5 Module des Datenschutzkonzepts

Das generische Datenschutzkonzept für medizinische Forschungsverbünde ist modular aufgebaut. Die Module unterscheiden sich durch unterschiedliche Rahmenbedingungen und Vorgehensweisen und passen somit zu unterschiedlichen wissenschaftlichen Fragestellungen. Da ein Forschungsverbund oft viele verschiedenartige Forschungsprojekte vereinigt, dienen die Module und die zentralen Infrastruktur-Komponenten als Bausteine, aus denen das Datenschutzkonzept des Verbundes zusammengesetzt werden kann.

Ein medizinischer Forschungsverbund besteht aus bis zu vier Modulen:

- **Klinisches Modul** – dieses dient der Gewinnung von Forschungsdaten aus dem direkten Behandlungszusammenhang; ferner können hier auch einfache oder informelle Forschungsprojekte wie Beobachtungsstudien oder Benchmarkingprojekte durchgeführt werden. Der wissenschaftliche Austausch von behandelnden Ärzten mit führenden Experten im direkten Interesse des Patienten wird gefördert. Der Online-Zugriff auf die Daten während der Behandlung ist notwendig.
- **Studienmodul** – hier werden klinische Studien durchgeführt, die auch den besonderen Regularien des Arzneimittelgesetzes (AMG) oder Medizinproduktegesetzes (MPG) unterliegen können.
- **Forschungsmodul** – in diesem werden besonders qualitätsgesicherte Daten für langfristige Forschungsprojekte zusammengeführt und vorgehalten, die für die Behandlung des einzelnen Patienten keine direkte Rele-

vanz haben und daher aus dem Behandlungskontext nicht zugänglich sein müssen; Beispiele hierfür sind epidemiologische Register.

- **Biobankenmodul** – dieses dient der Sammlung und Verwaltung von Biomaterialien (Proben und daraus gewonnene Materialien) für Forschungszwecke, insbesondere für die Erforschung molekulargenetischer Aspekte einer Erkrankung wie Fragestellungen der genetischen Epidemiologie.

Die Module unterscheiden sich in ihrer Zweckbestimmung und ihrer Datenprozessierung und unterliegen unterschiedlichen rechtlichen Rahmenbedingungen. Jedes dieser Module enthält eine spezifische zentrale Datenbank, in manchen Fällen auch mehrere gleichartige. Die Module werden durch zentrale Infrastruktur-Komponenten zum Identitätsmanagement für Patienten sowie zum Rechtemanagement für Teilnehmer des Forschungsverbundes ergänzt.

In diesem Kapitel werden die Module einzeln beschrieben, ihre unterschiedlichen Rahmenbedingungen und Verfahren spezifiziert und Anleitungen für das Datenschutzkonzept von „einfachen" Forschungsverbünden gegeben, die im Wesentlichen nur aus einem Modul bestehen (s.a. Abb. 6).

Kombinationsvarianten der unterschiedlichen Module wie auch zentrale Aspekte des Identitäts- und Rechtemanagements in einem Forschungsverbund sind dann Gegenstand des folgenden Kapitels 6.

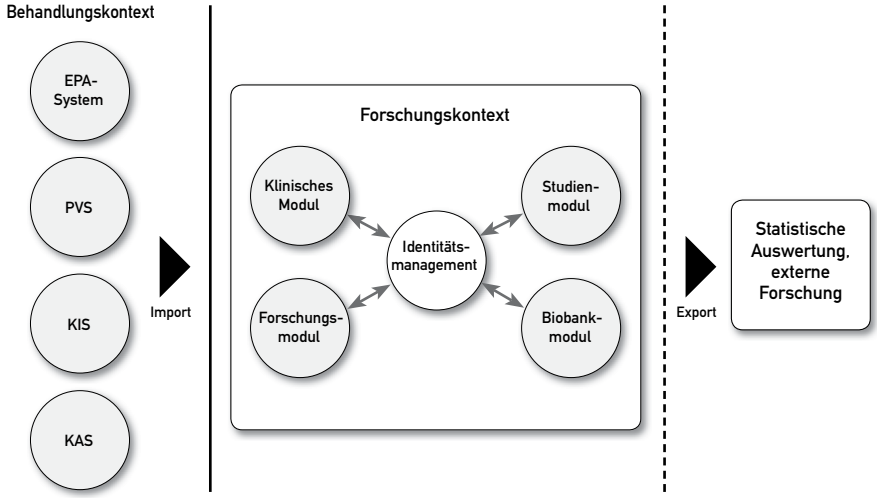

Abb. 6 Module eines medizinischen Forschungsverbunds; neben dem Identitätsmanagement sind auch andere zentrale Dienste nötig, etwa Rechtemanagement oder Datenqualitätsmanagement.

5.1 Klinisches Modul

Das klinische Modul stellt die Adaption des Modells A des bisherigen generischen TMF-Datenschutzkonzepts dar; die Einordnung in die neue Struktur ist in Kapitel 6.1.7 beschrieben.

Die Bezeichnung als „Klinisches Modul" folgt der Bezeichnung „klinisch-(wissenschaftliches) Forschungsnetz" aus dem bisherigen Datenschutzkonzept. Sie soll darauf hindeuten, dass in diesem Modul klinische Forschung betrieben wird, also im Wesentlichen Forschung direkt am Patienten in engem Versorgungsbezug[19]. Die spezialgesetzlich geregelten klinischen Studien werden wegen ihrer besonderen gesetzlichen und methodischen Rahmenbedingungen nicht hier, sondern in das Studienmodul eingeordnet, siehe Kapitel 5.2.

5.1.1 Zweck und Anwendungsbereich

Das Ziel des Klinischen Moduls ist die Ableitung und Bereitstellung von Forschungsdaten aus dem normalen Behandlungsgeschehen, in erster Linie ohne zusätzliche erhebliche Intervention zu Forschungszwecken. Dieses Ziel wird beispielsweise im Rahmen von Beobachtungsstudien, der Dokumentation von Heilversuchen oder bei gesundheitsökonomischen Studien realisiert und erfordert dazu eine klinisch fokussierte Vernetzung. Die Einsetzbarkeit des Klinischen Moduls ergibt sich insbesondere bei der Erforschung von Erkrankungen, die so selten sind oder deren Behandlung so komplex ist, dass sie die Leistungsfähigkeit von einzelnen Regelversorgungszentren überfordert. In diesen Fällen ist die enge Kooperation und Kommunikation spezialisierter Zentren unverzichtbare Voraussetzung sowohl für die effektive Behandlung als auch für aussagekräftige Forschungsergebnisse.

Patienten mit chronischen, seltenen oder besonders schweren Erkrankungen werden oft sowohl von ihren Hausärzten als auch zusammen mit breit gefächerten spezialisierten klinischen Zentren, wie z.B. Spezialkliniken, spezialisierten niedergelassenen Ärzten, sogenannten Referenzlaboren oder Referenzpathologien, betreut. Durch das Hinzuziehen spezialisierter und im jeweiligen Fachgebiet besonders erfahrener Behandlungsteams soll eine höhere Diagnostik- und Therapiequalität erreicht werden, als dies alleine im Bereich der Regelversorgung möglich ist. Solche Kooperationsstrukturen auf- oder auszubauen, ist Aufgabe z.B. der Kompetenznetze in der Medizin oder der Netze für seltene Erkrankungen.

19 Die ebenfalls diskutierte Bezeichnung als „Versorgungsmodul" wurde – obwohl in einigen Forschungsverbünden im Gebrauch – verworfen, da die Verwechslungsgefahr mit den Strukturen der direkten Krankenversorgung zu groß ist.

Wegen der fundierten Erfahrung und des hier gebündelten Sachverstandes tragen die spezialisierten Zentren besondere Verantwortung sowohl für die Versorgung nach aktuellem Stand des Wissens als auch in der Weiterentwicklung und Evaluation von diagnostischen und therapeutischen Verfahren. Im Bereich der Versorgung fallen ihnen oft Aufgaben in der Beratung von Patienten (Zweitmeinung) wie auch von Ärzten zu, die an der Regelversorgung beteiligt sind. So soll ein vom Zentrum initiierter Behandlungspfad oder Therapieplan im klinischen Alltag zumindest teilweise auch von nicht spezialisierten Behandlungsteams heimatnah und kostengünstig durchgeführt werden können. Bei Änderungen im Krankheitsverlauf oder zu vorher festgelegten Zeitpunkten erfolgt die Wiedervorstellung der Patienten im spezialisierten Zentrum.

Auch die spezialisierten klinischen Zentren greifen bei ihrer Arbeit wiederum auf weitere Spezialisten zurück. So werden beispielsweise besondere Laboruntersuchungen oft nicht in allen Zentren durchgeführt, selbst wenn hier auf Grund der Behandlung bestimmter Patientenkollektive die Ergebnisse dieser Methoden benötigt werden. Die Durchführung hochspezieller Analysen erfolgt ebenso oft in einem wiederum hierfür spezialisierten Zentrum, das die Anforderungen mehrerer klinischer Zentren bündelt und bearbeitet. Die Behandlung der oben genannten komplexen Krankheitsprobleme wird so auf viele Expertenschultern verteilt, um den für den Patienten höchsten Effizienzgrad mit dem Ziel des optimalen Behandlungserfolges zu erreichen. Diese intensive Art der Behandlung übersteigt die Leistungen der „Regelversorgung“ und wird – wenn überhaupt – aus den Mitteln des Forschungsverbundes finanziert. Insbesondere ist sie in Abgrenzung zur reinen Behandlungsdokumentation oder gewöhnlichen Patientenakte mit einem deutlich erhöhten Dokumentationsaufwand verbunden. Ob dieser erhöhte Dokumentations- und Kommunikationsaufwand tatsächlich mit einem verbesserten Behandlungserfolg einhergeht, ist im Idealfall Gegenstand einer systematischen Versorgungsforschung.

