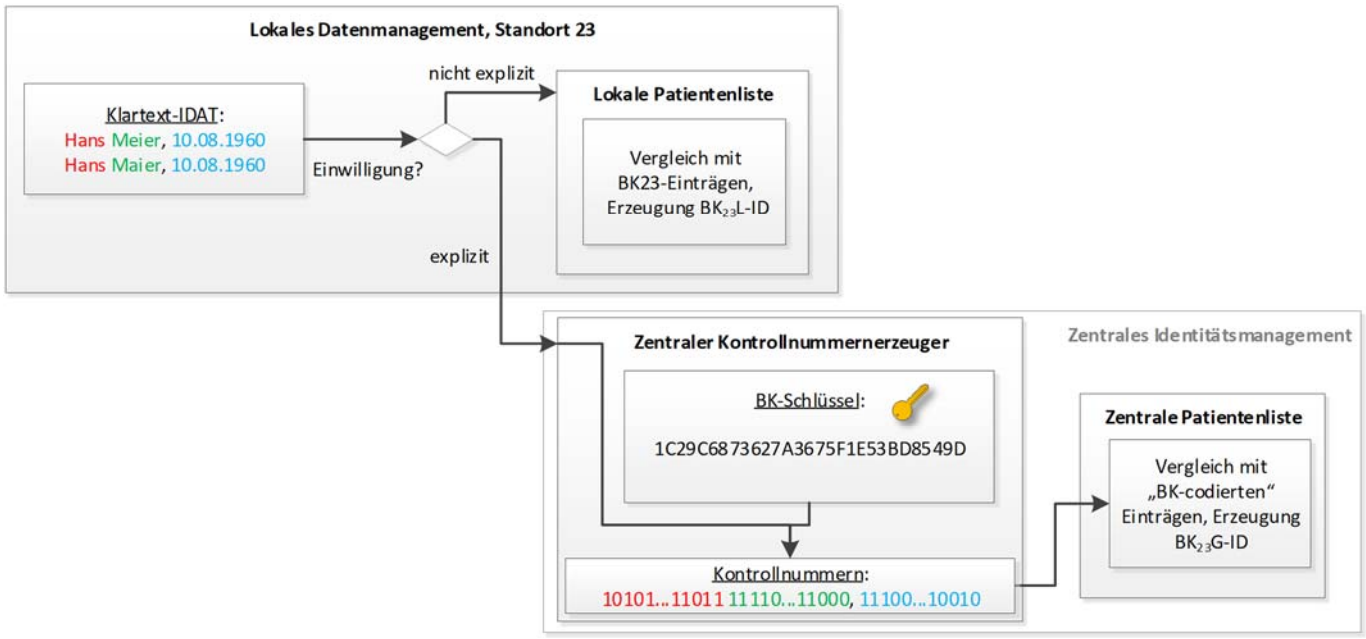

Abbildung 2 - Beispielhaftes Record Linkage-Verfahren.

Kontrollnummern-Erzeuger

Kommt zur Erstellung globaler Pseudonyme zum Einsatz und wandelt Identifikationsdaten (Klartext-IDAT) durch eine spezielle Einwegverschlüsselung in unlesbare und nicht rückführbare, aber immer noch gewichtet vergleichbare Zeichenketten („Kontrollnummern“[9]) um. Um Wörterbuchattacken zu vermeiden, wird dabei ein Keyed-Hash Message Authentication Code verwendet, wobei der verwendete Schlüssel (im folgenden „Geheimnis“) für jede Instanz des Kontrollnummern-Erzeugers eindeutig und nur dort bekannt ist.[10] Daraus folgt die Voraussetzung eines organisatorisch unabhängigen Betriebs dieses Moduls.

Da erzeugte Kontrollnummern über alle Standorte hinweg vergleichbar sein müssen, kommt ein zentraler Kontrollnummern-Erzeuger zum Einsatz. Die empfangenen Daten (IDAT) werden vom Kontrollnummernerzeuger nicht gespeichert. Als weitere Sicherheitsmaßnahme (z.B. gegen Angriffe mit Probeverschlüsselungen), werden die dort erzeugten Kontrollnummern nicht an den Brückenkopf zurückgegeben, sondern direkt an die zentrale Patientenliste übermittelt. Die erstellte globale ID wiederum wird nie dem zentralen Kontrollnummern-Erzeuger bekannt gemacht (Details siehe Abschnitt 3.2).

Zentrale Patientenliste

Vergibt für eine Gruppe von Kontrollnummern eines Patienten ein globales Pseudonym. Ihr Record-Linkage-Algorithmus kann dabei Patienten selbst bei abweichender Schreibweise wiedererkennen.

Manuelles Linken

Eine Prüfoberfläche erlaubt einem berechtigten Administrator, Ergebnisse des automatischen Matchings zu überprüfen und ggfls. zu korrigieren, d.h. Duplikate zusammenzuführen. Hierfür werden die Matchgewichte (Vergleichswerte zwischen den einzelnen Attributen von zu prüfenden Patienten) angezeigt und es besteht die Möglichkeit, zur Entscheidungsfindung auf medizinische Daten zuzugreifen. Diese Komponente ist deshalb beim Betreiber der zentralen MDS-Datenbank, wo ohnehin MDAT gespeichert sind, angesiedelt.

[9] Streng genommen sind das also keine Nummern. Idee und Name wurden (in angepasster Form) aus dem Bereich epidemiologischer Krebsregister übernommen.

[10] Für technische Details siehe: Schnell R, Bachteler T, Reiher J: Privacy-preserving record linkage using Bloom filters. BMC Medical Informatics and Decision Making 2009, 9:41. http://www.biomedcentral.com/1472-6947/9/41

2.3 Zentrale MDS-Datenbank

Die zentrale MDS-Datenbank nimmt mithilfe einer Webschnittstelle die von den Teilern verschickten MDAT entgegen und verwahrt sie in einer Datenbank. Die Speicherung erfolgt zusammen mit der MDS*G-ID, um die Zuordnung verschiedener Datensätze eines Patienten zueinander möglich zu machen. Die MDAT umfassen folgende Datensätze:

- *MDS-K*: Meldedatensatz aus klinischen Daten. Diese beinhalten Daten zum Patienten, zum Primärtumor, zur Primärtherapie, zum Ansprechen und zum Vitalstatus und basieren meist auf dem onkologischen Basisdatensatz der Arbeitsgemeinschaft deutscher Tumorzentren (ADT und GEKID)[11].
- *MDS-B*: Meldedatensatz zu Biomaterialproben. Der MDS-B umfasst Auskunft über das Vorhandensein von Biomaterial von Patienten und allgemeine Informationen zur Beschreibung des Biomaterials (z.B. Gewebetyp, Probenart).
- Im Rahmen bestimmter CCP-Anwendungen, etwa DKTK-assoziierter Studien und Registern, können zusätzliche Datenelemente in die CCP-IT eingebracht werden, die das Vorhandensein von Daten dokumentieren und diese somit auffindbar machen. Diese Datenelemente werden in Abstimmung mit dem Betreiber der jeweiligen CCP-Anwendung mit den Standorten gesondert diskutiert.

Autorisierte Nutzer (siehe auch Abschnitt 5.1, „Authentifizierung“) können in einer Suchmaske mittels definierter Suchkriterien Abfragen auf diesem Datenbestand ausführen; diese Funktion wird im Abschnitt 3.4 („Zentrale Suche“) beschrieben. Im Rahmen der Protokollierung von Suchvorgängen können identifizierende Daten des zugreifenden Forschers und seine Eingaben in das System, bspw. Suchabfragen, gespeichert werden.

2.4 Suchbroker für die dezentrale Suche

Der Suchbroker für die dezentrale Suche stellt eine Schnittstelle zur Formulierung von Anfragen zur Verfügung und verwaltet diese Anfragen. Er verarbeitet keine personenbezogenen Daten von Patienten. Personenbezogene Daten von zugreifenden Benutzern können im Rahmen der Projektverwaltung (vgl. Abschnitt 3.5) und Protokollierung gespeichert werden.

2.5 Metadata Repository

Das Metadata Repository (MDR) speichert die Bedeutung (Semantik) sämtlicher im DKTK verwendeten (Nutz-) Datenelemente. Es bietet ein kontrolliertes Vokabular (Syntax) und kann maschinenlesbare, strukturierte Aussagen über Datenelemente machen, bspw. konzeptuelle Domänen oder Wertebereiche. Hier sind auch die Meldedatensätze definiert. Da das MDR keine personenbezogenen Daten verarbeitet, wird innerhalb dieses Datenschutzkonzepts nicht weiter darauf eingegangen.

[11] www.tumorzentren.de/onkol-basisdatensatz.html

3. Datenverarbeitende Prozesse

3.1 Import in Brückenkopf

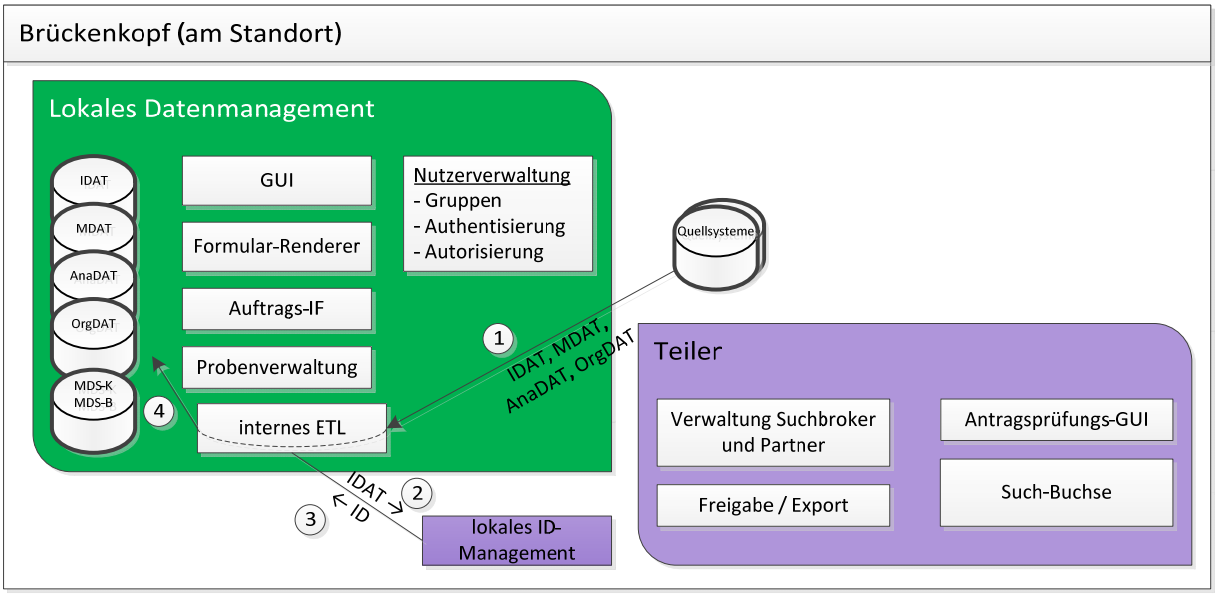

Abbildung 3 - Import von Daten in den Brückenkopf

Abbildung 3 zeigt, wie Daten aus Quellsystemen eines Standorts in den Brückenkopf importiert werden:

1. Identifizierende, medizinische und Probendaten werden aus mehreren Quellsystemen durch einen ETL-Prozess extrahiert.
2. Identifizierende Daten werden mithilfe des lokalen Identitätsmanagements mit einem primären Patientenidentifikator erster Stufe versehen (Details siehe Abschnitt 3.2, „Pseudonymisierung“).
3. Der ETL-Prozess ordnet den Identifikator dem Datensatz zu.
4. Daten werden im lokalen Datenmanagement abgelegt.

3.2 Pseudonymisierung

Artikel 32 der DSGVO fordert in Absatz 1 lit. a. die Verarbeitung personenbezogener Daten in pseudonymisierter Form, sofern der Zweck der Verarbeitung damit erreicht werden kann. Die Umsetzung dieser Anforderung wird im Folgenden erläutert.

Bei jeder erstmaligen Pseudonymisierungsanfrage für einen Patienten wird grundsätzlich zunächst ein lokales Brückenkopf-spezifisches Pseudonym erstellt (BK#L-ID), vgl. 2.2. Je nach Einwilligungsstatus des Patienten kann zusätzlich ein globales Brückenkopf-Pseudonym angefordert werden (BK#G-ID).

Um eine Zuordnung von Patienten zu Studien oder Projekten, die im Rahmen des DKTK oder dessen Kooperationspartner durchgeführt werden, zu gewährleisten, wird ein weiterer Pseudonymisierungsprozess benötigt. Dieser Prozess soll Daten, die innerhalb einer CCP-Anwendung † am Standort # für einen gegebenen Patienten erfasst werden, mit den für denselben Patienten am Brückenkopf # vorliegenden Daten miteinander verknüpfen können (z.B. Daten aus der Tumordokumentation und Daten zu Biomaterial). Außerdem soll eine solche Verknüpfung auch standortübergreifend möglich sein. Es obliegt dem Betreiber einer solchen Anwendung, die Patienten im Rahmen der Einwilligung auf das erhöhte Re-Identifizierbarkeitsrisiko aufgrund des Zusammenführens von Daten hinzuweisen.

Pseudonymisierungsprozess über eine API

Eine CCP-Komponente oder -Anwendung † (im Folgenden „CCP-Anwendung †“), die entweder innerhalb oder außerhalb des Brückenkopfes an einem gegebenen Standort # implementiert ist, kann über eine API Anfragen an das lokale ID-Management stellen und lokale oder globale Pseudonyme (s. 2.2 „Identitätsmanagement“) anfordern. Dieser Prozess soll zum Beispiel in obengenannter JIP-Plattform zum Einsatz kommen.

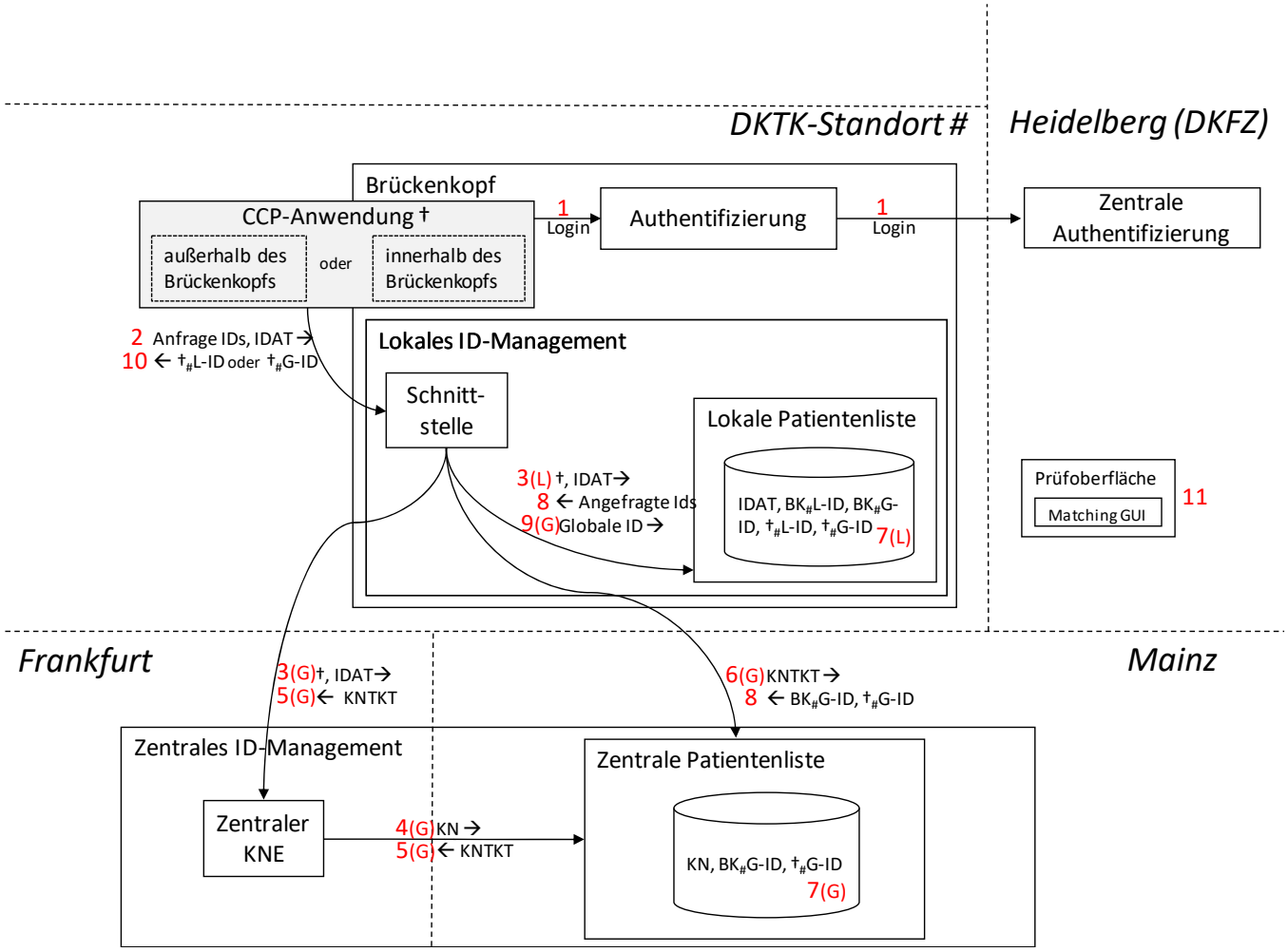

Abbildung 4 – Erzeugung lokaler (L) und globaler (G) Pseudonyme. Anfrage über API einer CCP-Anwendung †.

Abbildung 4 zeigt, wie die Pseudonymisierungsfunktion genutzt wird, um ein Pseudonym zu erhalten.

1. Die CCP-Anwendung † authentifiziert sich gegen den Authentifizierungsdienst. Dieser überprüft, ob die Berechtigung zur Pseudonymisierung für diese Anwendung vorliegt.
2. Das lokale Identitätsmanagement erhält den Typ des gewünschten Pseudonyms sowie die Klartext-IDAT eines Patienten über eine API-Anfrage der CCP-Anwendung †.
3. Die Schnittstelle übermittelt die Kennung der CCP-Anwendung †, zusammen mit den IDAT …
    - Im Fall Anforderung eines lokalen Pseudonyms (L): … an die lokale Patientenliste.
    - im Fall *A*nforderung eines globalen Pseudonyms (G): … an den Kontrollnummern-Erzeuger des zentralen Identitätsmanagements.

(Die Schritte 4 bis 6 und 9 sind nur für die Anforderung globaler Pseudonyme (G) relevant.)

4. Der zentrale Kontrollnummern-Erzeuger errechnet aus den Klartext-IDAT und seinem Geheimnis (verbundweit vergleichbare) Kontrollnummern (KN), verwirft die IDAT und übermittelt die KN an die zentrale Patientenliste.
5. Die zentrale Patientenliste erstellt ein temporäres Kontrollnummern-Ticket (KNTKT) und gibt dies an das lokale Identitätsmanagement zurück.
6. Das lokale Identitätsmanagement übermittelt das eben erhaltene Ticket KNTKT, an die Patientenliste des zentralen Identitätsmanagements. Durch die Verwendung des Tickets bleiben die verbundweit vergleichbaren KN dem lokalen Identitätsmanagement verborgen.
7. Erzeugung der ID, im Fall…
    - (L) Die lokale Patientenliste erzeugt für die erhaltenen IDAT mithilfe des Pseudonym-Generators die angeforderte(n) lokale(n) ID(s) und speichert diese in der Datenbank.
    - (G) Das zentrale Identitätsmanagement gleicht die erhaltenen Kontrollnummern mit den bestehenden ab (KN-Matcher). Im Falle eines Treffers wird eine bestehende ID zurückgegeben; falls kein passender Datensatz gefunden wird, wird mithilfe des Pseudonym-Generators eine neue ID erzeugt und zusammen mit den Kontrollnummern in der Datenbank gespeichert.
8. Das lokale Identitätsmanagement erhält als Antwort auf seine Anfrage die angefragte(n) ID(s). Es erfährt nicht, ob der Patient bereits bekannt war.
9. Fall (G) Das lokale Identitätsmanagement meldet die erhaltene(n) globale(n) ID(s) an die lokale Patientenliste. (Im lokalen Datenmanagement wird gespeichert, dass der Patient mit der $BK_{\#}$L-ID am Projekt † teilnimmt und dort unter dem Pseudonym $†_{\#}$-ID geführt wird. Dies ermöglicht eine Suche nach Patienten aufgrund ihrer Projektzugehörigkeit.)
10. Die ID wird als Antwort auf die ursprüngliche Anfrage zurückgegeben. Es ist nicht erkennbar, ob der Patient bereits bekannt war. Es ist aber erkennbar, ob es sich um eine lokale oder um eine globale ID handelt.
11. (optional) Sollte die Patientenliste sich nicht sicher sein, ob ein Patient schon in der Liste steht oder nicht, erfährt das der für das Record Linkage verantwortliche Administrator. Er entscheidet manuell auf Basis von Matchgewichten und – falls vorhanden – den in der zentralen MDS-Datenbank gespeicherten MDAT, ob es sich um denselben Patienten handelt.

Pseudonymisierungsprozess über einen Web-Browser

CCP-Anwendungen, die nicht über eine API auf die Pseudonymisierung im Brückenkopf zugreifen, verwenden eine Pseudonymisierungsfunktion über einen Web-Browser. Abbildung 5 erläutert die hierfür nötigen Schritte.

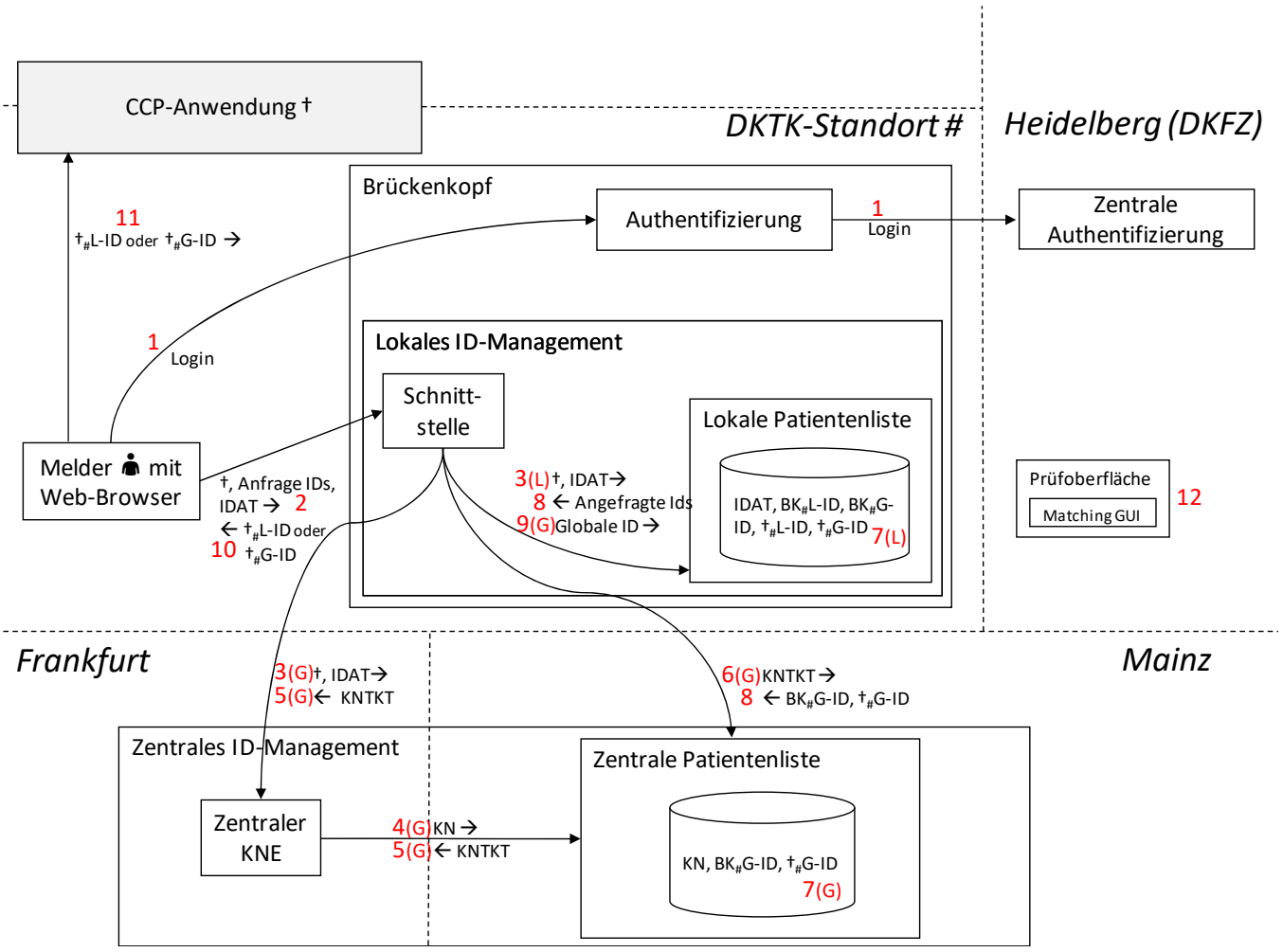

Abbildung 5 – Erzeugung lokaler (L) und globaler (G) Projekt-Pseudonyme. Anfrage über den Web-Browser einer CCP-Anwendung †.

1. Mithilfe seines Web-Browsers meldet sich der Nutzer der CCP-Anwendung † mit seinem DKTK-Login am Standort # an. Der Authentifizierungsdienst überprüft, ob die Berechtigung zur Pseudonymisierung für diesen Nutzer vorliegt.
2. Die Webseite des Brückenkopfs zeigt dem Nutzer diejenigen CCP-Anwendungen an, für die er pseudonymisieren darf. Der Nutzer wählt die gewünschte CCP-Anwendung † und den Typ des gewünschten Pseudonyms aus und trägt die IDAT des zu pseudonymisierenden Patienten in eine Webmaske ein.

   (Schritte 3-9 entsprechen den oben beschriebenen Schritten 3-9 bei der Erzeugung von Pseudonymen über eine API.)

10. Als Antwort auf seine Anfrage aus Schritt 2 bekommt der Nutzer das projektspezifische Pseudonym (†#L-ID bzw. †#G-ID) angezeigt.
11. Der Nutzer trägt das Pseudonym in die Datenbank der CCP-Anwendung † ein (z.B. via Copy-Paste).
12. Siehe oben Punkt 11.

Dieser Prozess soll zum Beispiel in obengenannter RadPlanBio-Plattform zum Einsatz kommen.

3.3 Umschlüsselung von Pseudonymen

Werden Daten zwischen CCP-Komponenten und -Anwendungen übertragen, müssen Pseudonyme umgeschlüsselt werden. Bei einem Upload an die zentrale MDS-Datenbank (vgl. 2.3) wird zum Beispiel das Pseudonym im Brücken-

kopf (BK...) in das Pseudonym der zentralen MDS-Datenbank umgeschlüsselt (MDS...). Dazu kommt ein asymmetrisches Verschlüsselungsverfahren zum Einsatz, wobei der private Schlüssel nur der Zielanwendung, hier der zentralen MDS-Datenbank, bekannt ist. Der Ablauf ist hier exemplarisch für die Umschlüsselung der $BK_{\#}$G-ID beschrieben (vgl. das Sequenzdiagramm Abbildung 6):

1. Der Teiler übermittelt die $BK_{\#}$G-ID des betreffenden Patienten am Standort # an die zentrale Patientenliste.
2. Die zentrale Patientenliste bestimmt die zugehörige MDS$_*$G-ID.
3. Die zentrale Patientenliste verschlüsselt die MDS$_*$G-ID asymmetrisch mit dem öffentlichen Schlüssel (-*Pub*) der zentralen MDS-Datenbank.
4. Die verschlüsselte MDS$_*$G-ID ((MDS$_*$G-ID)) wird an das lokale Datenmanagement zurückgegeben.
5. Die (MDS$_*$G-ID) und die zu übermittelnden Daten (MDAT) werden vom lokalen Datenmanagement an die zentrale MDS-Datenbank übermittelt.
6. Die zentrale MDS-Datenbank entschlüsselt die (MDS$_*$G-ID) mit ihrem privaten Schlüssel (*-Priv)*.
7. Die zentrale MDS-Datenbank speichert die MDS$_*$G-ID und die MDAT.
8. Die erfolgreiche Bearbeitung wird dem lokalen Datenmanagement zurückgemeldet.