Für diese und weitere ähnliche Szenarien stellt das Klinische Modul einen Mechanismus bereit, der die Erhebung und Verarbeitung von klinischen Forschungsdaten weitgehend in den Behandlungsprozess integriert. Wesentliche Merkmale dieser Integration sind:

- Erstbehandler stellen den Kontakt zwischen dem Patienten und dem Forschungsverbund her. Dazu gehören Aufklärung und Einholung der Einwilligungserklärung hinsichtlich der Teilnahme des Patienten an dem Forschungsverbund, sowie die Erfassung des Patienten im Klinischen Modul.
- Erstbehandler und weitere Behandler haben Onlinezugriff auf identifizierende Daten (IDAT) und medizinische Daten (MDAT), solange ein Behandlungsverhältnis zum jeweiligen Patienten besteht.
- Alle Behandler dokumentieren ihre jeweiligen Erkenntnisse in einem gemeinsamen medizinischen Datenbestand (MDAT), der in einer zentralen Klinischen Datenbank gespeichert wird.

- Alle Behandler können im Umgang mit der Online-Datenerfassung des Klinischen Moduls die im jeweiligen Behandlungszusammenhang üblichen identifizierenden Patientendaten (Name, Vorname, Versichertennummer, usw.) nutzen.

Der Kern des Klinischen Moduls besteht aus einer Klinischen Datenbank (KDB), die ausschließlich medizinische Daten (MDAT), jedoch keine Identitätsdaten (IDAT) enthält; je nach organisatorischen Anforderungen (z.B. Trennung nach Krankheits-Subentitäten) kann das Klinische Modul auch mehrere Klinische Datenbanken beherbergen. Die Identitätsdaten werden in einer getrennten Patientenliste (PL) gehalten. Beide Datenbestände sind über einen gemeinsamen Schlüssel PID_K verknüpft, der ausschließlich zwischen diesen beiden Systemen kommuniziert wird, ansonsten jedoch geheim bleibt. Die beiden Komponenten Klinische Datenbank und Patientenliste müssen räumlich getrennt angeordnet sein und dürfen nicht derselben Daten verarbeitenden Stelle unterstehen. In einer Klinischen Datenbank wird also das Prinzip einer pseudonymen Speicherung bei gleichzeitig personenbezogenem Zugriff im Behandlungszusammenhang umgesetzt.

Innerhalb des Behandlungsgeschehens haben Berechtigte Zugriff auf die Klinische Datenbank und die Patientenliste und können – wie in den meisten Behandlungsszenarien üblich – mit dem Patienten namentlich kommunizieren. Im Forschungsumfeld besteht kein Zugriff auf die Patientenliste, so dass hier nur pseudonymisierte medizinische Daten zur Verfügung stehen. Ein Rückgriff auf die Identitäten ist nur unter Mitwirkung des Betreibers der Patientenliste möglich, so dass diesem treuhänderische Aufgaben zufallen.

Im Gegensatz zu einem Studienmodul (s. Kap. 5.2) steht im Klinischen Modul die Behandlung der Patienten im Vordergrund, wird aber z.B. im Sinne einer Beobachtungsstudie wissenschaftlich begleitet und ausgewertet. Das Forschungsziel ist im Gegensatz zum Studienmodul nicht von vornherein durch Hypothesen eng umrissen, entsprechend kann die nötige Aufbewahrungsdauer der Daten unbestimmt sein. Diese Offenheit bringt erhöhte Anforderungen an Patientenaufklärung und -einwilligung mit sich und erfordert ein im Vergleich zum Studienmodul strengeres Pseudonymisierungsverfahren – das verwendete Pseudonym ist im Gegensatz zum SIC des Studienmoduls (s. Kap. 5.2) dem behandelnden Arzt nicht bekannt.

Auch versorgungsnahe Register, z.B. klinische Krebsregister oder klinische Datawarehouses, können bei entsprechender Konstruktion durch ein Klinisches Modul modelliert werden. Das gleiche gilt für wissenschaftsgetriebene Studien (IIT), soweit sie nicht unter die Regularien von AMG und MPG fallen.

Typisch für Verbünde, die nur ein Klinisches Modul haben, ist die auf einen langen Zeitraum ausgerichtete Datensammlung, die besondere datenschutzrechtliche Überlegungen und Maßnahmen erfordert. Wichtig ist hier, dass der Verbund oder die zentrale Datenbank selbst „die Studie“ ist, auf die sich

die Einwilligung bezieht, sodass nicht für jedes Teilprojekt, das die Daten verwendet, neue Einwilligungen eingeholt werden müssen. Natürlich bewirkt eine umfassende, sogar über eine elektronische Patientenakte hinausgehende Dokumentation mit erweiterter Datenerfassung für aktuelle oder künftige Forschungsfragen einen erhöhten Schutzanspruch, der zwingend zusätzliche Schutzmaßnahmen nach sich zieht. In einem größeren Netz werden die Daten des Klinischen Moduls (im nötigen Umfang) für Forschungszwecke in der Regel in andere Module übertragen. Die Konstruktion des Klinischen Moduls erlaubt aber auch, insbesondere für kleinere Netze, Forschungsfragen direkt mit den Daten des Klinischen Moduls anzugehen. Dafür ist ein anonymisierter oder, falls dieser nicht zielführend ist, ein pseudonymisierter Export vorgesehen. Für einfache Auswertungen, auch ökonomischer Fragestellungen, reicht dabei in der Regel ein anonymisierter Export.

Das Klinische Modul kann durch eine Bilddatenbank oder eine Biobank ergänzt werden. Hierbei sind zwei Varianten denkbar, die sich durch den Anknüpfungspunkt der zusätzlichen Datenbanken unterscheiden:

- Die Bilddatenbank bzw. Biobank kann über ein eigenes Pseudonym mit der Patientenliste verknüpft werden. Die Zusammenführung – auch zu Forschungszwecken – erfordert dann immer einen Rückgriff auf die Patientenliste, auch wenn die IDAT hierfür nicht benötigt werden. Dafür wird das Reidentifizierungsrisiko der Klinischen Datenbank nicht erhöht.
- Alternativ können Bilddatenbank und Biobank ohne direkte Anbindung an die Patientenliste geführt und dafür über geeignete Schlüssel mit der Klinischen Datenbank verbunden werden. Dadurch wird der Datensatz der Klinischen Datenbank effektiv verbreitert.

Eine genauere Beschreibung dieser Anbindung ist im Kapitel 6.5 zum Maximalmodell bzw. Kapitel 5.4 zum Biobankenmodul und dem ausführlicheren generischen Datenschutzkonzept für Biomaterialbanken [2] zu finden.

In einer Klinischen Datenbank können auch Daten von Sensoren am Patienten und unterstützenden technischen Geräten („AAL-Daten“) gespeichert werden; solche Daten sind den medizinischen Daten zuzuordnen. Die datenschutzgerechte Gewinnung und Übermittlung solcher Daten sowie ihre Qualitätssicherung bedürfen gesonderter Überlegungen, die nicht Gegenstand dieses generischen Datenschutzkonzepts für medizinische Forschungsverbünde sein können. Werden in diesem Kontext Daten vom Patienten selbst eingegeben, so entspricht dies der in Kapitel 5.2.4 beschriebenen Situation.

5.1.2 Anwendungsfälle

5.1.2.1 Patienten in das Klinische Modul aufnehmen

Als Erstkontakt aus Sicht des Forschungsverbunds ist derjenige Kontakt mit dem Erstbehandler zu werten, der – nach entsprechender Aufklärung und Ein-

holung der Einwilligung (vgl. Kap. 3.2.3.1) – zu einer Aufnahme des Patienten in den Forschungsverbund führt. Hier wird im Wesentlichen ein Eintrag in der Patientenliste erzeugt und ein Basisdatensatz in der Klinischen Datenbank hinterlegt. Ist der Patient bereits mit gleichen oder ähnlichen Angaben in der Patientenliste eingetragen, so ordnet das System den Patienten nach Möglichkeit richtig zu und weist, wenn das nicht zweifelsfrei möglich ist, auf die mögliche Verwechslungsgefahr hin. Es ist darauf zu achten, dass dabei nicht die Identität eines anderen Patienten enthüllt wird.

5.1.2.2 Rechte an Mit- und Weiterbehandler vergeben

Die Autorisierung von Mitbehandlern hinsichtlich des lesenden Zugriffs auf die zentral gespeicherten Daten erfolgt grundsätzlich durch einen Vorbehandler in Absprache mit dem Patienten oder durch den Patienten selbst; die Umsetzung wird, soweit sie nicht automatisiert ablaufen kann, durch einen zuständigen Systemadministrator (Datenmanager, evtl. Rechtemanager) vorgenommen. So wird z.B. ein Hausarzt bei der Überweisung an eine Spezialklinik vorab die Überweisung selbst und die Erteilung der Zugriffsberechtigung mit dem Patienten besprechen und dann online erteilen, oder, je nach Organisation des Forschungsverbunds, dem Rechtemanagement einen entsprechenden Auftrag erteilen. Die Autorisierung kann explizit einem aktuellen Mit- oder Weiterbehandler erteilt werden. Optional kann sie auch für zukünftige Behandler erteilt werden. Diese Autorisierungen werden in der Patientenliste oder in einem separaten Rechtemanagement geeignet hinterlegt.

5.1.2.3 Daten im Behandlungsprozess erheben

Grundsätzlich kann jeder Behandler nur auf die von ihm bzw. von seiner Dienststelle selbst eingegebenen Daten lesend und schreibend (nachträgliche Änderungen werden protokolliert) zugreifen. Durch eine entsprechende Autorisierung (s. o.) kann einem Mit- oder Nachbehandler Einsicht in die Daten gewährt werden.

5.1.2.4 Behandlungsqualität sichern

Zugriffe zum Zweck der Qualitätssicherung können sich entweder an einzelnen, sachlich zusammenhängenden Angaben im gesamten Bestand oder an breit gefächerten Angaben zum einzelnen Patienten orientieren. Letzteres kann nur durch (Mit-)Behandler erfolgen. Der ausschließlich lesende Zugriff auf begrenzte MDAT kann einzelnen Qualitätsbeauftragten (s. Kap. 5.1.4.6) erteilt werden. Hier ist jedoch der Zugang zu den Identitätsdaten der Patientenliste verwehrt. Außerdem ist darauf zu achten, dass nicht durch die Häufung von Funktionen in der Qualitätssicherung in einer Hand eine Reidentifizierung möglich wird.