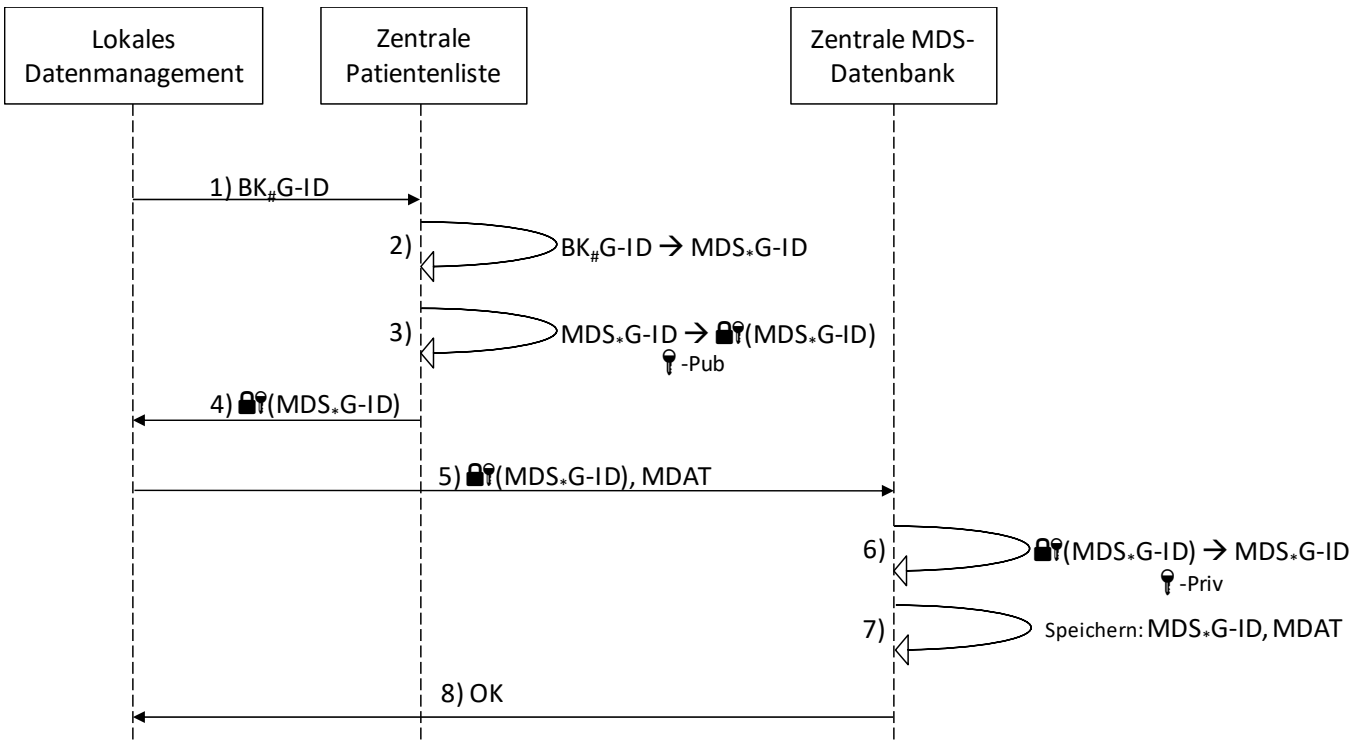

Abbildung 6 – Datenübermittlung an die zentrale MDS-Datenbank. (MDS$_*$G-ID) = MDS$_*$G-ID, verschlüsselt mit öffentlichem Schlüssel (-Pub) der zentralen MDS-Datenbank.

Um Wörterbuchattacken zu vermeiden, wird durch Randomisierung im Verschlüsselungsalgorithmus sichergestellt, dass die wiederholte (d.h. zeitlich hintereinander erfolgende) Verschlüsselung der gleichen MDS$_*$G-ID verschiedene Chiffrate erzeugt.

3.4 Zentrale Suche

Mit der zentralen Suche können Forscher des DKTK und dessen Kooperationspartner den Datenbestand der zentralen MDS-Datenbank durchsuchen und im Sinne einer Machbarkeitsanalyse abfragen, ob Daten und Proben vorhanden sind, die für ein Forschungsvorhaben relevant sein könnten. Die zentrale MDS-Datenbank stellt dafür ein

Webformular bereit, in dem Attribute der Meldedatensätze nach vorgegebenen Werten oder per Freitextsuche durchsucht werden können. Mehrere Suchattribute können durch logische Operatoren frei kombiniert werden.

Nach Ausführen der Suchabfrage erhält der anfragende Forscher maximal folgende Informationen[12]:

- Die Anzahl der Patienten bzw. Proben, die die Suchkriterien erfüllen.
- Die Altersverteilung der gefundenen Patienten in 10-Jahres-Intervallen.
- Die Geschlechtsverteilung (Anzahl Patienten männlichen / weiblichen / unbekannten Geschlechts).
- Die Verteilung auf die Standorte.
- Kontaktdaten der Standorte, an denen die Daten erhoben wurden.

Die Datensätze selbst werden nicht übermittelt. Ein eventueller Zugriff auf Daten durch den anfragenden Forscher sowie die datenschutzrechtliche Grundlage dafür wird zwischen diesem und dem jeweiligen Dateneigentümer (= Standort) verhandelt und findet außerhalb der zentralen MDS-Datenbank statt.

Upload in die zentrale MDS-Datenbank

Beim Upload von MDAT in die zentrale MDS-Datenbank kommt der oben beschriebene Prozess der Datenübermittlung mittels anwendungsspezifischen Pseudonyms zum Einsatz (vgl. 3.3).

a) Upload von MDAT *explizit eingewilligter Patienten*

Der Upload in die zentrale MDS-Datenbank erfolgt automatisch nach einem festen Zeitintervall (in der Regel täglich). Dabei werden aktuelle (d.h. seit dem letzten Upload hinzugekommene) MDAT von *explizit eingewilligten Patienten* gemäß der Meldedatensätze MDS-K und MDS-B vom Teiler aus dem lokalen Datenmanagement ausgelesen und über eine sichere HTTPS-Verbindung in die zentrale MDS-Datenbank exportiert.

Die übermittelten Daten können von den Administratoren von Brückenkopf und MDS-Datenbank im Rahmen von Wartungsarbeiten (vgl. Abschnitt 4.3 „Zugriff durch Systemadministratoren“) eingesehen werden. Ansonsten erfolgt durch den Upload selbst keine Sichtbarmachung, die Daten stehen mit dem Upload aber für die Zentrale Suche (Abschnitt 3.4) zur Verfügung.

b) Upload von MDAT *nicht explizit eingewilligter Patienten*

Falls lokale Datenschutzvoraussetzungen dies erlauben, kann im Brückenkopf auch ein Upload von Datensätzen *nicht explizit eingewilligter Patienten* an die zentrale MDS-Datenbank erfolgen. Dies kann zum Beispiel möglich sein, wenn am Standort eine lokale Patienteneinwilligung die Weitergabe pseudonymisierter oder anonymisierter Daten zu Forschungszwecken erlaubt und die Daten anonym weitergeben werden (näheres zu den datenschutzrechtlichen Aspekten siehe, Abschnitt 6.2 und Anlage 0). Diese Funktion erfordert eine zweistufige Freischaltung:

1. Generelle Freischaltung in der Konfiguration des Brückenkopfs. Dies erfordert den administrativen Zugriff auf Betriebssystemebene.
2. Aktivierung und Bestätigung durch den Administrator in der Benutzeroberfläche des Brückenkopfs (vgl. Abbildung 7). Das entsprechende Bedienelement erscheint nur, wenn die Freischaltung auf Systemebene (Punkt 1) erfolgt ist.

[12] Derzeit sind die ersten drei Punkte umgesetzt, die weiteren Punkte geben den maximalen Umfang eventueller Erweiterungen wieder.

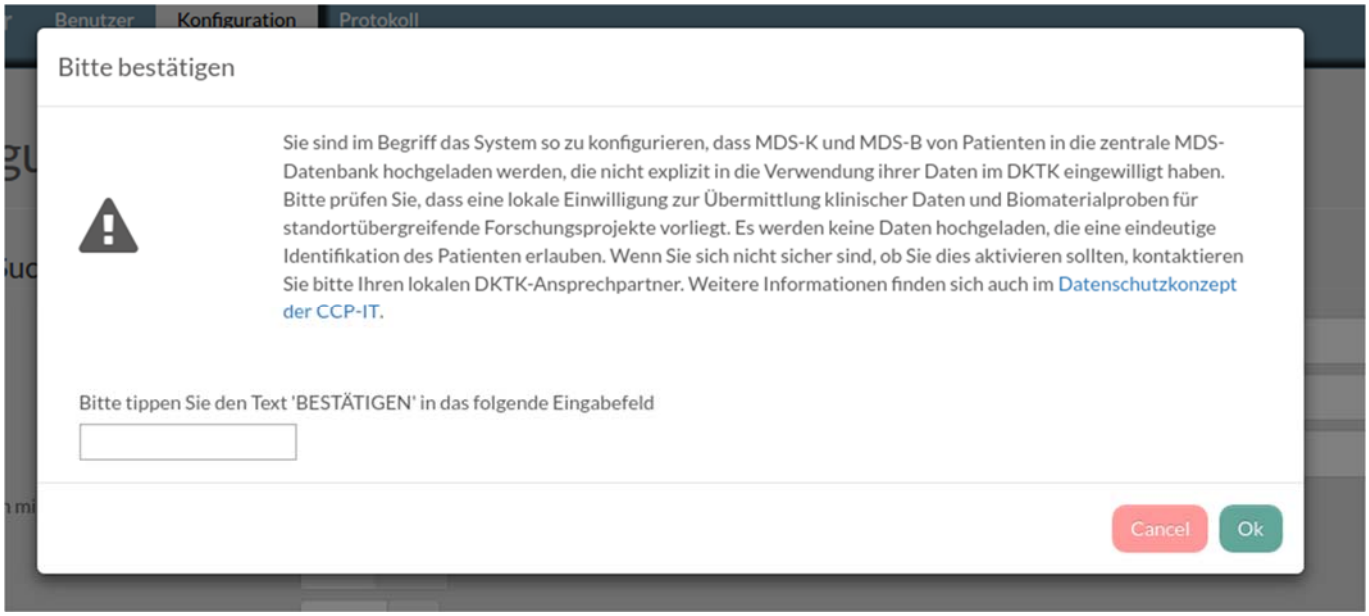

Abbildung 7 – Aktivierung des Uploads lokal eingewilligter Patienten im Brückenkopf

Der Upload erfolgt technisch wie im Fall *explizit eingewilligter* Patienten, an Stelle der $BK_{\#}$G-ID wird bei lokal eingewilligten Patienten aber die $BK_{\#}$L-ID übermittelt, um die verschlüsselte MDS_{*}G-ID abzufragen. In diesem Fall ist die MDS_{*}G-ID nicht standortübergreifend vergleichbar. Durch einen im Teiler konfigurierbaren Filter wird außerdem sichergestellt, dass nur für das DKTK relevante Fälle hochgeladen werden.

c) Upload von Daten aus CCP-Anwendungen

Sollen Daten aus einer CCP-Anwendung † an die zentrale MDS-Datenbank hochgeladen werden, wird zunächst die zur projektspezifischen $†_{\#}$-ID zugehörige $BK_{\#}$-ID aus der lokalen Patientenliste ermittelt. Daraufhin erfolgt die Abfrage der MDS_{*}G-ID wie unter a) und b) beschrieben. Der Teiler überträgt dann die MDS_{*}G-ID, die zu übermittelnden Daten sowie die Information über die Zugehörigkeit zur CCP-Anwendung † an die zentrale MDS-Datenbank.

3.5 Dezentrale Suche

Wie die zentrale Suche dient die dezentrale Suche dem Auffinden von „passenden“ Patienten und Proben für ein Forschungsvorhaben, berücksichtigt im Gegensatz dazu aber auch Patienten, deren Daten nicht an die zentrale MDS-Datenbank übermittelt wurden. Da bei diesen angenommen werden muss, dass keine Rechtsgrundlage für die Übermittlung von Daten aus dem zuständigen Standort heraus gegeben ist, erfolgt hier keine automatische Übermittlung von Suchergebnissen ohne Freigabe des datenhaltenden Standorts.

Das Suchformular der dezentralen Suche wird vom Suchbroker für die dezentrale Suche bereitgestellt. Sie erlaubt nicht nur die Suche nach den Meldedatensätzen, sondern allen im Metadata Repository (vgl. 2.5) abgelegten Begriffen; zusätzlich sind Ergänzungen im Freitext (Prosa) möglich. Der anzufragende Datensatz ist hier also prinzipiell unbeschränkt. Die Anfrage wird zunächst gespeichert und dem anfragenden Forscher lediglich ihre Speicherung mitgeteilt. Die Teiler der Standorte rufen in regelmäßigen Abständen neu hinzugekommene Anfragen vom Suchbroker ab und ermitteln, welche Datensätze im lokalen Datenmanagement den Suchkriterien entsprechen. Der Inhalt der Anfrage sowie die gefundenen Datensätze können an jedem Standort von einer dazu berechtigten Person eingesehen werden. Diese kann nun den anfragenden Forscher kontaktieren, um eine mögliche Weitergabe von Daten oder Proben zu vereinbaren. Dieser Vorgang erfolgt wiederum außerhalb der CCP-IT und die damit verbundenen datenschutzrechtlichen Fragen müssen im Einzelfall von den beteiligten Personen geklärt werden.

4. Organisatorische Rahmenbedingungen

Die datenverarbeitenden Personen und Institutionen sowie Datenempfänger in der CCP-IT verteilen sich auf die Betreiber der zentralen Komponenten sowie die am DKTK teilnehmenden Standorte.

4.1 Betrieb der Komponenten

Der Betrieb der Brückenköpfe erfolgt durch die im DKTK vertretenen Partnerstandorte sowie die DKTK-Kooperationspartner:

DKTK-Partnerstandorte

- Berlin: Charité Comprehensive Cancer Center
- Dresden: Universitätsklinikum Dresden, Technische Universität Dresden
- Essen / Düsseldorf: Westdeutsches Tumorzentrum am Universitätsklinikum Essen, Heinrich-Heine-Universität Düsseldorf
- Frankfurt / Mainz: Universitäres Centrum für Tumorerkrankungen Frankfurt, Johann Wolfgang Goethe-Universität Frankfurt, Georg-Speyer-Haus - Chemotherapeutisches Forschungsinstitut in Frankfurt am Main, Krankenhaus Nordwest Frankfurt, Universitätsmedizin Mainz
- Freiburg: Tumorzentrum - Comprehensive Cancer Center Freiburg, Albert-Ludwigs-Universität Freiburg, Universitätsklinikum Freiburg, Max-Planck-Institut Freiburg
- Heidelberg: Deutsches Krebsforschungszentrum (DKFZ) mit dem Nationalen Centrum für Tumorerkrankungen (NCT)
- München: Klinikum der Universität München, Klinikum rechts der Isar der TU München
- Tübingen: Universitätsklinikum Tübingen, Eberhard-Karls-Universität

DKTK-Kooperationspartner

DKTK-Kooperationspartner sind externe Einrichtungen, die sich über eine vertragliche Vereinbarung der CCP-Infrastruktur des DKTK angeschlossen und damit entsprechende Rechte und Verpflichtungen übernommen haben. Die aktuellen DKTK-Kooperationspartner sind in Anlage 7 aufgeführt.