5.1.2.5 Expertenforum organisieren

In einigen medizinischen Forschungsverbünden ist die Einrichtung von Expertenforen sinnvoll, in denen ausgewählte Experten medizinische Aspekte von Erkrankungsfällen diskutieren. Dieses Szenario ist vor allem bei seltenen Erkrankungen von Bedeutung, aber auch in anderen Verbünden, wenn es um schwierige Diagnosen und Therapieempfehlungen geht. Die Experten können gezielt angefragt werden oder von sich aus Kommentare zu einem Fall abgeben. Dabei handelt es sich auch haftungsrechtlich nicht um ein Konsil, das auf einem Auftragsverhältnis im Behandlungszusammenhang beruht und in der Regel personenbezogen durchgeführt wird. Im Expertenforum werden Daten nur pseudonymisiert bereitgestellt.

a) Fragestellungen für ein Expertenforum: Aufgabe ist die fallbezogene Diskussion zu einer Erkrankung. Konkrete Fragen zu Diagnose oder Therapie können gestellt werden; es sollen aber auch spontane Beiträge möglich sein, die Hypothesen oder Ideen formulieren. Ergebnisse kommen dem behandelten Patienten direkt zugute.

b) Teilnehmerkreis: Teilnehmer des Forums sind namentlich benannte Experten, die persönlich zum Forum zugelassen werden. Diese können auch im Ausland ansässig sein. Die Liste der Experten sollte dem betroffenen Patienten, idealerweise sogar öffentlich bekannt sein. Empfohlen wird, eine solche Liste kontinuierlich aktualisiert im Web bereit zu stellen. Die Einbindung eines Expertenforums muss durch die Einwilligungserklärung der Patienten abgedeckt sein. Dort ist ggf. auch auf die Möglichkeit der Einbindung ausländischer Experten explizit hinzuweisen.

c) Datenspeicherung und Datenzugang: Die Daten werden in der Klinischen Datenbank gespeichert. Der Online-Zugang für die Experten ist für die Dauer der Diskussion befristet, etwa 2 bis 4 Wochen; danach wird der Zugang zum jeweiligen Fall wieder gesperrt.

d) Personenbezug: Der Bezug auf die Identitätsdaten ist in diesem Szenario nicht notwendig; andererseits ist eine Verständigung nötig, auf welchen Fall sich die Diskussion bezieht. Daher ist die Einführung eines Pseudonyms speziell für diesen Zweck nötig. Der jeweils im persönlichen Behandlungszusammenhang stehende Arzt, ggf. auch Konsiliar, muss das Pseudonym dem konkreten Patienten zuordnen können. Nach Ablauf der Diskussionsfrist wird der Zugang zu den Falldaten und zum Pseudonym außer für behandelnde Ärzte gesperrt. Das Pseudonym muss allerdings in der Datenbank verbleiben, um auch später eingehende Beiträge zu diesem Fall noch zuordnen zu können und auch, um die Dokumentation der vorher eingegangenen Beiträge nachvollziehbar zu halten.

5.1.2.6 Datenqualität sichern

Für die Datenqualitätssicherung sind unter Umständen umfangreiche Datenzugriffe notwendig (s. dazu Kap. 6.8). Auch Monitoring-Prozesse können im Klinischen Modul vorgesehen sein.

5.1.2.7 Auskunft geben

Die Patienten haben ein Recht auf Auskunft über die von ihnen gespeicherten personenbezogenen Daten. Zudem sind diese auf Verlangen der Patienten auch zu korrigieren (vgl. Kap. 4.4.1). Der Patient wendet sich hierzu an den aktuell behandelnden Arzt, der Zugriff auf den vollständigen Datensatz des Patienten hat und diesem entsprechend Auskunft geben kann. Vom Patienten gewünschte Änderungen sind, sofern medizinisch unproblematisch, vom behandelnden Arzt vorzunehmen. Sollten Änderungen gewünscht werden, die einer medizinisch korrekten Dokumentation widersprechen, muss dies ggf. als Rückzug der Einwilligung gewertet werden, so dass der betreffende Datensatz zu löschen oder zu anonymisieren ist. Der behandelnde Arzt muss verhindern, dass durch Korrekturen oder Löschungen ein aus medizinischer Sicht unzutreffendes Bild des Patienten und der Behandlung gezeichnet wird.

5.1.2.8 Daten sperren, anonymisieren oder löschen

Die Löschung oder Sperrung kann vom Patienten über jeden teilnehmenden Behandler oder über die Netzwerkzentrale beantragt werden. Sie führt ggf. zur Entfernung des Eintrags aus der Patientenliste sowie zur Sperrung aller klinischen Daten (MDAT). Optional kann der Patient einer Anonymisierung zustimmen. Die Durchführung obliegt in jedem Fall dem Betreiber der jeweiligen Datenbank.

Generell sollte bereits mit der Aufnahme eine Vereinbarung über den Verbleib der gesammelten Daten im Todesfall getroffen werden. Im Klinischen Modul ist im Todesfall mindestens die Löschung oder Sperrung der IDAT in der Patientenliste erforderlich.

5.1.2.9 Machbarkeit einer Auswertung oder Studie prüfen

Die Fallsuche dient im Wesentlichen der Feststellung, ob eine gegebene Fragestellung mit dem aktuellen Bestand mit Aussicht auf Erfolg bearbeitet werden kann. Sie kann von entsprechend autorisierten Wissenschaftlern online vorgenommen werden. Bei der Fallsuche werden nur aggregierte Daten (Fallzahlen, Mittelwerte, etc.) bereitgestellt und für die Ausgabe der Ergebnisse von Datenbankabfragen Mindestanzahlen von Datensätzen festgelegt; dadurch soll verhindert werden, dass durch geschickt formulierte Abfragen einzelne Datensätze identifiziert werden können. Der Zugriff auf Identitätsdaten

bleibt verwehrt, ebenso der Zugriff auf einzelne MDAT-Sätze. Dieses Verfahren ist auch im Forschungsmodul enthalten, siehe Kapitel 5.3.2.4, und kann ggf. auch zur Schätzung von Inzidenzen verwendet werden.

5.1.2.10 Rekrutierung unterstützen

Um Patienten für klinische Studien zu rekrutieren, ist letztlich ein Rückgriff auf MDAT und IDAT notwendig. Das Klinische Modul kann ein besonders effizientes Verfahren bereitstellen. Dabei werden gezielt die behandelnden Ärzte informiert, deren gemeldete Patienten für eine spezifizierte Studie geeignet sind. Diese sind letztlich für die eigentliche Rekrutierung verantwortlich. Alternativ können für eine Rekrutierung durch Dritte mittels konsekutiven Zugriffs auf Klinische Datenbank und Patientenliste geeignete Listen erstellt und daraufhin die Patienten kontaktiert werden, sofern eine entsprechende Einwilligung vorliegt.

5.1.2.11 Daten an Forscher weitergeben

Der Export medizinischer Daten zu Forschungszwecken erfolgt nach wissenschaftlicher, ethischer und datenschutzbezogener Begutachtung durch entsprechende Gremien. Verantwortlich für den eigentlichen Export (nach Auftrag durch die entsprechenden Gremien) ist der Betreiber der Klinischen Datenbank. Der Export erfolgt wenn möglich anonymisiert, sonst pseudonymisiert. Ein Onlinezugriff ist nicht vorgesehen.

5.1.2.12 Ergebnisse mitteilen

Im Rahmen wissenschaftlicher Auswertungen pseudonym exportierter Daten des Klinischen Moduls können Ergebnisse entstehen, die für die weitere Behandlung einzelner Patienten relevant oder zumindest von Interesse sein können. In so einem Falle wird zunächst geprüft, ob die Rückmeldung solcher Ergebnisse mit dem Patienten vereinbart wurde, oder ob eine dringende medizinische Notwendigkeit besteht, die Ergebnisse mitzuteilen. Wenn eine Mitteilung erforderlich oder gewünscht ist, wird im Regelfall der aktuell behandelnde Arzt informiert und über das Ergebnis der Auswertung in Kenntnis gesetzt. Dieser informiert dann den Patienten über das Ergebnis und berät ihn hinsichtlich möglicher Konsequenzen. In Ausnahmefällen und falls in dieser Form mit dem Patienten vereinbart, kann auch eine Kontaktierung direkt durch den Forschungsverbund stattfinden.

5.1.3 Daten und Datenflüsse

Der Datenbestand des Klinischen Moduls entsteht durch die kontinuierliche interaktive Nutzung des Moduls im Behandlungszusammenhang. Darüber

hinaus sind Übermittlungen größerer Datensätze in oder aus der Klinischen Datenbank im Rahmen des Klinischen Moduls kaum erforderlich.

Der Zugriff auf MDAT identifiziert durch IDAT während der Erst-, Weiter- oder Mitbehandlung erfolgt in drei Schritten. Nach Prüfen der Berechtigung und nach Auffinden des Patienten in der Patientenliste wird ein weiteres, nur für diesen konkreten Vorgang verwendetes temporäres Pseudonym – hier Zugriffsticket (TKT) genannt, im Modell A des bisherigen generischen Datenschutzkonzepts als TempID bezeichnet – erzeugt und an den Berechtigten sowie an die Klinische Datenbank übermittelt. Der Berechtigte erhält mit dem TKT Zugriff auf die entsprechenden MDAT. Dabei ist die Gültigkeitsdauer des TKT auf den Zeitbedarf einer typischen Arbeitssitzung beschränkt. Der technische Ablauf wird in der Abbildung 14 im Kapitel 6.1 zum Identitätsmanagement beschrieben.

Die Erzeugung eines TKT kann unterbleiben, wenn für einen bestimmten Vorgang nur der Zugriff auf eine der beiden Komponenten erforderlich ist. Beispiele hierfür sind ein Update der IDAT, z.B. nach Namensänderung, oder ein Export von Forschungsdaten.

Das im Klinischen Modul verwendete Pseudonym PID_K wird zu keinem Zeitpunkt an einem weiteren Ort außer der Patientenliste und den Klinischen Datenbanken, in denen der Patient geführt wird, gespeichert.

Datenflüsse zwischen dem Klinischen Modul und evtl. vorhandenen weiteren Modulen des Forschungsverbundes werden in Kapitel 6 beschrieben, insbesondere in den Kapiteln 6.3 und 6.5. Der direkte Datenexport aus der Klinischen Datenbank zu Forschungszwecken ähnelt dem aus der Forschungsdatenbank, sofern dort kein Online-Zugriff vorgesehen ist, siehe Kapitel 5.3.2.9.

Externe Forscher können, da für den Export stets neue (Einmal-)Pseudonyme verwendet werden, selbst kein Follow-up durchführen, sondern benötigen im Bedarfsfall immer einen Export der gesamten Historie. Dadurch wird insbesondere der Aufbau einer externen Schatten-Datenbank verhindert.

5.1.4 Nutzer, Rollen und Rechte

Das Klinische Modul betrachtet überwiegend die Rollen des behandelnden Arztes (in der Regel mehrere Ärzte für jeden einzelnen Patienten) und des Wissenschaftlers, dazu verschiedene Systemadministratoren.

5.1.4.1 Behandelnder Arzt

Die im Behandlungsprozess tätigen Ärzte erwarten von einer klinisch fokussierten Vernetzung eine Optimierung ihrer Prozessstrukturen, um so Diagnostik und Therapie für ihre Patienten verbessern zu können. Da die suffiziente Zuarbeit der Kliniker zur Forschung auch bei maximaler technischer Hilfe-

stellung, nicht zuletzt durch den zusätzlichen Aufwand bei der Patientenführung und -aufklärung, immer Mehrarbeit erfordert, erwarten die klinisch tätigen Ärzte von der klinisch-wissenschaftlichen Vernetzung des Klinischen Moduls darüber hinaus eine Verminderung redundanter Arbeitsvorgänge. Daraus ergeben sich die nachfolgenden Anforderungen:

- Der Zugriff auf krankheitsbezogene Informationen der Patienten muss verwechslungsfrei und fehlerlos möglich sein. Die Erfassung jeglicher patientenbezogener Daten muss der Fortschreibung einer Krankengeschichte dienen und bei einer Wiedervorstellung des Patienten verfügbar sein, auch – mit Einwilligung des Patienten – bei einem Wechsel des Behandlers.
- Die im Forschungsdatensatz definierten Informationen aus allen im Forschungsnetz teilnehmenden diagnostischen und therapeutischen Bereichen (z.B. Arztpraxis, Klinik, Labor), die im Behandlungsprozess erforderlich sind, sollen patientenbezogen zeitnah und lückenlos zusammengeführt werden können, um so den Informationsstand zwischen den am Behandlungsprozess Beteiligten zu optimieren.
- Die Doppelerfassung klinischer Daten zur wissenschaftlichen Dokumentation muss, soweit möglich, vermieden werden, die Ableitung der wissenschaftlich relevanten Daten aus den klinischen Daten ist aus Gründen der Arbeitserleichterung und der Qualitätssicherung anzustreben.
- Die Suche nach eigenen Patienten anhand beliebiger Suchkriterien sowie einfache Auswertungen über eigene Patienten sollten möglich sein.

Führen wissenschaftliche Untersuchungen zu Ergebnissen, die für den individuellen Patienten relevant sind, so muss der behandelnde Arzt in die Lage versetzt werden können, mit diesem Patienten Kontakt aufzunehmen, um den Behandlungsprozess an die neue Situation anzupassen.

5.1.4.2 Laborarzt

Auch Laborärzte können als behandelnde Ärzte registriert werden, sofern diese einen Untersuchungsauftrag erhalten, der ein für die Behandlung des Patienten relevantes Ergebnis ergibt. Laborärzte erhalten einen eingeschränkten Zugang zu den klinischen Daten des Patienten in Abhängigkeit von der durch sie zu erbringenden Untersuchung. Sie können ihr Ergebnis – sofern dieses im Datensatz des Forschungsnetzes vorgesehen ist – online in den klinischen Datenbestand eingeben. Laborärzte werden von den behandelnden Ärzten direkt beauftragt und erhalten dadurch Zugang zur Klinischen Datenbank.

5.1.4.3 Wissenschaftler

„Wissenschaftler“ oder „Forscher“ kommen in einem Forschungsverbund in verschiedenen Varianten vor und müssen in ihrer Rolle dementsprechend differenziert werden:

- der Leiter des Forschungsverbunds oder eines zentralen Teilprojekts (Studienleiter) und seine Mitarbeiter, die mit den anfallenden Daten neue Erkenntnisse gewinnen wollen,
- teilnehmende Ärzte mit eigenen Forschungsinteressen,
- das „biostatistische Personal" des Forschungsverbunds, das die Auswertungen direkt vornimmt,
- externe Forscher, die Daten (evtl. auch Proben) zur Erforschung eigener Fragestellungen übermittelt bekommen, z.B. Epidemiologen oder Vertreter der Industrie; dieser Gruppe ist auch ein medizinischer Qualitätsbeauftragter, siehe Kapitel 5.1.4.6, zuzuordnen,
- Experten als Teilnehmer an einem Expertenforum, die durch die Diskussion seltener Fälle Ideen und Hypothesen für neue Forschungsansätze gewinnen können.

Die beteiligten leitenden Wissenschaftler erwarten durch die Teilnahme am Forschungsnetz nicht nur, mehr Patienten in ihre Forschung einzubringen, sondern auch den klinischen Bezug ihrer Forschung besser herstellen zu können. Gerade bei chronischen und besonders schweren oder seltenen Erkrankungen sind Rückgriffe auf fallbezogene frühere Informationen und frühere biologische Proben oftmals von besonders großem Interesse, wenn Prognose und Therapieeffekte betrachtet werden sollen. Die Anforderungen der Wissenschaftler betreffen daher besonders folgende Punkte:

- Die zentrumsübergreifende Zusammenführung von diagnostischen und therapeutischen Daten soll helfen, eine möglichst große Zahl Patienten der wissenschaftlichen Evaluation zur Verfügung zu stellen.
- Eine übergreifende epidemiologische Aus- und Bewertung der fallbezogenen Informationen muss möglich sein.
- Der Zusammenhang der klinisch erhobenen Daten mit den Ergebnissen der Forschung, z.B. an biologischen Proben, muss hergestellt werden können, um so die Wertigkeit der Untersuchung für den Behandlungsfall besser beurteilen zu können.

Sonstige teilnehmende Ärzte ohne eigentliche Forschungsinteressen sollen Auswertungen über ihre eigenen Patienten machen können oder im Sinne des Benchmarking vergleichende Statistiken anfordern können; deren Anfertigung fällt in den Aufgabenbereich des Qualitätsbeauftragten.

5.1.4.4 Administrator für die Patientenliste (PL)

Der Betrieb einer Patientenliste wird in Kapitel 6.1 zum Identitätsmanagement näher erklärt. Im Zusammenhang mit dem Klinischen Modul ist festzuhalten, dass zusätzlich zu den Identitäten auch die Behandlungsbeziehungen zwischen Ärzten und Patienten in geeigneter Weise ermittelt und abgebildet werden müssen. Dem Administrator der Patientenliste obliegt im Wesentlichen die Überwachung der Zugriffe im Behandlungszusammenhang. Zu den Auf-

gaben des Administrators gehören auch manuelle Korrekturen bei Falscheingaben in die Patientenliste oder bei softwareseitig unauflösbaren Namenskonflikten.

5.1.4.5 Administrator für eine Klinische Datenbank (KDB)

Der Betrieb einer Klinischen Datenbank erfolgt weitgehend unabhängig von der Patientenliste. Jedoch müssen beide Datenbanken kompatible Identitätsmerkmale verwenden. Dazu gehört sinnvollerweise, wenn auch nicht zwingend erforderlich, die Verwendung der gleichen Benutzernamen, z.B. im Rahmen eines netzweiten einheitlichen Benutzer- und Rechtemanagements.

5.1.4.6 Qualitätsbeauftragter

Der Qualitätsbeauftragte bearbeitet Fragestellungen der medizinischen Qualitätssicherung und des Benchmarkings. Das erfordert das Aufstellen vergleichender Statistiken. Hierzu benötigt er Zugriff auf geeignete exportierte Teildatensätze der MDAT. In seiner technischen Rolle und seinen Rechten unterscheidet er sich nicht von einem externen Forscher.

5.1.4.7 Klinischer Monitor

Im Klinischen Modul kann auch ein Monitoring-Verfahren vorgesehen sein; im Gegensatz zum Studienmodul ist dieses hier aber optional. Das Verfahren unterscheidet sich jedoch nicht von dem in Kapitel 5.2.4 beschriebenen.

5.1.5 Verantwortlichkeiten

Allgemeine Aussagen, die für alle Forschungsverbünde gelten, sind in Kapitel 6.6, Organisatorische Regelungen, zusammengefasst.

Zentrales Merkmal des Klinischen Moduls ist die Trennung von identifizierenden und medizinischen Daten in Patientenliste und Klinischer Datenbank, die durch verschiedene Daten verarbeitende Stellen betrieben werden. Damit soll unterbunden werden, dass eine Stelle Kontrolle über beide Datenbestände erhält. Beide Betreiber sind verpflichtet, unabhängige Zugangsmechanismen und Zugangsprotokolle vorzuhalten, müssen aber einheitliche Zugriffsrichtlinien implementieren, wobei ein zentrales Rechtemanagement hilfreich sein kann. Dieses kann auch in die (Standard-)Benutzerverwaltung der Klinischen Datenbank integriert sein, sofern deren Administration dadurch nicht zu Interessenskonflikten führt.

Ferner muss die Nutzung der MDAT zu Forschungszwecken bzw. der IDAT zu Zwecken der Benachrichtigung bei besonderen Erkenntnissen oder der Rekrutierung für Studien durch den Ausschuss Datenschutz kontrolliert werden.

Dieser weist den jeweiligen Administrator der Klinischen Datenbank bzw. der Patientenliste entsprechend an.

5.1.6 Besondere Aspekte der Realisierung

Software, die für das Datenmanagement des Klinischen Moduls geeignet ist, fällt in eine von drei Kategorien:

- web-basierte Lösungen, die mit Hilfe eines Webservers, einer dahinter liegenden Datenbank und interaktiven Webseiten „selbst gestrickt" werden,
- EDC-Systeme,
- EPA-Systeme (wenn eine pseudonyme Datenhaltung unterstützt wird).