Der Betrieb der zentralen Komponenten erfolgt an folgenden Stellen:

- Zentrale Patientenliste: Abteilung Medizininformatik, Institut für medizinische Biometrie, Epidemiologie und Informatik, Universitätsmedizin der Johannes Gutenberg-Universität Mainz.
- Zentraler Kontrollnummernerzeuger: Dezernat 7 – Informations- und Kommunikationstechnologie (DICT), Universitätsklinikum Frankfurt.
- Zentrale MDS-Datenbank und zentrale Suche, Metadata Repository, Authentifizierungsdienst, Suchbroker für die dezentrale Suche und Wartungsdienste für Brückenköpfe: Abteilung Verbundinformationssysteme, Deutsches Krebsforschungszentrum Heidelberg.

4.2 Teilnehmende Forscher

Teilnehmende Forscher sind die Personen, die über die zentrale und die dezentrale Suche Anfragen an das System stellen können. Generell können alle Mitglieder der Standorte des DKTK und dessen Kooperationspartner als teilnehmende Forscher die CCP-IT nutzen, wobei jeder Standort selbst entscheidet, welche seiner Mitglieder eine Zugangsberechtigung erhalten (siehe auch Abschnitt 5.1, „Authentifizierung von Benutzern“).

Wissenschaftler, die nicht Mitglieder eines Standorts des DKTK oder dessen Kooperationspartner sind, können auf Antrag vom Ausschuss für Datenschutz eine Zugangsberechtigung erhalten. Diese ist angemessen zu befristen.

4.3 Zugriff durch Systemadministratoren

Die in der CCP-IT gespeicherten Daten können prinzipiell von den Administratoren der verwendeten IT-Infrastruktur eingesehen werden. Zugriffe auf die Daten durch Administratoren dürfen nur erfolgen, wenn dies zur Erfüllung ihrer Aufgaben zwingend erforderlich ist. Soll Unterstützung durch Personen außerhalb des Standorts erfolgen (z.B. durch Mitarbeiter des DKFZ als Betreiber der zentralen Komponenten der CCP-IT), wird hierfür ein Vertrag zur Auftragsverarbeitung geschlossen. Alle Administratoren sind auf diesen Grundsatz und auf ihre Pflicht zur Verschwiegenheit hinzuweisen[13]. Die Verantwortung dafür tragen die teilnehmenden Standorte in Bezug auf die lokalen Komponenten, das DKFZ in Bezug auf die zentralen Komponenten.

4.4 Ausschuss für Datenschutz

Vom Lenkungsausschuss des DKTK wird ein Ausschuss für Datenschutz eingesetzt. Dieser erfüllt insbesondere folgende Aufgaben:

- Prüfung und Bewilligung von Anträgen externer Forscher[14] für die Nutzung der CCP-IT (zentrale und dezentrale Suche).
- Prüfung und Bewilligung von Anträgen auf Export medizinischer Daten und/oder Bereitstellung von Biomaterial für externe Forschungsprojekte.
- Prüfung und Bewilligung von Anträgen auf die Benachrichtigung betroffener Patienten über Forschungsergebnisse.

Darüber hinaus ist der Ausschuss für Datenschutz erster Ansprechpartner für datenschutzrechtliche Angelegenheiten. Der Ausschuss für Datenschutz wird so besetzt, dass jeder der DKTK-Standorte darin vertreten ist. Zu den Mitgliedern zählen mindestens:

- Ein Arzt, der vorwiegend in der Behandlung betroffener Patienten tätig ist.
- Ein Wissenschaftler, der mit den in der CCP-IT verwalteten Daten (oder Daten ähnlichen Typs) forscht.
- Ein Datenschutzbeauftragter oder ein mit dem Thema Datenschutz vertrauter Jurist.

Zusätzlich kann ein Vertreter der Entwickler der CCP-IT in beratender Funktion hinzugezogen werden.

Seit 17. Oktober 2014 besteht der Ausschuss für Datenschutz aus den Mitgliedern des DKTK-Lenkungsausschusses und dem Datenschutzbeauftragten des DKFZ als Träger des DKTK.

5. Maßnahmen zum Datenschutz

Bei der Verarbeitung personenbezogener Daten werden die in Art. 32 Abs. 1 DSGVO genannten Schutzziele wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen berücksichtigt und eventuell bestehende Risiken (s. auch „Risikobeurteilung im Rahmen der Datenschutz-Folgenabschätzung“, Anlage 6) durch geeignete technische und organisatorische Maßnahmen dauerhaft eingedämmt. Diese Maßnahmen werden im Folgenden erläutert.

5.1 Maßnahmen zur Wahrung der Vertraulichkeit und Integrität (Art. 32 Abs.1 lit b DSGVO)

Informationelle Gewaltenteilung *(Trennungskontrolle)*

Konsequent durchgeführt wird eine informationelle Gewaltenteilung. Das bedeutet, dass die Komponenten mit unterschiedlichen Betreibern logisch, physikalisch und organisatorisch getrennt voneinander laufen, was die Gefahr eines Datenlecks verringert:

[13] Dies ist im Rahmen des Arbeitsverhältnisses an der zuständigen Institution durchzuführen und zu dokumentieren.
[14] D.h. Personen, die nicht Mitglied des DKTK-Verbunds sind.

- Das zentrale Identitätsmanagement wird getrennt betrieben von den übrigen zentralen Komponenten der CCP-IT. So kann jemand, der in der CCP-IT auf klinische oder Biomaterialdaten Zugriff hat, diese keinen realen Patienten zuordnen.
- Innerhalb des zentralen Identitätsmanagements wird der Kontrollnummernerzeuger (zu schützen ist hier das verbundweite Geheimnis) getrennt betrieben von der Patientenliste. So ist sichergestellt, dass die in der Patientenliste gespeicherten Kontrollnummern keinen direkten Rückschluss auf die Identität des Patienten zulassen.

Für die konkreten Betreiber der zentralen Komponenten vgl. Abschnitt 4.1.

Authentifizierung (*Zugangs- und Zugriffskontrolle*)

Authentifizierung von Benutzern

Die Authentifizierung von teilnehmenden Forschern (im Folgenden auch „Benutzer“) gegenüber der CCP-IT erfolgt über Benutzername und Passwort gegenüber einem zentralen Authentifizierungsdienst. Im Fall von Mitarbeitern an DKTK-Standorten wird dieser Dienst vom DKFZ betrieben. Die Prüfung von Identität und Berechtigung von Benutzern erfolgt dabei auf Standort- oder Projektebene. Dazu wird pro Standort bzw. -Projekt eine zuständige Person ernannt, welche die Anträge zum Zugriff auf die CCP-IT entgegennimmt, Identität und Berechtigung prüft und dann dem DKFZ die freizuschaltenden Personen mitteilt.

Im Fall von Forschern an Standorten von DKTK-Kooperationspartnern erfolgt die Authentifizierung bevorzugt über den Authentifizierungsdienst DFN-AAI[15]. Falls die Authentifizierung über DFN-AAI an einem Standort nicht implementiert ist, erhalten Nutzer an diesen Standorten Nutzerkonten am DKFZ mit den entsprechenden Berechtigungen nach obigem Modell.

Im Fall von externen Forschern prüft der Ausschuss für Datenschutz Identität und Berechtigung und veranlasst die Freischaltung durch das DKFZ.

Die Freischaltung von Benutzern des Brückenkopfs erfolgt direkt durch den jeweiligen Standort. Dabei sind lokale Regelungen des Datenschutzes (zum Beispiel Sichtbarkeit bestimmter Patienten in bestimmten Abteilungen) zu berücksichtigen.

Bei seiner Anmeldung an der CCP-IT wird jeder Nutzer über seine Rechte und Pflichten im Rahmen einer Nutzungsvereinbarung informiert. Die Bestätigung der Vereinbarung durch den Nutzer wird protokolliert und ist Voraussetzung zur Freischaltung für die Plattform.

Authentifizierung von Komponenten

Zugriffe einer CCP-IT-Komponente auf eine andere über das Internet erfolgen nur nach erfolgreicher Authentifizierung, d.h. nicht nur die Berechtigung (Autorisierung), sondern auch die Identität der zugreifenden Komponente wird geprüft.

[15] Die DFN-AAI-Föderation ist ein Dienst des DFN-Vereins für wissenschaftliche Einrichtungen (Universitäten, Institute) und Anbieter (kommerziell und nicht kommerziell). Sie schafft das notwendige Vertrauensverhältnis sowie einen organisatorischen und technischen Rahmen für den Austausch von Benutzerinformationen zwischen Einrichtungen und Anbietern. Für mehr Informationen siehe: https://www.aai.dfn.de.

Maßnahmen in der IT-Infrastruktur

Sicherheit der gespeicherten Daten *(Zugriffskontrolle)*

Alle in den zentralen Komponenten der CCP-IT erhobenen Daten werden auf verschlüsselten Festplattenpartitionen gespeichert. Der zugehörige Schlüssel befindet sich jeweils auf einem getrennten Medium pro Server (z.B. Papier, USB-Stick). Dieses Medium wird nur während des Mount- bzw. Bootvorgangs benötigt und wird ansonsten sicher verwahrt. Nur der Administrator des jeweiligen Servers hat Zugriff auf „sein" Schlüsselmedium. Der Schlüssel kann nicht errechnet werden. Alle Server befinden sich in Rechenzentren, die über eine personengebundene Zugangskontrolle (zum Beispiel per Chipkarte) verfügen.

Sicherheit der Kommunikation *(Weitergabekontrolle)*

Die Vertraulichkeit der Kommunikation zwischen den Komponenten wird durch folgende Maßnahmen sichergestellt:

- Die Kommunikation zwischen den Komponenten erfolgt grundsätzlich über verschlüsselte Verbindungen (HTTPS). Die dafür eingesetzten Schlüssel und Zertifikate sind so zu erstellen, dass sie den aktuell anerkannten Anforderungen entsprechen (z.B. Schlüssellänge).
- Durch Firewalls wird sichergestellt, dass die Server, auf denen die zentralen Komponenten laufen, nur über diejenigen Protokolle und Ports erreichbar sind, die für die Kommunikation mit Benutzern oder anderen Komponenten erforderlich sind (in der Regel HTTPS-Verbindungen). Der administrative Zugang ist auf das Intranet des Betreibers beschränkt.
- Alle Kommunikationsvorgänge zwischen dem Brückenkopf und zentralen Komponenten werden vom Brückenkopf initiiert. Der Brückenkopf kann dadurch hinter einer Firewall oder einem Proxyserver betrieben werden, ohne über eine öffentliche Adresse aus dem Internet erreichbar zu sein. Jeder Brückenkopf besitzt einen individuellen Schlüssel und kann nur mit diesem mit zentralen Komponenten kommunizieren. Durch dieses Schlüssel-Schloss-Prinzip soll sichergestellt werden, dass ein Standort nicht die Rolle eines anderen Standortes einnehmen kann.

Protokollierung (*Eingabekontrolle*)

Es erfolgt eine Protokollierung der Zugriffe von Forschern auf die Komponenten sowie zwischen den Komponenten untereinander. Das Protokoll enthält mindestens:

- Die Identität der zugreifenden Person oder Komponente.
- Datum und Uhrzeit des Zugriffs.
- Den Inhalt des Zugriffs (die übermittelten Daten, ggfls. aggregiert) oder Informationen, aus denen dieser rekonstruiert werden kann (z.B. Verweis auf einen Datenbankeintrag o.ä.). Davon ausgenommen ist die Übertragung von IDAT an den Kontrollnummerngenerator.

Das Protokoll wird zusammen mit den Nutzdaten des entsprechenden Servers gespeichert und zwischen einem und sechs Monaten aufbewahrt. Die aufgezeichneten Daten werden nur für folgende Zwecke verarbeitet und eingesehen:

- Im Rahmen der technischen Administration (insbesondere zur Fehlersuche).
- Zur Aufdeckung möglicher Missbrauchsfälle.
- Zur Erstellung anonymisierter Nutzungsstatistiken.

Über die Protokollierung wird der Nutzer bei seiner ersten Anmeldung an der CCP-IT informiert.

5.2 Verfügbarkeit und Belastbarkeit

Die für eine Komponente Verantwortlichen verpflichten sich, geeignete Maßnahmen zu ergreifen, damit die von den jeweiligen Komponenten verarbeiteten Daten ohne signifikante Einschränkungen verfügbar sind, beispielsweise durch regelmäßige und umfassende Datensicherungen.

Ebenso werden die jeweiligen Verantwortlichen Maßnahmen ergreifen, um die Daten bei einem eventuellen Verlust innerhalb einer angemessenen Zeit und vollständig wiederherzustellen.

5.3 Vertragsbeendigung durch einzelne Verbundpartner

Scheidet ein einzelner Partner aus der CCP-IT aus, übergibt er bei Beendigung des Vertrags eine Dokumentation der Patienteneinwilligungen an den Betreiber des zentralen Identitätsmanagements oder ggfls. einen Treuhänder. Auf Grundlage dieser Dokumentation prüfen die Betreiber der zentralen Komponenten, ob weiterhin eine Rechtsgrundlage zur Datenverarbeitung vorliegt und die Daten ggfls. zu anonymisieren oder zu löschen sind.

5.4 Überprüfung und Aktualisierung der benötigten Maßnahmen

Das in Artikel 32 Abs. 1 lit. d DSGVO geforderte Verfahren zur Überprüfung und Aktualisierung der Maßnahmen zum Datenschutz obliegt den Standorten in Bezug auf die lokalen Komponenten, dem DKFZ in Bezug auf die zentralen Komponenten. Auf Verlangen müssen geeignete Dokumente vorgelegt werden. Die jeweils Verantwortlichen dokumentieren die Verarbeitungstätigkeit im Sinne des Artikels 30 DSGVO.

6. Wahrung von Betroffenenrechten

Wie unter 1.3 dargelegt, behandelt dieses Datenschutzkonzept ausschließlich die Prozesse zur übergreifenden Vernetzung von Standorten innerhalb der CCP-IT. Im Folgenden werden daher Maßnahmen zur Wahrung der Betroffenenrechte beschrieben, die sich auf zentrale Prozesse und Komponenten beziehen. Entsprechende Maßnahmen in Bezug auf lokale Prozesse obliegen den Standorten (s. auch Anlage 0).

6.1 Aufklärung und Einwilligung

Im Falle von *explizit eingewilligten Patienten* ist die informierte Einwilligung (siehe Anlage 1) Rechtsgrundlage der Datenverarbeitung. Mit der Einwilligung erklärt sich der Patient insbesondere dazu bereit, dass

- seine identifizierenden Daten an das zentrale Identitätsmanagement übermittelt werden,
- medizinische Daten gemäß MDS-K und MDS-B an die zentrale MDS-Datenbank übermittelt werden und
- diese Daten von Forschern des DKTK und dessen Kooperationspartner gemäß der Funktionsweise der zentralen Suche durchsucht werden können.