Es gibt aber bisher keine auf dem Markt verfügbare Software, die die Anforderungen an ein Klinisches Modul in einem Forschungsverbund vollständig abdeckt. Schwachpunkt ist die Erfüllung der Notwendigkeit, MDAT und IDAT nirgends außer auf dem Client-Rechner eines behandelnden Arztes gleichzeitig erscheinen zu lassen. Bei einem web-basierten System, bei dem Standard-Browser als Clients verwendet werden, besteht zwar grundsätzlich die Möglichkeit, aus einem einzigen Webformular Daten von verschiedenen Servern abzurufen. Diese als „Cross-Site-Scripting" bekannte Möglichkeit wurde in der Vergangenheit aber als schwerwiegende Sicherheitslücke diskreditiert und wird daher in gängigen Sicherheitseinstellungen unterbunden. Derzeit können drei mögliche Realisierungsvarianten unterschieden werden:

1. Bei einer Auftrags- oder Eigenprogrammierung können solche technischen Möglichkeiten der Datenzusammenführung im Webbrowser genutzt werden[20], die derzeit nicht als Cross-Site-Scripting angesehen und unterdrückt werden. Für einfach gestaltete Szenarien lassen sich so vergleichsweise leicht umzusetzende Software-Lösungen zur Verfügung stellen.
2. Für gehobene Ansprüche – von denen man zumindest in größeren Forschungsverbünden ausgehen muss – wird man in der Regel anstreben, ein kommerzielles Datenmanagementsystem (EDC- oder RDE-System) einzusetzen, wie es vor allem für klinische Studien auf dem Markt angeboten wird. Solche Systeme halten die strikte Trennung zwischen IDAT und MDAT bisher in der Regel aber nicht ein. Verwenden sie für die Applikationslogik einen von der Datenbank getrennten Anwendungsserver, so lässt sich die Datenzusammenführung auf diesen beschränken. Im besonders zu prüfenden Einzelfall könnten die Anforderungen des Klinischen Moduls dann insofern erfüllt werden, als der Anwendungsserver von einem unabhängigen Datentreuhänder betrieben wird.

20 Z.B. auch ein von der Universität Münster zusammen mit der TMF angebotenes Werkzeug, siehe http://www.tmf-ev.de/Produkte/P014012

3. Eine dritte Umsetzungsvariante besteht in dem Einsatz einer entsprechenden Proxy-Software in jeder behandelnden Einrichtung, die die getrennte Anforderung von IDAT und MDAT und die zusammengeführte Weiterleitung an den Client übernimmt[21].

Näher an den Bedürfnissen der klinischen Dokumentation sind vermutlich bestehende Softwaresysteme zur Abbildung von elektronischen Patienten- oder Krankenakten (EPA). Bei diesen Systemen ist die pseudonyme Speicherung samt getrennter Datenhaltung von MDAT und IDAT ebenfalls eine kritische Anforderung. Auch für solche Softwaresysteme ist zu klären, welche der möglichen Varianten einer abgesicherten Zusammenführung von IDAT und MDAT umgesetzt wird.

Die ohnehin strikt empfohlene kryptographische Absicherung aller Datenübertragungswege hilft im Klinischen Modul auch, die Trennung von MDAT und IDAT besonders effektiv umzusetzen: Wenn beide Übertragungswege, d.h. von der Klinischen Datenbank und von der Patientenliste zum peripheren Client, vollständig verschlüsselt sind und sich die Datenströme nicht außerhalb des Clients treffen, kann ein unbefugter Reidentifikationsversuch auch nicht mit Hilfe eines Abhörens des Netzes unternommen werden.

Das Thema der Selbstdokumentation durch Patienten stellt sich im Klinischen Modul genau so wie im Studienmodul dar und wird dort behandelt, siehe Kapitel 5.2.4.

5.2 Studienmodul

5.2.1 Zweck und Anwendungsbereich

Das Studienmodul dient der sicheren Durchführung und Administration einzelner und klar voneinander abgegrenzter, klinischer Forschungsprojekte. Im Unterschied zum Anwendungsbereich des Klinischen Moduls steht jeweils eine explizit formulierte klinische Forschungsfrage im Vordergrund. Entsprechend konkret können Zweck und Dauer der Datenspeicherung angegeben werden, was ein im Vergleich zum Klinischen Modul vereinfachtes Pseudonymisierungsverfahren ermöglicht. Beispielhaft hierfür stehen klinische Studien zur Bewertung neuer oder neu eingesetzter Medikamente oder Medizinprodukte, die gemäß den gesetzlichen Bestimmungen des AMG oder MPG durchzuführen sind. Allerdings ist das Studienmodul in seiner Nutzbarkeit nicht auf solche gesetzlich geregelten Studien beschränkt.

21 Gerade in kleineren behandelnden Einrichtungen wie beispielsweise Arztpraxen könnte eine solche Zwischenstation zwischen dem öffentlichen Netz und dem Rechner des behandelnden Arztes auch aus Sicherheitsgründen befürwortet werden, weitere Hinweise in [weitere Hinweise in 30]

Das Studienmodul muss für einen forschenden Personenkreis, der ggf. keinen Behandlungsauftrag des Patienten und möglicherweise auch keinen direkten Kontakt zu dem Patienten hat, einen pseudonymisierten oder anonymisierten Zugriff auf die Patientendaten erlauben. Allerdings ist in den allermeisten Studien oft schon aus Sicherheitsgründen auch ein Rückschluss auf die Identität eines Patienten unter bestimmten Umständen notwendig, so dass sich die Verwendung anonymer Kennungen verbietet. Im Arzneimittelrecht ist zudem die Verwendung von Pseudonymen vorgeschrieben. Im Folgenden wird daher nur noch auf die pseudonymisierte Datenhaltung im Studienmodul eingegangen. Die pseudonymisierte Speicherung und Verarbeitung der Daten im Studienmodul setzt als Rechtsgrundlage in aller Regel eine informierte Einwilligung der Probanden voraus (vgl. Kap. 4). Prinzipiell ließe sich ein stark vereinfachtes Studienmodul auch mit anonymen Kennungen nutzen; einige Anwendungsfälle könnten dann jedoch nicht in der hier beschriebenen Form umgesetzt werden.

Für das Studienmodul wird keine doppelte Pseudonymisierung gemäß Modell B in der ersten Version der generischen Datenschutzkonzepte der TMF vorausgesetzt. Zusätzliche Schutzmaßnahmen werden erst erforderlich, wenn die Daten einer Studie oder eines Forschungsprojekts nach dessen Ende weiterhin in pseudonymisierter Form gespeichert und mit den Daten aus anderen Forschungsprojekten zusammengeführt werden sollen.

5.2.2 Anwendungsfälle

5.2.2.1 Patienten aufklären und Einwilligung einholen

Wenn die Kriterien und Voraussetzungen für die Aufnahme eines Patienten in eine klinische Studie gegeben sind, klärt der behandelnde Arzt oder Prüfarzt den Patienten umfassend auf und dokumentiert dessen schriftliche Einwilligung (vgl. Kap. 3.2.3.1). Dies kann nur an einer Stelle geschehen, wo die Aufbewahrung der identifizierenden Daten der Probanden unproblematisch ist. Im Regelfall ist dies die jeweilige ärztlich geleitete, behandelnde Einrichtung oder, im Falle einer übergreifenden Dateninfrastruktur, zusätzlich ein zentraler Datentreuhänder.

Als datenschutzrechtliche Besonderheit in klinischen Studien nach Arzneimittelrecht ist zu beachten, dass der Patient darüber aufzuklären ist, dass seine Daten auch nach einem Widerruf weiterhin verwendet werden, falls dies gemäß § 40 (2a) Satz 2 Nr. 3 AMG erforderlich ist, um Wirkungen des zu prüfenden Arzneimittels festzustellen, um sicherzustellen, dass schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden, oder um der Pflicht zur Vorlage vollständiger Zulassungsunterlagen zu genügen.

5.2.2.2 Patienten in eine Studie aufnehmen

Im Anschluss an die Dokumentation der schriftlichen Einwilligung wird für einen Patienten ein Subject Identification Code (SIC) als pseudonyme ID erstellt. Der SIC dient im Laufe der Studie zur Identifikation eines Datensatzes, gerade auch für die Kommunikation zwischen verschiedenen an der Studie beteiligten Personen.

5.2.2.3 Daten erheben

Die Erhebung von Studiendaten wird im Regelfall in Kenntnis des konkreten Probanden, aber nur unter Verwendung des Pseudonyms durchgeführt. Aus der Perspektive eines generischen Datenschutzkonzepts ist es dabei unerheblich, ob zunächst auf Papier dokumentiert wird und diese Bögen (CRF) in der behandelnden Einrichtung oder in einer durch die Studienleitung mit der die Datenerfassung und -verarbeitung beauftragten Studienzentrale in eine elektronische Studiensoftware (EDC) übertragen werden oder ob überhaupt keine Papier-Bögen mehr eingesetzt werden und direkt eine Eingabe in ein Studiensoftwaresystem erfolgt. Wichtig ist, dass in allen Fällen die Daten lediglich im Zusammenhang mit dem SIC als pseudonymer Kennung und ohne Einsicht in die identifizierenden Daten der Probanden dokumentiert werden.

Dabei können die Studiendaten eines Patienten ggf. auch in verschiedenen Einrichtungen oder durch verschiedene Studienärzte erhoben werden. In diesen Fällen ist zu klären, dass für alle beteiligten Stellen das Vorliegen der Einwilligung eindeutig dokumentiert ist und dass alle Daten mit dem gleichen SIC als pseudonymer Kennung für eine spätere Zusammenführung versehen werden.

5.2.2.4 Unerwartete Ereignisse managen

Unerwartete Ereignisse von medizinischer Relevanz können in jedem klinischen Forschungsprojekt auftreten und führen zu bestimmten Kommunikationsanforderungen. Besonders gesetzlich geregelt sind diese im AMG für klinische Studien mit einem besonderen, pharmakologisch begründeten Risikopotenzial für die Probanden. Neben der behandlungsseitigen, klinischen Dokumentation solcher Ereignisse ist somit auch eine Dokumentation im Zusammenhang mit dem Forschungsprojekt notwendig. Hierfür genügt im Regelfall die Zuordnung der medizinisch relevanten Daten zu dem Pseudonym des betroffenen Probanden.