Sofern möglich, sollte eine solche Einwilligung von jedem *nicht explizit eingewilligten Patienten*, dessen Daten im Brückenkopf gespeichert werden, in der Folge eingeholt werden (in der Regel beim nächsten Patientenkontakt). Mit Einholen der Einwilligung wird der Patient außerdem über sein Recht auf Auskunft und Widerruf informiert.

6.2 Rechtsgrundlage bei *nicht explizit eingewilligten Patienten*

Daten von Patienten *ohne explizite Einwilligung* für die Verwendung der Daten und/oder Proben durch das DKTK liegen unter der Hoheit des behandelnden Standorts. In Bezug auf die Patientenrechte sind also die lokalen Regelungen des Standorts zu berücksichtigen.

Es ist zwischen a) der Speicherung im Brückenkopf und b) dem Upload von Daten in die zentrale MDS-Datenbank zu unterscheiden.

a) Die Erhebung und Speicherung der Daten von Patienten von *nicht explizit eingewilligten Patienten* erfolgt nur in der behandelnden Institution. Dennoch reicht der Behandlungsvertrag nicht als Rechtsgrundlage für diese Datenverarbeitung aus. Ähnlich wie zum Beispiel bei einem Clinical Data Warehouse verfolgt die Speicherung in diesem Fall nämlich nicht mehr den ursprünglichen Zweck der medizinischen Versorgung, sondern dient der medizinischen Forschung. Hier ist zunächst zu prüfen, ob eine lokale Einwilligung in die Verwendung und Weitergabe von klinischen Daten und/oder Biomaterialproben (i.d.R. nach Ethik-Votum für standortübergreifende Forschungsprojekte) als Rechtsgrundlage für diese Datenverarbeitung vorliegt. Falls dies nicht zutrifft, sind die jeweiligen landesrechtlichen Regelungen mit den entsprechenden Ausnahmetatbeständen zu prüfen. Sollten diese im Einzelfall eine Verwendung von Bestandsdaten aus dem Behandlungskontext für die medizinische Forschung zulassen, können diese auch ohne Einwilligung verwendet werden. Ebenso ist die Speicherung von Daten von *nicht explizit eingewilligten Patienten* im Brückenkopf unbedenklich, sofern sichergestellt ist, dass diese Daten auch nach der Speicherung im Brückenkopf nur von der behandelnden Einheit eingesehen werden können (vgl. Abschnitt 7, „Lokale Umgebung“).
Falls es für einen der beteiligten Standorte keine spezialgesetzlichen Ermächtigungsregelungen für die Verwendbarkeit der Daten aus dem Behandlungskontext zu Forschungszwecken (z.B. Landeskrankenhausregelungen) gibt, so kann eine Erhebung der Daten von *nicht explizit eingewilligten Patienten* auf Basis der Forschungsklauseln des jeweiligen Landesdatenschutzrechts (für öffentliche Stellen der Länder) oder des Bundesdatenschutzgesetzes (für Stellen in privater Trägerschaft) möglich sein. Die Regelungen sehen eine Verarbeitung personenbezogener Daten auch ohne Einwilligung vor, wenn „dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann“[16]. Im Fall der *nicht explizit eingewilligten Patienten* ist aus folgenden Gründen davon auszugehen, dass diese Anforderungen erfüllt werden:
   - Die Wichtigkeit der translationalen Krebsforschung ist in der Fachwelt anerkannt. Ihre Förderung durch das BMBF und andere öffentliche Stellen belegt das große öffentliche Interesse an den Forschungszielen des DKTK. Im Sinne des Gesetzes ist das „wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens“ hoch anzusetzen.
   - Die Daten dieser Patienten verlassen nicht die Institution, die sie ohnehin erhoben und gespeichert hat. Der Personenkreis, der diese Daten einsehen kann, ändert sich durch die Speicherung im Brückenkopf also nicht, lediglich die Zweckbindung an die Behandlung entfällt. Die Pseudonymisierung der Daten erschwert zudem die Reidentifizierung des Patienten aus den Daten im Brückenkopf. Das Interesse des Patienten daran, diese Datenverarbeitung zu verhindern, kann deshalb im Vergleich zum wissenschaftlichen Interesse als gering angesehen werden.
   - Wegen der immer stärkeren Zergliederung der Forschung im Bereich der Onkologie, mit zahlreichen molekular definierten Subgruppen, wird in Zukunft weder ein Standort alleine über die für Forschungsprojekte ausreichende Menge an Daten verfügen, noch wird die Anzahl der *explizit eingewilligten Patienten* in absehbarer Zeit groß genug für die wissenschaftlichen Ziele des DKTK sein. Die Bedingung, dass „der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann“ ist damit ebenso als erfüllt anzusehen.

[16] §13, Abs. 2, Bundesdatenschutzgesetz. Diese Stelle ist beispielhaft erwähnt, im konkreten Fall gelten ggfls. entsprechende Regelungen der Landesdatenschutzgesetze. Da an dieser Stelle nicht alle möglichen lokal gültigen Ausnahmetatbestände erfasst werden können, ist eine Prüfung vor Ort erforderlich.

- Eine Beschränkung auf Daten *explizit eingewilligter Patienten* würde zu einem Bias in den Suchergebnissen der Plattform führen, da auch innerhalb jedes Standorts manche Kliniken eine Patienteneinwilligung erfolgreich ausrollen und andere nicht. Es ist also im Sinne einer repräsentativen Datenbasis notwendig, eine solche Selektion zu vermeiden.

b) Beim Upload von Daten in die zentrale MDS-Datenbank verlassen MDAT die behandelnde Institution. Daher muss, zusätzlich zur Rechtsgrundlage für die Speicherung von Daten im Brückenkopf (a), geprüft werden, ob der Upload des datensparsamen MDS (siehe Anlage 0) durch eine lokale Patienteneinwilligung oder durch landesrechtliche Regelungen datenschutzrechtlich legitimiert ist. Dies kann zum Beispiel dann gegeben sein, wenn die lokale Patienteneinwilligung eine pseudonymisierte Weitergabe der erhobenen Daten erlaubt, oder wenn der zu übermittelnde Datensatz als anonym betrachtet wird. In letzterem Fall sind die übermittelten Daten nicht mehr als personenbezogen anzusehen und unterliegen dadurch nicht den Datenschutzgesetzen (siehe Anlage 0).

Sofern möglich, sollte von *nicht explizit eingewilligten Patienten*, deren Daten im Brückenkopf gespeichert werden, in der Folge eine explizite Einwilligung eingeholt werden (in der Regel beim nächsten Patientenkontakt). Falls der Patient diese ablehnt, sind die bereits gespeicherten Daten zu löschen. Daten von Patienten, die der Verwendung ihrer Daten zu Forschungszwecken generell widersprochen haben, dürfen nicht in den Brückenkopf importiert werden.

6.3 Auskunft und Berichtigung

Alle Patienten, deren Daten in den technischen Komponenten verwendet werden, haben das Recht, Auskunft über die in der CCP-IT über sie gespeicherten Daten zu erhalten. Der Antrag auf Auskunft ist an die behandelnde Klinik zu stellen. Der Betreiber der lokalen Patientenliste im Brückenkopf der Klinik vergibt für den Auskunftsvorgang eine eindeutige, nicht-sprechende[17] Fallnummer und meldet diese an den Antragsteller zurück. Die Anfrage wird nun, unter Nennung der Fallnummer und der MDS∗G-ID, aber ohne Nennung der $BK_{\#}$-ID, an den Betreiber der zentralen MDS-Datenbank weitergeleitet. Dieser erstellt einen menschenlesbaren Ausdruck der Daten (mit Ausnahme der MDS∗G-ID) und stellt diese unter Nennung der Fallnummer in einem versiegelten Umschlag der zuständigen Klinik zu. Diese kann nun anhand der Fallnummer den Patienten identifizieren und ihm den Ausdruck aushändigen.

Die in der zentralen Patientenliste gespeicherten Kontrollnummern liegen nicht in menschenlesbarer Form vor und können prinzipiell nicht in die ursprünglich eingegebenen Klartextdaten zurücktransformiert werden (vgl. Abschnitt 3.2). Eine Auskunft über diese Daten findet deshalb nur auf ausdrücklichen Wunsch des Patienten statt. In Antwort auf den allgemeinen Antrag auf Auskunft wird der Patient darüber informiert, dass eine Mitteilung der IDAT aufgrund der Chiffrierung impraktikabel ist und auf sein Recht, dennoch einen Ausdruck dieser Daten anzufordern, hingewiesen.

Erlangt ein Patient Kenntnis davon, dass die über ihn gespeicherten Daten falsch sind, kann er sich zum Zwecke der Berichtigung seiner Daten an die behandelnde Klink wenden. Diese wird die Korrektur der Daten in den Primärsystemen vor Ort veranlassen. Über die in Kapitel 3 beschriebenen Prozesse werden in der Folge auch die in den verschiedenen Komponenten vorliegenden Daten des betroffenen Patienten aktualisiert.

Möchte ein betroffener Patient von seinem Recht auf Datenübertragbarkeit Gebrauch machen, muss er sich ebenfalls an die behandelnde Klinik wenden. Diese wird, wie oben beschrieben, einen Auskunftsvorgang in die Wege leiten und die vorhandenen Daten in einer maschinenlesbaren Form zur Verfügung stellen.

[17] D.h. für Dritte ist kein Rückschluss auf Daten oder Pseudonyme des Patienten möglich.

6.4 Beschwerde

Sämtliche Patienten, deren Daten in den technischen Komponenten verwendet werden, haben das Recht, Beschwerde über die Verarbeitung ihrer Daten einzulegen. Die Beschwerde ist an den Datenschutzbeauftragten des DKFZ (datenschutz@dkfz.de) zu richten. Unberührt hiervon gilt das Recht auf Beschwerde bei einer Aufsichtsbehörde.

6.5 Widerruf, Löschung, Anonymisierung

Sämtliche Patienten, deren Daten in den technischen Komponenten verarbeitet werden, haben unter bestimmten Bedingungen (vgl. DSGVO Art. 18) das Recht, eine Einschränkung der Verarbeitung ihrer Daten zu verlangen und eine bereits gegebene Einwilligung in die Verarbeitung ihrer Daten in der CCP-IT zu widerrufen. Beide Fälle werden durch die CCP-IT auf dieselbe Weise bearbeitet und im Folgenden als „Widerruf" bezeichnet. Der Widerruf ist an einen der Standorte (in der Regel die behandelnde Klinik) zu richten. Der betroffene Patient kann mit dem Widerruf zusätzlich die vollständige Löschung seiner Daten beantragen. Fehlt dieser Antrag, so erfolgt eine Anonymisierung.

Nach Prüfung des Widerrufs wird der Antrag auf Löschung oder Anonymisierung zunächst an den Betreiber der lokalen Patientenliste weitergeleitet. Zwecks Löschung oder Anonymisierung der Daten in der zentralen Patientenliste wird deren Betreiber die $BK_{\#}G$-ID des Patienten mitgeteilt, entsprechend den Betreibern der CCP-Anwendungen die anwendungsspezifischen IDs des Patienten. Im Falle einer Löschung werden alle dem Patienten zugeordneten Datensätze in den Patientenlisten und den CCP-Anwendungen gelöscht. Im Falle der Anonymisierung werden die Datensätze in den Patientenlisten gelöscht und in den Datensätzen der CCP-Anwendungen die anwendungsspezifischen IDs des Patienten jeweils durch ein zufälliges Pseudonym ersetzt. Durch den Algorithmus zur Pseudonymerzeugung ist sichergestellt, dass die Pseudonyme eines gelöschten oder anonymisierten Patienten am jeweiligen Standort nicht mehr für neue Patienten verwendet werden.

Die Löschung bzw. Anonymisierung ist von den zuständigen Betreibern zeitnah, maximal innerhalb von 14 Werktagen, vorzunehmen[18]. Der Betreiber der zentralen Patientenliste informiert wiederum alle Standorte über die Löschung oder Anonymisierung. In den Standorten werden eventuell lokal gespeicherte Daten des Patienten gelöscht, oder (bei Anonymisierung) die $BK_{\#}G$-IDs durch $BK_{\#}L$-IDs ersetzt[19]. Dieser Vorgang wird protokolliert und dem Betreiber der zentralen Patientenliste bestätigt.

Der Abschluss der Löschung oder Anonymisierung wird von den Betreibern der CCP-Anwendungen und der zentralen Patientenliste dem Standort, an dem der Widerruf eingegangen ist, mitgeteilt und von diesem dem Patienten schriftlich bestätigt. Eine entsprechende Mitteilung ergeht auch an den Datenschutzbeauftragten am DKFZ.

6.6 Dauer der Speicherung

Die erhobenen Daten bleiben in den zentralen Komponenten der CCP-IT gespeichert, so lange es für sie eine sinnvolle wissenschaftliche Verwendung im Rahmen der Patienteneinwilligung gibt. Falls die Daten nicht mehr in der vorgesehenen Form genutzt werden können (z.B. falls die CCP-IT außer Betrieb genommen wird), prüft der Ausschuss für Datenschutz, ob eine Rechtsgrundlage für eine anderweitige Verwendung der Daten, gegebenenfalls in anonymisierter Form, besteht. Falls diese Prüfung negativ ausfällt, sind die zentralen Daten zu löschen. Hinsichtlich der nur lokal in den Brückenköpfen gespeicherten Daten ist die Entscheidung über den weiteren Umgang mit den Daten von jedem Standort individuell zu treffen, da diese Daten möglicherweise weiter für Behandlungszwecke oder eigene Forschungsvorhaben genutzt werden dürfen.

[18] Die meist impraktikable Löschung oder Anonymisierung in Datensicherungen ist verzichtbar, sofern die Sicherungen nur durch den zuständigen Systemadministrator eingesehen werden können und alte Sicherungen regelmäßig gelöscht werden.

[19] Der Patient wird also im Sinne der CCP-IT von einem *explizit eingewilligten* zu einem *nicht explizit eingewilligten* Patienten.

7. Lokale Umgebung

Bei Installation und Betrieb der Brückenköpfe sind die lokalen Bestimmungen des Standorts hinsichtlich Datenschutz und -sicherheit zu beachten. Generell werden die für den Betrieb der zentralen Komponenten genannten Maßnahmen (siehe Abschnitt 5.1, „Maßnahmen in der IT-Infrastruktur“) empfohlen. Da die Komponenten des Brückenkopfes über das Intranet der jeweiligen Einrichtungen kommunizieren, kann hier auf die Verwendung verschlüsselter Verbindungen verzichtet werden.

Sofern der Brückenkopf nicht von der behandelnden Einheit selbst betrieben wird, ist durch Zugriffsrechte sicherzustellen, dass deren Datenhoheit gewahrt bleibt. Die Regelungen hinsichtlich administrativer Zugriffe (Abschnitt 4.3) gelten entsprechend.

Sollte trotz getroffener Sicherheitsmaßnahmen eine Datenpanne eintreten, ist der Prozess bei meldepflichtigen Datenpannen (Art. 33 und 34, DSGVO) vom betroffenen Standort durchzuführen. Außerdem ist der Datenschutzbeauftragte des DKFZ unverzüglich darüber zu informieren.

7.1 Lokale Bestimmungen für den Standort [Standort]

[Sollte es abweichende Bestimmungen für die lokal an Ihrem Standort laufenden Komponenten oder Prozesse geben, können Sie diese hier einsetzen. Andernfalls löschen Sie den Abschnitt.]

Anhang

1. Patienteneinwilligung DKTK

Eine Mustererklärung ist beim CCP Office verfügbar. Sie dient als Vorlage, die von jedem Standort an lokale Erfordernisse angepasst wird. Diese tatsächlich eingesetzte Einwilligungserklärung erhalten Sie beim Standortvertreter in der AG CCP-IT. Autor der Mustererklärung ist das CCP Office; zuständiger Ansprechpartner ist:

Barbara Uhl
Wissenschaftliche Projektkoordination

Deutsches Konsortium für Translationale Krebsforschung (DKTK)
CCP-Office

Universitätsklinikum Frankfurt
Med. Klinik II
Haus 33, Zi. 208
Theodor-Stern-Kai 7
60590 Frankfurt am Main

Tel.: +49 (0)69 / 6301 84237
Fax: +49 (0)69 / 6301 7463
E-Mail: b.uhl@dkfz.de

2. Anonyme Weitergabe festgelegter sparsamer Datensätze in die zentrale MDS-Datenbank zum Zweck der Machbarkeitsanalysen für Forschungsprojekte

Die Sachlage zur Anonymität der Datensätze in der zentralen MDS-Datenbank wurde federführend vom CCP Office erstellt; zuständiger Ansprechpartner ist:

Kristina Ihrig
Wissenschaftliche Projektkoordination

Deutsches Konsortium für Translationale Krebsforschung (DKTK)
CCP-Office

Universitätsklinikum Frankfurt
Med. Klinik II
Haus 33, Zi. 208
Theodor-Stern-Kai 7
60590 Frankfurt am Main

Tel.: +49 (0)69 / 6301 84237
Fax: +49 (0)69 / 6301 7463
E-Mail: k.ihrig@dkfz.de

DKTK: Anonyme Weitergabe festgelegter sparsamer Datensätze in die zentrale MDS-Datenbank zum Zweck der Machbarkeitsanalysen für Forschungsprojekte

Hintergrund:

Die folgenden Erläuterungen dienen der Einschätzung, ob lokal vorliegende Patientendaten (festgelegter Meldedatensatz (MDS[1])) in die zentrale MDS-Datenbank (DB) auf Basis **der Datenschutzgesetze** weitergegeben werden dürfen.

Der Zweck der zentralen MDS-DB ist die Machbarkeitsprüfung von Forschungsprojekten mit Hilfe der Anzeige einer Fallzahl von Suchergebnissen.

Das Bundesdatenschutzgesetz (BDSG) und die LDSG bzw. BlnDSG greifen nicht, wenn Daten anonymisiert worden sind[2]. Gemäß BDSG[3]/anderer DSG[4] besteht Anonymität, wenn „Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“.

Für den am teilnehmenden Standort stattfindenden datenverarbeitenden Schritt der Pseudonymisierung oder Anonymisierung liegt eine Einwilligung des Patienten vor.

Daraus resultiert, dass die Weitergabe von Daten in die zentrale MDS-DB für die zentrale Suche zum Zweck der Machbarkeitsprüfung von Forschungsprojekten zulässig ist, da die Anonymität gewährleistet ist.

Informationen zur Anonymität der zentralen MDS-DB:

- Die Inhalte eines Datensatzes sind reduziert (datensparsam).
- Ein Datensatz enthält keine personenbezogenen Daten (z.B. Klarnamen).
- Die Daten zu Biomaterial eines Patienten beziehen sich auf verwaltende Angaben (z.B. Tumorgewebe, Normalgewebe).
- Die klinischen Daten eines Patienten sind eine Teilgruppe des ADT[5]-Basisdatensatzes, der im Rahmen des KFRG[6] an andere Datenbanken weitergegeben werden darf.
- Die zentrale MDS-DB enthält ein Pseudonym mit einer Standortinformation als ein doppelt verschlüsseltes Pseudonym (MDS-Pseudonym), mit dem Ziel, wiederholte Datenimporte von den Standorten inkrementell durchzuführen. Dadurch werden höchste technische Anforderungen beachtet und faktisch Anonymität erreicht (siehe Datenschutzkonzept, Abschnitt 3.4 und 3.1, 10.10.2014). Dies ist durch die TMF e.V. bereits positiv begutachtet worden.

Zuständige Ansprechperson im DKTK:

Kristina Ihrig, Dipl.-Biol. (CCP Office)
E-Mail: k.ihrig@dkfz.de
Tel.: 069-6301-84237

[1] Meldedatensätze
[2] Metschke, Wellenbrock (2002): Datenschutz in Wissenschaft und Forschung
[3] BDSG, §3, Abs. 6
[4] Bayern, Berlin, Baden-Württemberg, Hessen, Rheinland-Pfalz; SächsDSG modifiziert
[5] Arbeitsgemeinschaft Deutscher Tumorzentren e.V. und GEKID
[6] Krebsfrüherkennungs- und Registergesetz

3. Votum der AG Datenschutz der TMF

Die Arbeitsgruppe Datenschutz der Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF e.V.) hat zu diesem Datenschutzkonzept in seiner Fassung vom 28.02.2019 das anhängende Votum ausgesprochen.

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

TMF e. V. · Charlottenstraße 42/Dorotheenstraße · 10117 Berlin

Berlin, 13. März 2019

Stellungnahme zum Datenschutzkonzept für die Clinical Communication Platform (CCP-IT) im Deutschen Konsortium für Translationale Krebsforschung (DKTK)

Das Datenschutzkonzept für die CCP-IT wurde von der TMF-Arbeitsgruppe „Datenschutz" mehrfach, zuletzt auf der Sitzung am 13. März 2019, beraten. Der AG liegt das Konzept in der Version vom 28. Februar 2019 vor. Es handelt sich um eine Fortschreibung des Konzepts vom 8. Januar 2014, das am 16. Januar 2014 von der Arbeitsgruppe befürwortet wurde.

Das vorliegende Konzept beschreibt eine Plattform, die neben der Bereitstellung von Infrastruktur-Komponenten (wie Datenintegrations-, Pseudonymisierungs- und Authentifizierungsprozessen) vor allem Anfragen nach Fallzahlen und Machbarkeit von Forschungsprojekten ermöglichen soll. Zu diesem Zweck werden medizinische Daten von Krebspatienten (einschließlich Hinweisen auf vorhandene Biomaterialproben) der teilnehmenden Kliniken pseudonymisiert in einer zentralen Datenbank, der „MDS-Datenbank", gesammelt, in der Regel beruhend auf einer entsprechenden Einwilligung der betroffenen Patienten. Da die Datenbank Pseudonyme verwendet, die ansonsten nur in der Patientenliste bekannt sind, erfüllt das Konzept die Anforderungen an das Klinische Modul des TMF-Datenschutzleitfadens. Im zentralen Identitätsmanagement können auch verschiedene Pseudonyme (im Sinne eines Privacy Preserving Record Linkage) verknüpft werden. Insofern, als

- überhaupt kein Online-Zugriff außer statistischen Abfragen auf die zentrale Datenbank vorgesehen ist,
- ein zusätzlicher Schutz durch die Umwandlung lokaler in globale Pseudonyme eingerichtet ist,

ist das Konzept sogar deutlich strenger als das generische TMF-Konzept. Die konkrete Ansiedlung der Datenbanken bei verschiedenen Institutionen unterstützt eine wirksame informationelle Gewaltenteilung. Die Besetzung des Ausschusses Datenschutz ist konkret in Form der beteiligten Rollen beschrieben.

Parallel dazu sollen aber auch Daten von Patienten nutzbar gemacht werden, für die keine explizite (DKTK-) Einwilligung vorliegt. Hierbei handelt es sich um „Altfälle", auch von Kooperationspartnern, die onkologische Spitzenzentren, aber nicht Mitglieder des DKTK sind. Die Erforderlichkeit, solche Fälle ohne vorliegende explizite Einwilligungserklärung einzubeziehen, ist im Abschnitt 6.2 des Konzepts ausführlich begründet. Zunächst sind dies sehr viele, die Anzahl wird aber im Laufe der Zeit abnehmen, da neue Fälle grundsätzlich nur mit Einwilligung aufgenommen werden, und bei Altfällen die Einwilligung nach Möglichkeit (bei Weiterbehandlung) nachgeholt werden soll. Für die Daten dieser Patienten, als „nicht explizit eingewilligte Patienten" bezeichnet, sind je nach Rechtslage zwei Optionen vorgesehen:

- Sie werden nur in den behandelnden Einrichtungen in einem sogenannten Brückenkopf gespeichert, der nicht von außerhalb zugänglich ist. Dieser ist nach dem Modell eines klinischen Data-Warehouse konzipiert und muss natürlich den entsprechenden lokal geltenden Datenschutzregeln genügen. Hierfür beherbergt er ein lokales

TMF e. V.
Charlottenstraße 42/Dorotheenstraße
D-10117 Berlin
Tel.: +49 (30) 22 00 24 70
Fax: +49 (30) 22 00 24 799
E-mail: info@tmf-ev.de
Internet: www.tmf-ev.de

Commerzbank AG
BLZ: 100 400 00
Kto.: 737 811 000
IBAN: DE60 1004 0000 0737 8110 00
BIC: COBADEFFXXX
St-Nr.: 27/640/56509
USt-IdNr.: DE244871253

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Identitätsmanagement, das natürlich auch an anderer Stelle (des gleichen Standorts) angesiedelt sein kann. Die Plattform erlaubt keine direkten Abfragen auf die zugehörigen Datenbestände dieser Patienten, sondern dient nur zur Vermittlung von externen Anfragen nach Fallzahlen, die vor Ort außerhalb dieses Systems im Rahmen der rechtlich erlaubten Möglichkeiten bearbeitet werden. Die Bearbeitung solcher Anfragen betrifft nicht die Plattform selbst und ist daher nicht Gegenstand des vorliegenden Datenschutzkonzepts.

- Unter der Voraussetzung, dass die am Ort der Entstehung geltenden Datenschutzregeln einen pseudonymisierten Datenexport erlauben, z. B. aufgrund einer vom DKTK unabhängigen Einwilligung für Forschungszwecke oder Forschungsklauseln in einem Landeskrankenhausgesetz, wird ein reduzierter Datensatz nach expliziter Freigabe in die zentrale Datenbank geladen. Die Prüfung der Zulässigkeit liegt in der Verantwortung der kooperierenden Einrichtung. Da in diesem Fall kein globales Pseudonym erzeugt wird, ist hierbei eine Verknüpfung mit Daten derselben Person aus anderen Quellen nicht möglich.

Neu im Vergleich zum Konzept von 2014 sind im Wesentlichen die Punkte:

- Anpassungen an die DSGVO,
- Einbeziehung zusätzlicher Kooperationspartner in Form von behandelnden Einrichtungen, die nicht Mitglieder des DKTK sind,
- zusätzliche Anwendungsfälle („CCP-Anwendungen"), die die Infrastruktur und auch die Datenbank der Plattform nutzen,
- eventuelle Speicherung von Daten in der zentralen Datenbank ohne explizite Einwilligung,
- Modifikationen in den Pseudonymisierungsprozessen.

Verantwortliche Stelle für die Datenverarbeitung ist das Deutsche Krebsforschungszentrum (DKFZ) in Heidelberg, z. T. in gemeinsamer Verantwortung mit den teilnehmenden Kooperationspartnern.

Die AG Datenschutz sieht in dem Teil des Konzepts, der Patienten mit Einwilligung betrifft, eine Umsetzung einer strengeren Variante des Klinischen Moduls des TMF-Datenschutzleitfadens. Der Teil, der für Patienten ohne Einwilligung nur die Weiterleitung von externen Anfragen vorsieht, wird als unproblematisch bewertet. Nicht Gegenstand dieser Stellungnahme sind

- die Einwilligungserklärungen, die in der jeweiligen Verantwortung der teilnehmenden Einrichtungen liegen,
- die rechtlich bindenden vertraglichen Regelungen mit Kooperationspartnern,
- die rechtliche Würdigung der eventuellen zentralen Speicherung von Daten ohne Einwilligung aufgrund spezieller Rechtsgrundlagen,
- die Datenschutzkonzepte von CCP-Anwendungen, insbesondere die Einschätzung des Reidentifizierungsrisikos durch Speicherung zusätzlicher Daten.

Ansonsten hat die AG keine Einwände gegen das vorgelegte Konzept.

Prof. Dr. Klaus Pommerening
Sprecher der AG Datenschutz
und verantwortlicher Berichterstatter

13.03.2019 21:28

4. Aktueller Meldedatensatz (MDS)

Der **MDS-K** (klinische Daten) enthält Attribute, wodurch klinische Daten zum Patienten, zum Primärtumor, zur Primärtherapie, zum Ansprechen und zum Vitalstatus für die zentrale Suche der zentralen MDS-Datenbank zur Verfügung stehen.

Der **MDS-B** (Biomaterialdaten) enthält 5 Attribute, welche eine eindeutige Identifizierung des Biomaterials erlauben.