In gesetzlich geregelten Studien nach AMG sind darüber hinaus auch gesetzliche Meldepflichten unerwünschter Ereignisse zu beachten. Die Kennzeichnung solcher Datensätze mit den Initialen und Geburtsdaten der Probanden, die in Anlehnung an internationale Empfehlungen [z.B. 31] bisher häufig verwendet wurde, ist nicht als ausreichende Pseudonymisierung anzusehen

[11, S. C34]. Die internationalen Vorgaben erlauben jedoch die Verwendung echter Pseudonyme in Kombination mit dem Alter des Probanden, wenn entsprechende nationale Vorgaben dies vorschreiben. Da im AMG die Pseudonymisierung der Daten in der Kommunikation mit dem Sponsor einer Studie vorgeschrieben ist und dieser wiederum für die Meldung unerwünschter Ereignisse gegenüber den Behörden verantwortlich ist, wird hierfür die durchgängige Verwendung der Pseudonyme – also hier der SICs – mit der Angabe des Alters und ohne Angabe des Geburtsdatums empfohlen. Dies gilt auch, wenn die Meldepflichten vom Sponsor an den Leiter der klinischen Prüfung oder andere Einrichtungen delegiert werden.

5.2.2.5 Datenqualität sichern

Auch die Prozesse der Qualitätssicherung klinischer Forschungsdaten sind mit einer Kommunikation pseudonymer Daten verbunden, wobei ein Kommunikationspartner die Zuordnung des Pseudonyms zum Patienten kennt und der andere im Regelfall nicht. So können im zentralen Datenmanagement Rückfragen zu den Daten eines Patienten formuliert werden, ohne dass die Identitätsdaten des Patienten hierfür benötigt werden. Wenn diese Rückfragen vom Studienarzt oder anderem ärztlich geführten Personal mit Patientenkontakt bearbeitet werden, geschieht dies im Regelfall in Kenntnis der Identität des betroffenen Patienten.

Ein wichtiges Verfahren zur Sicherstellung korrekter Daten in klinischen Studien ist das Monitoring. Dies wird durch speziell geschulte und hierfür beauftragte Personen durchgeführt, die in die beteiligten behandelnden Einrichtungen gehen und dort die erhobenen Daten mit den Quelldaten, im Regelfall den Patientenakten, abgleichen. Da dabei ein zusätzlicher Personenkreis Kenntnis personenbezogener Daten erhält, müssen die Patienten über dieses Verfahren aufgeklärt worden sein und dazu ihre Einwilligung gegeben haben (vgl. § 40 (2a) Satz 2 Nr. 1 Buchstabe a AMG).

Eine weitere Möglichkeit zur Sicherung einer hohen Datenqualität ist z.B. die Einbindung einer Referenzbefundung (vgl. Kap. 3.2.4.1).

5.2.2.6 Audit durchführen oder unterstützen

Durch Audits werden Prozessabläufe hinsichtlich der Erfüllung von Anforderungen und Richtlinien bewertet. Im Regelfall werden diese von speziell hierfür geschulten, unabhängigen und externen Fachleuten durchgeführt. Im Kontext von klinischen Studien ist ein Audit Bestandteil der Qualitätssicherung. Hierbei werden sämtliche Prozesse auf Übereinstimmung mit Studienplan, Richtlinien, SOPs und anderen verbindlichen Festlegungen – auch hinsichtlich Datenschutzmaßnahmen – geprüft. Ein Zugriff auf konkrete Daten ist, im Gegensatz zum Monitoring, allenfalls stichprobenartig nötig; ein Personenbezug muss im Regelfall nicht offenbart werden.

5.2.2.7 Auskunft geben

Die Patienten haben ein Recht auf Auskunft über die von ihnen gespeicherten personenbezogenen Daten. Zudem sind diese auf Verlangen der Patienten auch zu korrigieren (vgl. Kap. 4.4.1). Der Patient wendet sich hierzu an den zuständigen Prüf- bzw. Studienarzt, der Zugriff auf den vollständigen Datensatz des Patienten hat und diesem entsprechend Auskunft geben kann. Wenn im Falle einer AMG-Studie ein Patient die Entblindung seiner Studienmedikation verlangt, so ist dies nach Prüfung im Einzelfall entweder als Prüfplanverletzung umzusetzen und zu dokumentieren, oder auch als Rückzug der Einwilligung zu interpretieren, der einen Studienabbruch für diesen Patienten zur Folge hat.

5.2.2.8 Daten auswerten

Die Auswertung klinischer Forschungsdaten wird im Regelfall von Personen durchgeführt, die keinen direkten Patientenkontakt im Rahmen der Datenerhebung hatten und die die Identitätsdaten der Patienten nicht benötigen. In Einzelfällen kann es Abweichungen hiervon geben, wenn z.B. der Sponsor einer klinischen Prüfung mit dem Behandler identisch ist (s. Kap. 5.2.3.3 und 6.2.3.3). Somit können die Daten für die Auswertung in pseudonymisierter Form bereitgestellt werden, sofern hierfür Gründe vorliegen. Dies können z.B. Vorschriften aus dem AMG zur pseudonymisierten Weitergabe von Patientendaten an den Sponsor sein oder der Umstand, dass im Rahmen der Auswertung mit Ergebnissen zu rechnen ist, die möglicherweise eine personenbezogene Rückmeldung an einzelne beteiligte Probanden auch aus Patientensicht wünschenswert erscheinen lassen und eine solche Rückmeldung vereinbart wurde. Wenn kein Grund für die pseudonymisierte Auswertung vorliegt, werden die Daten in anonymisierter Form bereitgestellt.

5.2.2.9 Ergebnisse mitteilen

Nach Auswertung der Daten einer Studie werden den Patienten klinisch relevante Ergebnisse durch die behandelnden Ärzte mitgeteilt. Alternativ kann im Rahmen der Einwilligung vereinbart werden, weitere Ergebnisse mitzuteilen und auch den Kreis der mitteilungsberechtigten Personen zu erweitern.

5.2.2.10 Daten archivieren

Die Archivierung aller medizinisch relevanten Behandlungsunterlagen gehört zu den allgemeinen ärztlichen Dokumentations- und Aufbewahrungspflichten. Der hierfür relevante Rechtsrahmen ist auf eine Reihe allgemeiner (z.B. MBO, SGB-V) oder spezialgesetzlicher Regelungen (z.B. RöV, StrlSchV) verteilt. Im Rahmen klinischer Studien kommen Regelungen wie das AMG oder das MPG hinzu, die neben der ärztlichen Dokumentation eines Behandlungsfalls auch zusätzliche Daten und Dokumente fokussieren, die studienspezifisch sind.

Hierzu gehören z.B. die Einwilligungserklärungen der Probanden, die Dokumentation unerwünschter Ereignisse oder die Case Report Forms (CRFs) [9; 10].

Aus Datenschutzsicht relevant ist, dass auch bei der Archivierung der Studienunterlagen eine Aufteilung in Archive mit Identifikationsdaten und solche mit lediglich pseudonymisierten Daten möglich ist. Bei Studien nach AMG ist die Pseudonymisierung aller Unterlagen vorgeschrieben, die dem Sponsor übermittelt werden. Dieser hat entsprechend nur pseudonymisierte Daten zu archivieren, während der Prüfer z.B. auch die unterschriebenen Einwilligungserklärungen der Probanden rechtssicher aufbewahren muss [9].

5.2.2.11 Daten sperren, anonymisieren oder löschen

Die Probanden in klinischen Forschungsprojekten haben jederzeit das Recht, ihre Einwilligung in die Teilnahme zurückzuziehen. Im Regelfall sind dann alle zentral wie dezentral gespeicherten Daten zu löschen oder zu anonymisieren. Im Falle einer Anonymisierung sind die Identitätsdaten zu löschen, so dass zwischen diesen und einer vormals pseudonymen Kennung keine Beziehung mehr hergestellt werden kann. Wenn zusätzlich zu einer zentralen Patientenliste auch dezentrale Listen in den behandelnden Einrichtungen geführt werden, so sind auch in diesen die Einträge für den jeweiligen Probanden zu löschen. Wenn davon auszugehen ist, dass die pseudonyme Kennung aufgrund ihrer früheren Verwendung von einigen Personen nach wie vor dem konkreten Probanden zugeordnet werden kann, so sollte die vormalige pseudonyme Kennung durch eine neue anonyme ID ersetzt werden.

In klinischen Prüfungen gemäß Arzneimittelrecht ist zu beachten, dass auch bei einem Widerruf der Einwilligung bestimmte Daten nach § 40 (2a) Satz 2 Nr. 2 und 3 AMG weiterhin pseudonymisiert gespeichert werden müssen. Dies betrifft insbesondere die Notwendigkeit einer Übermittlung vollständiger Daten an die Oberbehörden im Rahmen eines Zulassungsverfahrens und Fälle, in denen die Sicherheit der Probanden anderenfalls nicht gewährleistet werden könnte. In Zweifelsfällen sollte zunächst zumindest eine Sperrung der Daten erfolgen.

Verstirbt ein Proband, so ist analog zum Rückzug der Einwilligung, inklusive der im AMG definierten Ausnahmeregelungen, zu verfahren. Eine anonymisierte Auswertung der bisher erhobenen Daten ist im Regelfall jedoch möglich.

5.2.2.12 Weitere Anwendungsfälle

Die folgenden Anwendungsfälle mit Behandlungsbezug sind prinzipiell auch im Studienmodul umsetzbar:

- Auskunft an weiterbehandelnden Arzt
- Zugriffsberechtigungsvergabe durch Vorbehandler oder Patient an weiterbehandelnden Arzt und Auskunft
- Zugriffsvergabe (Ausführung) durch Datenmanager oder Rechtemanager an weiterbehandelnden Arzt und Auskunft

Wie solche Anwendungsfälle konkret und vor allem IT-gestützt umgesetzt werden können, hängt jedoch sehr von der verwendeten Software, insbesondere für die Datenerfassung und das Studiendatenmanagement, ab. Kennzeichnend für das Studienmodul bleibt jedoch der Zugriff auf die zentrale Datenbasis mit Hilfe einer pseudonymen ID. Der Zugriff behandelnder Ärzte unter Verwendung der identifizierenden Daten der Patienten und die Regelungen zur dafür nötigen Zugriffsvergabe werden in dem Kapitel 5.1 zum Klinischen Modul sowie in den Kapiteln 6.1 und 6.2 zum Identitäts- und Rechtemanagement detailliert beschrieben.

5.2.3 Daten und Datenflüsse

5.2.3.1 Variante mit zentraler Patientenliste

Im Regelfall umfasst das Studienmodul drei Arten beteiligter Stellen:

1. die behandelnden Ärzte bzw. Prüfärzte, respektive die beteiligten Zentren,
2. eine zentrale Patientenliste samt Administration
3. und eine oder mehrere Studiendatenbanken mit dem zuständigen Personal.

Grundsätzlich können in einem Studienmodul mehrere Studien mit unterschiedlichen Studienzentralen parallel oder nacheinander durchgeführt werden, so dass ggf. eine große Zahl behandelnder Einrichtungen und auch mehrere Studiendatenbanken parallel zu verwalten sind. Es wird auch in solchen Konstellationen eine zentrale Patientenliste empfohlen.

Nach Einwilligung des Probanden in die Teilnahme am Forschungsprojekt wird das hierzu unterschriebene Dokument entweder in der behandelnden Einrichtung oder bei einer zentralen Stelle, die auch die Patientenliste verwaltet, aufbewahrt. Für den Probanden wird eine pseudonyme ID erzeugt, die an zentraler Stelle in der Patientenliste zusammen mit den identifizierenden Daten gespeichert wird. Der Studiendatenbank als zentralem Dokumentationssystem wird entweder eine projekt- oder studienübergreifende ID als PID_S oder ein studienspezifischer Subject Identification Code (SIC) zur Verfügung gestellt. Bei der Nutzung von SICs im Rahmen einer Studie ist eine spätere Zusammenführung von Daten möglich, wenn im zentralen ID-Management die unterschiedlichen SICs eines Patienten zusammen mit einem einheitlichen PID_S verwaltet werden. Die detaillierten Anforderungen an die Erzeugung solcher IDs sind im Kapitel 6.1 zum ID-Management beschrieben. Eine von der TMF zur Verfügung gestellte Software-Komponente hierfür, der PID-Generator, ist in Kapitel 6.1.6.1 dargestellt.

Die behandelnde Einrichtung erhebt die identifizierenden Daten (IDAT) der Probanden. Diese werden zusammen mit den Daten über die erhebende Stelle ($OrgDAT_{PL}$) verschlüsselt an die zentrale Patientenliste geschickt. Diese speichert IDAT und $OrgDAT_{PL}$ und schickt eine pseudonyme ID, entweder PID_S oder

SIC, an die behandelnde Stelle zurück. Die behandelnde Einrichtung dokumentiert alle weiteren Daten zum Probanden (MDAT) zusammen mit der pseudonymen ID (PID_S oder SIC) und schickt diese an die Studiendatenbank zur Speicherung der Daten zur Laufzeit der Studie.

Die Studiendatenbank und die Patientenliste stehen unter getrennter administrativer Aufsicht, es gibt keine übergreifende Weisungsbefugnis. Die jeweiligen Aufgaben und Befugnisse sind in den Regelwerken des Forschungsverbunds definiert. Entsprechend der in Kapitel 6.7 aufgeführten Kriterien der Verhältnismäßigkeit kann in bestimmten Fällen von der administrativen Trennung auch abgesehen werden.

In der Studiendatenbank wird im Regelfall auch eine Information über die datenliefernde Stelle als Teil des medizinischen Datensatzes (MDAT) gespeichert. Somit wird die Herkunft eines Datensatzes in Bezug auf den Arzt oder Prüfer sowohl als Teil der MDAT in der Studiendatenbank wie auch als Teil der $OrgDAT_{PL}$ in der Patientenliste gespeichert. Dies ist unproblematisch, solange je datenliefernder Stelle oder je Zentrum eine ausreichend große Zahl an Probanden rekrutiert wird und eine Reidentifikation aufgrund der Kenntnis der Einrichtung ausgeschlossen werden kann. Wenn jedoch die Angabe der behandelnden Einrichtung ein nennenswertes Reidentifizierungsrisiko darstellt, muss diese Information aus dem MDAT-Datensatz entfernt werden und darf nur noch als $OrgDAT_{PL}$ als Teil der Angaben in der Patientenliste hinterlegt sein. Die doppelte Speicherung der datenliefernden Stelle bzw. der behandelnden Einrichtung führt zu einer vereinfachten Abbildung der Prozesse zur Qualitätssicherung und des Rückfragemanagements, wie auch des Monitorings und des Managements unerwarteter Ereignisse. Für diese Prozesse ist eine Beteiligung der Patientenliste dann nicht mehr notwendig. Hierfür kann jeweils eine direkte Kommunikation zwischen der Studiendatenbank und den datenliefernden Stellen genutzt werden.

Nach Abschluss des Forschungsprojekts oder der Studie sind die Daten der Studiendatenbank und der Patientenliste zu anonymisieren oder zu löschen, sofern keine Zusammenführung in zweifach pseudonymisierter Form in einer Forschungsdatenbank entsprechend der in Kapitel 6.4 beschriebenen Form geplant ist. Unabhängig von der weiteren Verarbeitung oder Löschung der Daten in der Studiendatenbank müssen ggf. die gesetzlichen Aufbewahrungspflichten, z.B. für klinische Studien gemäß AMG, berücksichtigt werden. Dies kann bedeuten, dass pseudonymisierte Daten weiterhin in einer Studienzentrale aufzubewahren sind, allerdings nicht mehr im direkten Zugriff der Forscher. Der Zugriff auf die archivierten Daten ist entsprechend zu regeln.

5.2.3.2 Variante ohne zentrale Patientenliste

In bestimmten Fällen wird eine zentrale Patientenliste entweder nicht benötigt oder nicht umsetzbar sein. Insbesondere wenn Patienten mit hoher Wahr-

scheinlichkeit nur in ein einziges Forschungsprojekt eingeschlossen werden und die Daten eines Patienten nur in genau einer Einrichtung erhoben werden, kann eine lokale Erzeugung von Pseudonymen je Einrichtung ausreichend sein. Allerdings ist zu beachten, dass eine Kontaktaufnahme mit den Patienten nicht mehr möglich ist, wenn die behandelnde Einrichtung diese nicht mehr vermitteln kann. Problematisch kann eine Umsetzung einer zentralen Patientenliste sein, wenn allein aus dem Vorhandensein eines IDAT-Datensatzes in der zentralen Datei Rückschlüsse auf eine z.B. stigmatisierende Erkrankung gezogen werden können. Insofern enthalten die IDAT im Regelfall indirekt auch ein medizinisches Datum wie z.B. die Diagnose. Eine zentrale Patientenliste wird im Regelfall nicht beschlagnahmesicher organisiert werden können, auch dann nicht, wenn ein Notar mit der Führung und Administration beauftragt wird (s. Kap. 4.2.5). Dies kann für bestimmte Patientengruppen eine zentrale Patientenliste so unattraktiv machen, dass ausreichende Rekrutierungsraten verhindert werden.

Ohne eine zentrale Patientenliste und damit im Regelfall auch ohne eine zentrale treuhänderische Verwaltung der Einwilligungserklärungen, werden die Einwilligungserklärungen und die identifizierenden Daten in den behandelnden Einrichtungen verbleiben. Es ist im Regelfall zu empfehlen, eine lokale Patientenliste anzulegen und sicher aufzubewahren, da dies im Falle von Nachfragen zu einem deutlich schnelleren Auffinden der nötigen Unterlagen führt. Die Verantwortlichkeiten für die lokale Patientenliste sind klar zu definieren und festzulegen.

In der Studiendatenbank ist in diesem Falle immer die datenliefernde Stelle zu vermerken. Die dadurch entstehenden potenziellen Reidentifikationsrisiken bei Zentren mit sehr geringen Rekrutierungszahlen sind zu berücksichtigen. Die Kommunikation zwischen Studiendatenbank und datenliefernden Stellen ist, von dieser Notwendigkeit abgesehen, analog zu der Variante mit zentraler Patientenliste konzipierbar.

5.2.3.3 Identität von Sponsor und Prüfer

Vornehmlich wissenschaftlich motivierte Arzneimittelstudien, so genannte Investigator Initiated Trials (IIT), unterliegen seit der 12. Novellierung des Arzneimittelrechts denselben Regularien wie die industriell gesponsorten Studien im Vorfeld einer Zulassung. Damit gilt auch hier das im AMG vorgeschriebene Pseudonymisierungsgebot bei Weiterleitung von Daten an den Sponsor. Wenn jedoch in einer monozentrischen Studie an einem Universitätsklinikum die Rollen des Sponsors und Prüfers zusammenfallen, ist eine durchgängige Pseudonymisierung gegenüber den im Behandlungsverhältnis stehenden Prüfärzten als Angestellten des Sponsors verzichtbar. Weitere Informationen zu diesem Spezialfall finden sich in Kapitel 4.3.1 zu den ethischen und rechtlichen Grundlagen.

5.2.4 Nutzer, Rollen und Rechte

Für die Patientenliste wird ein Administrator und ggf. eine Dokumentationskraft zur Unterstützung benötigt. Diese haben vollen Zugriff auf den IDAT-Datensatz und sind entsprechend zum datenschutzgerechten Umgang mit diesen Daten zu verpflichten. Insbesondere müssen sie bei Depseudonymisierungsanfragen die identifizierenden Daten zu den jeweiligen Pseudonymen herausgeben, wenn dies von dem hierfür zuständigen Gremium angeordnet wird. Solche Gremien, für die die Bezeichnung „Ausschuss Datenschutz" benutzt wird, werden ausführlicher in dem Kapitel 5.2.5 zu den Verantwortlichkeiten und bei den organisatorischen Regelungen in Kapitel 6.6 beschrieben.