Nr.	Merkmal
Allgemeine Daten	
A-0	Standortpseudonym
A-1	Geburtsmonat/-jahr (nicht durchsuchbar; Berechnung des Alters)
A-2	Geschlecht
Klassifikation von Primärtumoren	
K-1	Datum der TNM-Dokumentation/Datum Befund (nicht durchsuchbar)
K-2	Diagnosejahr/-datum (Jahr suchbar; Diganosedatum nicht durchsuchbar, Berechnung des Alters, Qualitätssicherung)
K-3	Alter bei Erstdiagnose
K-4	Diagnose
K-5	ICD-Katalog (Version)
K-6	Lokalisation
K-7	ICD-O Katalog Topographie (Version)
K-8	Seitenlokalisation
K-9	Morphologie
K-10	ICD-O Katalog Morphologie (Version)
K-11	Grading
K-12	UICC Stadium
K-13	TNM-T
K-14	TNM-m-Symbol
K-15	TNM-N
K-16	TNM-M
K-17	c/p/u-Präfix T
K-18	c/p/u-Präfix N
K-19	c/p/u-Präfix M
K-20	TNM-y-Symbol
K-21	TNM-r-Symbol
K-22	TNM-Version
K-23	Lokale Beurteilung Resttumor
K-24	Gesamtbeurteilung Resttumor
K-25	Fernmetastasen [ja/nein]
K-26	Datum diagnostische Sicherung (nicht durchsuchbar)
K-27	Lokalisation Fernmetastasen

Nr.	Merkmal
Generierter Suchkatalog	
K-31	Klinische-relevante Tumorentitäten: DKTK-Katalog: Übersetzung Tumorcodes für Diagnose & Morphologie in klinisch-relevante Gruppen]
Therapie des Primärtumors	
K-32	OP [ja/nein]
K-33	Intention OP
K-34	Strahlentherapie [ja/nein]
K-35	Intention Strahlentherapie
K-36	Stellung zur Operation
K-37	Chemotherapie [ja/nein]
K-38	Intention Chemotherapie
K-39	Stellung zur Operation
K-40	Immuntherapie [ja/nein]
K-41	Hormontherapie [ja/nein]
K-42	Knochenmarktransplantationen [ja/nein]
K-43	Weitere Therapie(n) [ja/nein]
Ansprechen auf Primärtherapie	
K-45	Ansprechen Primärtherapie
K-46	Datum des ersten Verlaufs (nicht durchsuchbar)
K-47	Lokales/regionäres Rezidiv
K-48	Datum (lokales/regionäres) Rezidiv (entspricht Verlaufsdatum, nicht durchsuchbar)
K-49	Lymphknoten-Rezidiv
K-50	Datum Lymphknoten-Rezidiv (entspricht Verlaufsdatum, nicht durchsuchbar)
K-51	Fernmetastasen
K-52	Datum Fernmetastasen (entspricht Verlaufsdatum, nicht durchsuchbar)
Aktueller Tumorstatus	
K-53	Ansprechen innerhalb der letzten 3 Monate
K-54	Monat.Jahr des letztbekannten Verlaufs (nicht durchsuchbar)
Vitalstatus	
K-55	Monat.Jahr des letztbekannten Vitalstatus (nicht durchsuchbar)
K-56	Vitalstatus [lebend/verstorben]
Biomaterial	
B-1	Patienten mit Biomaterial
B-2	Probentyp (z.B. Gewebeprobe)
B-3	Probenart (z.B. Tumorgewebe, Normalgewebe)
B-4	Entnahmedatum (nicht durchsuchbar)
B-5	Fixierungsart (z.B. Paraffin, Kryo/Frisch)

5. Checkliste Joint Controllership

Aufteilung der Verantwortlichkeiten im Sinne des Joint Controlling (Artikel 26 DSGVO).

ANLAGE 5: Checkliste Joint Controllership (Quelle bitkom[1])

(x) Die Kreuze stellen dar, welcher Verantwortliche, welche Aufgabe übernimmt.

Pflichten aus der DS-GVO	DKFZ	Standort
Festlegung des Zwecks und der Mittel der Datenverarbeitung	X	X
Festlegung der Art der personenbezogenen Daten	X	X
Art. 26 Abs. 1: Festlegung in einer Vereinbarung in transparenter Form, wer welche Verpflichtung gemäß dieser Verordnung erfüllt. Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln.	X (Datenschutzkonzept + Meldung der Verarbeitungstätigkeit)	X (Datenschutzkonzept + Meldung der Verarbeitungstätigkeit)
Art. 26 Abs. 1: Angabe einer Anlaufstelle für die betroffenen Personen.	X (DSK Kap.6)	
Art. 26 Abs. 2 : Das Wesentliche der Vereinbarung wird dem Betroffenen zur Verfügung gestellt.		X (Einwilligungserklärung)
Art. 27: Schriftliche Benennung eines Vertreters in der EU, falls ein Verantwortlicher nicht in der Union niedergelassen ist.	n/a	n/a
Art. 13: Informationspflicht bei Erhebung personenbezogener Daten.		X (Einwilligungserklärung)
Art. 14: Informationspflicht, wenn Daten nicht bei der betroffenen Person erhoben wurden.	n/a	n/a
Art. 15 Bearbeitung von Auskunftsverlangen.		X (DSK Kap. 6.3)
Art. 16: Bearbeitung von Berichtigungsanfragen.		X
Art. 17 o. 18: Bearbeitungen von Löschbegehren oder Beschränkung der Verarbeitung und **Art. 19** Mitteilung der Löschpflicht.	X (DSK Kap. 6.5)	X (DSK Kap. 6.5)
Art. 20: Abwicklung von Herausgabeverlangen (Datenportabilität).		X (DSK Kap. 1.3)
Art. 21: Bearbeitung von Widersprüchen.	X (DSK Kap. 6.2 und 6.5)	X (DSK Kap. 6.2 und 6.5)
Art. 24 Abs. 1 i.V. m. Art. 32: Festlegung der techn.-org. Maßnahmen nach Risikoabschätzung und ggf. Datenschutzfolgeabschätzung (Art. 35) und Konsultation einer Aufsichtsbehörde/ Übermittlung der notwendigen Informationen (Art. 36 (3)).	X (Datenschutzkonzept + Meldung der Verarbeitungstätigkeit)	X (Datenschutzkonzept + Meldung der Verarbeitungstätigkeit)
Art. 24 Abs. 1 Dokumentation der Auswahl der techn.-org. Maßnahmen (als Nachweis).	X (Datenschutzkonzept + Meldung der Verarbeitungstätigkeit)	X (Datenschutzkonzept + Meldung der Verarbeitungstätigkeit)
Art. 24 Abs. 1 Überprüfung und Aktualisierung der Maßnahmen.	X (DSK Kap. 5.4)	X (DSK Kap. 5.4)
Art. 28 Einschaltung von Auftragsverarbeitern bzw. Unterauftrags-verarbeitern und deren Überprüfung.		X (AV für Wartungszugänge)
Art. 30 Führung des Verzeichnisses der Verarbeitungstätigkeiten.	X	X
Art. 33, 34 Prozess bei meldepflichtigen Datenpannen.	X	X
Art. 37 Benennung eines Datenschutzbeauftragten.	X	X

[1] Quelle: https://www.bitkom.org/sites/default/files/file/import/170515-Joint-Controllership-online.pdf

Weitere zu empfehlende Regelungen:

Interne Ausgleichsregelung, falls einer der Verantwortlichen nach Art. 26 Abs. 3 von der betroffenen Person in Anspruch genommen wird.	n/a	n/a
Vertraulichkeitsverpflichtung.	X (DSK Kap. 4.3)	X (DSK Kap. 4.3)
Nutzung welcher Zertifikaten /Codes of Conduct		

6. Risikobeurteilung im Rahmen der Datenschutz-Folgenabschätzung

DKTK CCP-IT
Risikobeurteilung im Rahmen der Datenschutz-Folgenabschätzung
(Version 1.1 vom 23. Nov. 2020)

Definitionen und Vorgehensweise

Eine Datenschutz-Folgenabschätzung ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Dabei wird das Risiko allgemein als Produkt aus Eintrittswahrscheinlichkeit eines unerwünschten Ereignisses und der Schadensauswirkung als Konsequenz aus dem Ereignis angesehen.

Zur Risikobewertung werden Eintrittswahrscheinlichkeit und Schadenshöhe wie folgt festgelegt:
Die **Eintrittswahrscheinlichkeit** ist eine quantitative oder qualitative Angabe über die Wahrscheinlichkeit, mit der ein Risikoereignis innerhalb eines bestimmten Zeitraums eintritt.
Unter der Annahme, dass der Schadensfall eingetreten ist, gilt es, die Auswirkung des Schadens in Schweregrade einzuteilen. Der Schweregrad ist gegeben, wenn einer der unter „Beschreibung" angegebenen Punkte eintritt, wobei die höchste **Schadensauswirkung** zählt.

Schadenseintritts-wahrscheinlichkeit	**Beschreibung**
unwahrscheinlich	Der Eintritt eines Schadens soll als „unwahrscheinlich" gelten, wenn die Wahrscheinlichkeit für den Eintritt des Schadens bei weniger als 1% während der Projektlaufzeit bzw. Aufbewahrungsfrist liegt.
möglich	Als „möglich" soll gelten, wenn die Wahrscheinlichkeit für den Eintritt des Schadens bei weniger als 10% während der Projektlaufzeit bzw. Aufbewahrungsfrist liegt.
wahrscheinlich	Als „wahrscheinlich" soll gelten, wenn die Wahrscheinlichkeit für den Eintritt des Schadens bei mindestens 10% während der Projektlaufzeit bzw. Aufbewahrungsfrist liegt.

Schadensauswirkung	**Beschreibung**
unbedeutend	• Verstöße gegen Vorschriften und Gesetze haben geringfügige Konsequenzen. • Bei Schadensfällen bzgl. personenbezogener Daten kann der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen unwesentlich beeinträchtigt werden, es ist keine Beeinträchtigung der persönlichen Unversehrtheit denkbar.
moderat	• Verstöße gegen Vorschriften und Gesetze haben erhebliche Konsequenzen. • Bei Schadensfällen bzgl. personenbezogener Daten kann der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden, eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
wesentlich	• Verstöße gegen Vorschriften und Gesetze haben schwerwiegende Konsequenzen. • Bei Schadensfällen bzgl. personenbezogener Daten ist eine Gefahr für Leib und Leben oder eine Beeinträchtigung der persönlichen Freiheit des Betroffenen gegeben.

Risikomaßzahl
Für die Berechnung des Risikos werden sowohl den Eintrittswahrscheinlichkeiten als auch den Schadensauswirkungen Maßzahlen zugeordnet:

Eintrittswahrscheinlichkeit „unwahrscheinlich“ = 1
Eintrittswahrscheinlichkeit „möglich“ = 2
Eintrittswahrscheinlichkeit „wahrscheinlich“ = 3

Schadensauswirkung „unbedeutend“ = 2
Schadensauswirkung „moderat“ = 4
Schadensauswirkung „wesentlich“ = 6

Mit Hilfe der Risikomatrix wird die Risikomaßzahl als Produkt aus Eintrittswahrscheinlichkeit und Schadenauswirkung gebildet.

Eintrittswahrscheinlichkeit	**Schadensauswirkung**		
	unbedeutend (=2)	**moderat (=4)**	**wesentlich (=6)**
Unwahrscheinlich (=1)	**2**	**4**	**6**
Möglich (=2)	**4**	**8**	**12**
Wahrscheinlich (=3)	**6**	**12**	**18**

Auf Basis der berechneten Risikomaßzahlen werden drei Risikokategorien definiert:

2 - 4: kein oder geringes Risiko
6 - 12: mittleres Risiko
> 12: hohes Risiko

Bewerten des Risikos und Ermittlung der Eingriffsintensität / des Schutzbedarfs

Der Schutzbedarf einer natürlichen Person bei der Verarbeitung personenbezogener Daten in Bezug auf ihre Rechte und Freiheiten ergibt sich aus dem Risiko, das von der Verarbeitungstätigkeit und deren Eingriffsintensität ausgeht. Die DS-GVO kennt nur die Begriffe „Risiko“ und „hohes Risiko“, wobei „Risiko“ hier als „normales Risiko“ bezeichnet wird. Daneben verwendet die DS-GVO die Formulierung „voraussichtlich nicht zu einem Risiko“ führend. Da es vollständig risikolose Verarbeitungen nicht geben kann, wird die Formulierung „nicht zu einem Risiko“ von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko“ führend verstanden.

Der Schutzbedarf ergibt sich aus dem Risiko der Verarbeitungstätigkeit, bevor technische und organisatorische Maßnahmen bestimmt und umgesetzt wurden. Insofern gilt der folgende Zusammenhang zwischen Risiko(höhe), im Sinne eines Ausgangsrisikos, und Schutzbedarf(sstufe):

- kein oder geringes Risiko der Verarbeitung
- normaler Schutzbedarf für von der Verarbeitung betroffene Personen

- mittleres Risiko der Verarbeitung
- hoher Schutzbedarf für von der Verarbeitung betroffene Personen

- hohes Risiko der Verarbeitung
- sehr hoher Schutzbedarf für von der Verarbeitung betroffene Personen

Während der durch das Ausgangsrisiko definierte Schutzbedarf betroffener Personen bzgl. der Verarbeitungstätigkeit konstant bleibt, können die Risiken der Verarbeitung für die betroffenen Personen durch technische und organisatorische Maßnahmen verringert werden. Diese Maßnahmen verändern nicht den Schutzbedarf, sondern reduzieren das Risiko der Verarbeitungstätigkeit. Die zunächst vorhandenen Risiken müssen durch Verfahrensgestaltung und technische und organisatorische Maßnahmen so weit verringert werden, bis ein dem Risiko angemessenes und somit verantwortbares Schutzniveau für die Verarbeitungstätigkeit gewährleistet wird.
Bei der Identifizierung der möglichen Risiken werden Risikoquellen/Ursachen (interne und externe Personen, nicht-menschliche Quellen) sowie die möglichen Auswirkungen betrachtet.
Das Standard-Datenschutzmodell (SDM) sieht folgende Gewährleistungsziele vor:

- Datenminimierung
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Transparenz
- Nichtverkettung
- Intervenierbarkeit

Zu jedem Gewährleistungsziel werden mögliche Risiken/Schutzbedarf und die zur Minimierung dieses Risikos ergriffenen Maßnahmen nach folgendem Schema beschrieben:

Risiko	**Zugriff, Ausfall etc.**
Gefährdung/ Risikoquelle	Art der Gefährdung für den Betroffenen
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** unbedeutend bis wesentlich **Eintrittswahrscheinlichkeit:** unwahrscheinlich bis wahrscheinlich 2,4,6,8,12,18 normal, hoch
Maßnahmen	Gegenmaßnahmen
Bewertung	**Restrisiko**: Was könnte trotz Maßnahmen noch passieren? **Restrisikomaßzahl**: 2,4,6,8,12,18 **Tragbarkeit**: Wer kann das Risiko tragen? 2 - 4: kein oder geringes Risiko 6 - 12: mittleres Risiko > 12: hohes Risiko
Bemerkungen	Hinweise

1. Gewährleistungsziel: Datenminimierung

Risiko	**Upload an zentrale Suche: es werden zu viele Daten/Detailinformationen hochgeladen**
Gefährdung/ Risikoquelle	Identifizierung eines Patienten wird erleichtert, insbesondere bei Vorliegen einer seltenen Erkrankung. Es werden mehr Daten verarbeitet, als für das Erreichen des Verarbeitungszweckes erforderlich.
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** möglich 8 normal
Maßnahmen	Definition eines sparsameren Datensatzes (MDS, siehe Anhang zu DSK) für den Upload zur zentralen Suche, sowie Vergröberung der Informationen z.B. durch Verzicht auf konkrete Operationscodes oder komplettes Geburtsdatum Ergebnis liefert außerdem nur Anzahl der gefundenen Datensätze, nicht die Daten selbst, und die Zahl ist keinem individuellen Standort zuordenbar.
Bewertung	**Restrisiko**: nicht vorhanden **Restrisikomaßzahl**: 2 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

Risiko	**Erhöhte Gefahr der Re-Identifikation durch Verknüpfung mit zusätzlichen Daten aus Projekt-/Studiendatenbank**
Gefährdung/ Risikoquelle	Identifizierung eines Patienten wird durch breiteren Datenbestand erleichtert, insbesondere bei Vorliegen einer seltenen Erkrankung.
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** möglich 8 normal
Maßnahmen	Separate Pseudonyme für Patientendaten im Brückenkopf und in jeweiliger Projekt-/Studiendatenbank (für jedes Projekt eine eigene projektspezifische Patienten-ID; PSP-ID) Bei Erstanfrage wird nur die Zugehörigkeit zu einem Projekt und die entsprechende PSP-ID herausgegeben (keine MDAT). Herausgabe der MDAT erfolgt nur über direkte Freigabe durch den Projektleiter auf Basis der datenschutzrechtlichen Grundlage des jeweiligen Projektes.
Bewertung	**Restrisiko**: nicht vorhanden **Restrisikomaßzahl**: 2 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

2. Gewährleistungsziel: Verfügbarkeit

Risiko	**Daten werden von Unbefugten gelöscht**
Gefährdung/ Risikoquelle	Daten stehen, je nach Umfang der Löschung, für einen bestimmten Zeitraum nicht zur Verfügung
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** möglich 8 normal
Maßnahmen	Authentifizierungskontrolle (siehe DSK 5.1) regelmäßige Datensicherungen (siehe DSK 5.2)
Bewertung	**Restrisiko**: Dies hat keine Auswirkungen auf den Patienten (Daten werden im-Rahmen der CCP nur für Forschungszwecke verwendet; reines Forschungsprojekt). **Restrisikomaßzahl**: 2 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

Risiko	**Systemausfall**
Gefährdung/ Risikoquelle	Die zentralen CCP-Infrastrukturen und/oder die Brückenköpfe an den Standorten stehen (für Forschungsprojekte) nicht zur Verfügung
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung**: unbedeutend **Eintrittswahrscheinlichkeit**: möglich 4 normal
Maßnahmen	Siehe TOMs Betreiber, zuständiges Personal beim Betreiber Wiederherstellung
Bewertung	**Restrisiko**: Dies hat keine Auswirkungen auf den Patienten (reines Forschungsprojekt). **Restrisikomaßzahl**: 2 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

3. Gewährleistungsziel: Integrität

Risiko	**Daten werden manipuliert (verfälscht/vertauscht).**
Gefährdung/ Risikoquelle	*Zentrale Suche*: Keine Auswirkung auf die Patienten *Dezentrale Suche*: Einem Patienten kann fälschlicherweise die Teilnahme in einer nicht seiner Diagnose entsprechenden Studie vorgeschlagen werden.
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** unwahrscheinlich 4 normal
Maßnahmen	Eingaben in Formulare auf die Möglichkeit schadhafter Angriffe (Cross-Site-Scripting, SQL-Injection) untersuchen (Login, Passwort) Bereitstellen von Verhaltensregeln bei Sicherheitsvorfällen Lokale Verantwortung für Konsistenz zwischen Quellsystem und Datenbestand im Brückenkopf
Bewertung	**Restrisiko**: Fehlerhafte Daten werden nicht bemerkt. **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

Risiko	**Fehlerhafte Verknüpfung von Daten aufgrund von Pseudonymisierungsfehlern**
Gefährdung/ Risikoquelle	*Zentrale Suche*: Keine Gefährdung *Dezentrale Suche*: Einem Patienten kann fälschlicherweise die Teilnahme in einer nicht seiner Diagnose entsprechenden Studie vorgeschlagen werden. Bei häufigen Namen oder alternativen Schreibweisen von Namen können Personen fälschlicherweise als identische bzw. verschiedene Personen zugeordnet werden.
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** unwahrscheinlich 4 normal
Maßnahmen	Benachrichtigung des Administrators bei unsicherem Matching sowie manuelles Überprüfen von Record Linkage Ergebnissen
Bewertung	**Restrisiko**: Falsche manuelle Zuordnung **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

Risiko	**Fehlerhafte Verknüpfung von Daten aufgrund von fehlerhafter PSP-ID in der Projektdatenbank**
Gefährdung/ Risikoquelle	Keine Gefährdung für den Patienten. Auswirkungen nur auf Forschungsergebnisse / erhöhtes Risiko durch manuelle Eingaben
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** unbedeutend **Eintrittswahrscheinlichkeit:** möglich 4 normal
Maßnahmen	Bereitstellung von Schulungsmaterial; Unterweisung der Mitarbeiter des jeweiligen Projekts
Bewertung	**Restrisiko**: Falsche manuelle Zuordnung **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

4. Gewährleistungsziel: Vertraulichkeit

Risiko	**Zugriff durch Unbefugte**
Gefährdung/ Risikoquelle	*Zentrale Suche*: keine Gefährdung *Dezentrale Suche*: Identifizierung eines Patienten wird erleichtert, insbesondere bei Vorliegen einer seltenen Erkrankung *Projektspezifische Patienten-Pseudonymisierung*: Herausgabe von Daten an Unbefugte, mögliche Identifizierung eines Patienten Daten werden von Unbefugten eingesehen / verwendet. Daten werden gestohlen / kopiert / an Unbefugte übertragen und ggf. weiterverbreitet.
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** möglich 8 normal
Maßnahmen	Authentifizierung von Benutzern über einen zentralen Authentifizierungsdienst (siehe DSK 5.1) Festlegung eines Rechte- und Rollen-Konzeptes Regeln und Berechtigungen zur Freigabe der Daten (z.B. für Export aus Brückenkopf: intern bei Berechtigung im Behandlungskontext, extern nur nach Entscheid durch lokale Gremien; für Freigabe von Daten aus Forschungsdatenbanken: nur durch den jeweiligen Projektleiter) Verpflichtung auf Datengeheimnis Verschlüsselung von transferierten Daten Schutz vor äußeren Einflüssen Nachweise zur Gebäudesicherheit, möglicherweise durch Zertifizierung der DataCenter Prüfung der Maßnahmen durch TMF, positives Votum Lokale IT-Sicherheitskonzepte
Bewertung	**Restrisiko**: Umgehen oder technischer Fehler der aufgeführten Maßnahmen **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

Risiko	**Technische und Organisatorische Maßnahmen sind für die zentralen Komponenten nicht gemäß DSK umgesetzt / Wirksamkeit der Maßnahmen wird nicht überprüft.**
Gefährdung/ Risikoquelle	Definierte Maßnahmen entsprechen nicht mehr dem aktuellen Stand der Technik bzw. wurden nicht durchgeführt.
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** wesentlich **Eintrittswahrscheinlichkeit:** unwahrscheinlich 6 normal
Maßnahmen	ggf. Penetrationstest
Bewertung	**Restrisiko**: Sicherheitslücken trotz ergriffener und regelmäßig überprüfter Maßnahmen **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

5. Gewährleistungsziel: Transparenz

Risiko	**Fehlende vertragliche Regelungen zwischen den Kooperationspartnern, sowie unklare Rollendefinition und Rollenverständnis der Beteiligten**
Gefährdung/ Risikoquelle	Betroffener kann seine Rechte nicht durchsetzen
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** möglich 8 normal
Maßnahmen	Vertragliche Vereinbarung zur Teilnahme an der CCP-IT mit beteiligten Standorten Datenschutzkonzept der CCP-IT Regelungen für die Freischaltung von Usern für die spezifische Projekt-Pseudonymisierung
Bewertung	**Restrisiko**: Nichtbeachtung der vorliegenden Vertragsvereinbarungen **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

Risiko	**Fehlende oder unzureichende Einwilligungsdokumentation**
Gefährdung/ Risikoquelle	Daten des Betroffenen werden ohne dessen Einwilligung verarbeitet
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** möglich 8 normal
Maßnahmen	*Zentrale Suche*: Nur gekennzeichnete Datensätze werden in die zentrale Datenbank hochgeladen bzw. Upload aufgrund anderer Rechtsgrundlage nur mit zweifacher manueller Bestätigung durch den Administrator möglich; lokale Verantwortung für die Überprüfung der jeweiligen Rechtsgrundlage. *Dezentrale Suche*: Lokale Verantwortung für das Ausrollen einer Einwilligung, die einen Datenimport in den Brückenkopf zulässt, sowie die korrekte Dokumentation und Ausführung des Patientenwillens. *Projektspezifische Patienten-Pseudonymisierung*: Verantwortung beim Projektleiter zur Prüfung des Patientenwillens vor Herausgabe von Daten
Bewertung	**Restrisiko**: Verarbeitung der Daten trotz Maßnahmen **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

6. Gewährleistungsziel: Nicht-Verkettbarkeit

Risiko	**Nicht ausreichende Einschränkung der Verarbeitung**
Gefährdung/ Risikoquelle	Daten des Betroffenen werden ohne dessen Einwilligung aus mehreren Datenquellen zusammengeführt, was seine Identifizierung erleichtert.
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** möglich 8 normal
Maßnahmen	Verknüpfung von Daten nur bei Vorliegen konkreter Einwilligung Einsatz von unterschiedlichen Pseudonymen (lokale und globale Brückenkopf-Pseudonyme, Projekt-Pseudonyme, s. DSK 3.2 und 3.3)
Bewertung	**Restrisiko**: Zusammenführen der Daten trotz Maßnahmen **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

7. Gewährleistungsziel: Intervenierbarkeit

Risiko	**Der Betroffene kann seine Rechte auf Auskunft, Berichtigung etc. nicht wahrnehmen**
Gefährdung/ Risikoquelle	Falsche Daten werden nicht korrigiert, Auskunftsbegehren nicht erfüllt.
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** möglich 8 normal
Maßnahmen	Differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
Bewertung	**Restrisiko**: Nicht-Ausführen des Betroffenenwillens trotz Maßnahmen **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

Risiko	**Widerruf / Löschbegehren wird nicht umgesetzt**
Gefährdung/ Risikoquelle	Daten werden trotz Widerrufs / Löschbegehren eines Patienten nicht gelöscht (durch Fehler in der Prozesskette am Standort oder durch den Betreiber der zentralen Patientenliste).
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** unbedeutend **Eintrittswahrscheinlichkeit:** möglich 4 Normal
Maßnahmen	Definition eines Prozesses zum Umgang mit Widerruf oder Antrag auf Löschung der Daten (siehe DSK 6.5) auf zentraler und lokaler Ebene Rückmeldung zur lokalen Umsetzung des DSK wird von den teilnehmenden Standorten angefordert
Bewertung	**Restrisiko**: Definierter Prozess wird irrtümlicherweise nicht erfolgreich durchgeführt. **Restrisikomaßzahl**: 2 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

Für lokale DSFA

Risiko	**Import in den Brückenkopf: Daten werden nicht entsprechend ihres Einwilligungs-Status importiert**
Gefährdung/ Risikoquelle	Daten von Patienten werden nicht entsprechend ihres EW-Status (der Art der EW bzw. ob eine EW vorliegt) prozessiert und weitergegeben (in den Brückenkopf sowie an die zentrale Suche und an Forschungsprojekte); der Patientenwille wird nicht umgesetzt.
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** moderat **Eintrittswahrscheinlichkeit:** unwahrscheinlich 4 normal
Maßnahmen	Etablierung und Beschreibung eines transparenten, lokalen Prozesses zur Datenselektion und –weiterleitung im Rahmen der dezentralen Suche / des Exports aus dem Brückenkopf Regelmäßige Prüfung der relevanten Einwilligungen durch Anbindung eines Einwilligungs-Managements
Bewertung	**Restrisiko**: Verarbeitung der Daten trotz Maßnahmen **Restrisikomaßzahl**: 2 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

Risiko	**Technische und Organisatorische Maßnahmen sind für die lokalen Komponenten nicht gemäß DSK umgesetzt / Wirksamkeit der Maßnahmen wird nicht überprüft.**
Gefährdung/ Risikoquelle	Nicht autorisierte Nutzer können bei Übertragung oder Speicherung auf Daten zugreifen Nicht verschlüsselte Speichermedien Unsichere Verwahrung der Schlüssel
Analyse **Risikomaßzahl** **Schutzbedarf**	**Schadensauswirkung:** wesentlich **Eintrittswahrscheinlichkeit:** unwahrscheinlich 6 normal
Maßnahmen	Sichere Ablage der Daten (Verschlüsselung SQL Server) Beschreibung der Schnittstellen Protokollierung des Datenzugriffs Vier-Augen-Prinzip Sichere Maschine-zu-Maschine-Kommunikation Bestimmung zugriffsberechtigter Personen durch Rechte- und Rollenkonzept (nur Vergabe minimaler / notwendiger Berechtigungen) Protokollierung der Zugriffe Durchführung von Schulungsmaßnahmen Erstellung eines Notfallplans Etablierung und Beschreibung eines transparenten, lokalen Prozesses zur Datenselektion und –weiterleitung im Rahmen der dezentralen Suche / des Exports aus dem Brückenkopf
Bewertung	**Restrisiko**: Sicherheitslücken trotz ergriffener und regelmäßig überprüfter Maßnahmen **Restrisikomaßzahl**: 4 **Tragbarkeit**: kein oder geringes Risiko
Bemerkungen	

7. Aktuelle DKTK-Kooperationspartner

Anlage: DKTK-Kooperationspartner

Stand: 6.02.2019

Folgende Einrichtungen sind im Rahmen der C4-Förderung durch die Deutsche Krebshilfe als DKTK-Kooperationspartner der CCP-IT Plattform angeschlossen:

- Erlangen: Comprehensive Cancer Center (CCC)
- Hamburg: Universitätsklinikum Hamburg-Eppendorf,
  Universitäres Cancer Center Hamburg (UCCH)
- Köln/Bonn: Uniklinik Köln, Centrum für Integrierte Onkologie (CIO)
- Würzburg: Universität Würzburg,
  Comprehensive Cancer Center (CCC) Mainfranken
- Ulm: Universitätsklinikum Ulm, Comprehensive Cancer Center Ulm (CCCU)

8. Danksagung

Dieses Datenschutzkonzept beruht auf dem generischen Datenschutzleitfaden des TMF e.V. und stellt eine Aktualisierung der Version vom 8. Januar 2014 dar, die unter maßgeblicher Mitwirkung von Andreas Borg (Universitätsmedizin Mainz) erstellt wurde. Wir bedanken uns außerdem bei der TMF-Arbeitsgruppe Datenschutz (Berichterstatter: Prof. Dr. Klaus Pommerening, Johannes Gutenberg-Universität Mainz) für die kritische und unabhängige Prüfung des Konzepts.