Für die Studiendatenbank ist ebenfalls administratives Personal notwendig. Zudem sind hier die Mitarbeiter des zentralen Datenmanagements anzusiedeln, die Zugriff auf die Daten aller Probanden in der Studiendatenbank haben.

Die Studienärzte oder Dokumentationskräfte in den behandelnden Einrichtungen sollten nur die Daten ihrer Probanden sehen. Dies ist auch bei einem Electronic Capture System (EDC) – oft auch als Remote Data Entry System (RDE) bezeichnet – umzusetzen, in dem sowohl die Probanden, als auch die Prüfer jeweils genau einer datenliefernden Stelle zugeordnet werden.

Vermehrt werden auch Patienten selbst in die Dokumentationsabläufe eingebunden. So sind z.B. bei Forschungsprojekten zum Thema „Schmerzen" zunehmend „Schmerztagebücher" durch die Patienten selbst zu führen. Hintergrund dessen ist unter anderem die schon länger bekannte aber erst in der jüngeren Vergangenheit vermehrt diskutierte Unsicherheit retrospektiver Auskünfte von Patienten bei dem gleichzeitigen Wunsch nach möglichst relevanten und validen Endpunkten [vgl. z.B. 32]. Solche Funktionen können effektiv auch durch EDC-Systeme unterstützt werden, wobei dann sichergestellt werden muss, dass die Patienten nur jeweils auf ihre eigenen Daten zugreifen können. Zudem ist darauf zu achten, dass eine potenziell unsichere Systemumgebung beim Zugriff durch Patienten nicht die Sicherheit des Gesamtsystems gefährden darf.

In klinischen Studien, in denen eine bestimmte Datenqualität vorgeschrieben ist, werden Monitore eingesetzt, die die eingegebenen Daten auf Plausibilität und ggf. Übereinstimmung mit den Quelldaten überprüfen. Diese müssen sowohl Zugang zu den von ihnen zu überprüfenden zentralen Patientendaten, wie auch zu den Quelldaten in den beteiligten Zentren und behandelnden Einrichtungen haben. Da dieser Nutzerkreis außerhalb des Behandlungsverhältnisses steht und gleichzeitig auch Zugriff auf nicht pseudonymisierte Unterlagen hat, müssen Patienten entsprechend darüber aufgeklärt werden und darin einwilligen. Eine klare Verpflichtung aller Beteiligten auf einen datenschutzgerechten Umgang mit den Daten ist unerlässlich.

Im Rahmen klinischer Prüfungen nach AMG ist eine definierte Sponsorschaft Voraussetzung für die Zulassung der Studie. Ergänzend zu den Regelungen

für die Nutzer im Studienzentrum können auch besondere Zugriffsregeln an eine Sponsorrolle gebunden sein. Dies hängt davon ab, welche Aufgaben des Sponsors an die Studienzentrale delegiert werden. Einzelne Aufgabenfelder wie das SAE-Management oder die Archivierung der Daten können vom Sponsor an die Studienzentrale delegiert oder auch selbst übernommen werden. Entsprechend muss das Rollen- und Rechtesystem die Aufgabenverteilung abbilden können.

5.2.5 Verantwortlichkeiten

In einem Studienmodul ist möglicherweise die Verantwortlichkeit für die Durchführung einer einzelnen Studie von der Verantwortlichkeit für die Infrastruktur und das Studienmodul insgesamt zu trennen. Beide Verantwortlichkeiten, auch wenn sie von derselben juristischen Person übernommen werden, sollten klar geregelt und transparent dargestellt werden. Auf der Ebene einer einzelnen Studie ist ggf. auch die gesetzlich vorgeschriebene Verantwortlichkeit eines Sponsors festzulegen, wenn die Studie in den Anwendungsbereich des AMG oder MPG fällt. Wichtig ist die Festlegung einer übergeordneten Verantwortlichkeit dann, wenn die Daten nach der Beendigung einer Studie weiterhin pseudonymisiert vorgehalten und genutzt werden sollen (vgl. Kap. 6.4) oder wenn eine Studieninfrastruktur rechtlich unabhängig von einem oder mehreren Sponsoren einzelner Studien betrieben wird.

Die Gesamtverantwortung für das Studienmodul wird im Regelfall in der Studienzentrale liegen, die ggf. eine externe Einrichtung mit dem Aufbau und Management der Patientenliste beauftragt. Allerdings sind bei einer Einbettung des Studienmoduls in eine übergreifende Forschungsinfrastruktur auch andere Verantwortlichkeiten denkbar. So könnte die zentrale Verantwortlichkeit auch bei der Netzwerkzentrale eines übergeordneten Forschungsverbunds angesiedelt sein, insbesondere dann, wenn diese ggf. wechselnde Studienzentralen mit der Durchführung von Forschungsprojekten beauftragt.

In jedem Falle ist eine klare Benennung der Verantwortlichkeiten vorzunehmen. Insbesondere wird die Einrichtung eines zentralen Gremiums vorgeschlagen, welches über datenschutzrechtlich sensible Fragen, wie z.B. solche der Depseudonymisierung, zu entscheiden hat. Hierfür wird der Begriff „Ausschuss Datenschutz“ verwendet. Eine solche zentrale Einrichtung sollte zudem die Richtlinien und Policies im Umgang mit den Daten vorgeben.

Die Patientenliste ist der sensibelste Teil des Identitäts-Managements und ist damit, wenn sie zentral geführt wird, ein besonders schützenswerter Bereich. Datenschutzrechtlich ist zu berücksichtigen, dass die IDAT, obwohl sie in der Patientenliste nicht mit medizinischen Daten (MDAT) kombiniert werden, den betroffenen Personenkreis als Patienten eines Forschungsnetzes mit einem umschriebenen Krankheitsspektrum ausweisen können. Im Falle eines stigmatisierenden oder in anderer Hinsicht besonders sensiblen Krankheits-

bereichs ist daher eine auch in den Augen der betroffenen Patienten besonders vertrauenswürdige Stelle mit der Führung der Patientenliste zu beauftragen.

Die Studiendatenbank mit den medizinischen Daten (MDAT) und ggf. organisatorischen Daten unterliegt der Verantwortlichkeit der Leitungsebene der Studienzentrale bzw. den von dieser hierfür benannten Verantwortlichen. Die Verantwortlichkeit hierfür kann zudem in übergreifenden Forschungsinfrastrukturen in übergeordnete Verantwortlichkeiten eingebettet sein.

Nicht zu vergessen sind notwendige Regeln und Verantwortlichkeiten in den beteiligten Einrichtungen, in denen die Patienten untersucht und Daten erhoben werden. Wenn die Dateneingabe mittels EDC direkt in ein zentrales System erfolgt, sind auch Regeln für den Umgang mit den Zugangskriterien (z.B. Passwörter, PINs oder Chipkarten) zu definieren und einzuhalten. Hierfür müssen Verantwortliche in den beteiligten Einrichtungen festgelegt werden. Gleiches gilt für den Umgang mit einer lokalen Patientenliste, die üblicherweise ergänzend zu einer zentralen Liste geführt wird.

Wenn die Verantwortung für die Durchführung einer Studie bei einer vom Studienmodul rechtlich unabhängigen Stelle liegt, z.B. einem Sponsor gemäß AMG oder MPG, so hat dieser das Studienmodul bzw. einzelne Stellen wie die Studienzentrale oder an der Studie teilnehmende Zentren mit der Durchführung der relevanten Teilaufgaben zu beauftragen. Verantwortlichkeiten für Teilaufgaben wie z.B. die Datenerfasssung oder auch die Archivierung von Studiendaten können delegiert werden. Dabei hat ein Sponsor gemäß AMG jedoch die Pflicht, sich von der Eignung aller Beauftragten hinsichtlich einer GCP-konformen Durchführung einer Studie zu überzeugen und dies in ausreichendem Maße zu kontrollieren. Weitere Hinweise zur Sponsorschaft in klinischen Prüfungen nach der 12. AMG-Novelle können einem Kurzgutachten der Kanzlei Sträter entnommen werden [33].

5.2.6 Aspekte der Realisierung

Für die IT-Unterstützung klinischer Studien ist im Regelfall die Verwendung eines Studiensoftwaresystems empfehlenswert, welches z.B. die Definition elektronischer Eingabeformulare (Electronic Case Report Forms, eCRF) erlaubt, die von den beteiligten Einrichtungen für eine dezentrale Dateneingabe (Electronic Data Capture, EDC) genutzt werden können. Aus Datenschutzsicht ist entscheidend, dass solche Systeme eine verschlüsselte Übertragung der Daten (SSL) garantieren und zudem sicherstellen, dass keine identifizierenden Daten in direktem Zusammenhang mit medizinischen Daten erfasst und an den zentralen Server übermittelt werden. Zudem sollte gewährleistet sein, dass die Mitarbeiter eines beteiligten Zentrums nur die Daten „ihrer" Patienten einsehen und verändern können. Wenn Patienten in die Dokumentation derart eingebunden werden, dass sie auch einen Zugang zu dem Softwaresystem bekommen, muss darüber hinaus sichergestellt sein, dass jeder Patient nur seine eigenen Daten sieht und ggf. bearbeiten kann.

Solche Softwaresysteme bieten im Regelfall auch eine Funktion für die Erzeugung pseudonymer IDs (als Subject Identification Code, SIC), so dass für die Durchführung einzelner Studien ggf. kein zusätzliches Pseudonymisierungstool benötigt wird. Zu berücksichtigen ist allerdings, dass häufig keine zentrale Speicherung und Verwaltung der identifizierenden Daten mit angeboten wird. Eine Reidentifizierung eines Patienten ist dann nur mit Hilfe der dezentralen Listen in den beteiligten Einrichtungen oder bei manueller Durchsicht der ggf. zentral hinterlegten Einwilligungserklärungen möglich. Spätestens wenn ein übergeordnetes ID-Management benötigt wird, z.B. für die Zuordnung von Datensätzen eines Patienten aus mehreren Studien zueinander oder bei Beteiligung mehrerer Softwaresysteme mit unterschiedlichen Pseudonymisierungsvorgaben oder -funktionen, reichen die Funktionen dieser Softwaresysteme üblicherweise nicht mehr aus. In diesen Fällen empfiehlt sich die Verwendung einer hierfür spezialisierten Softwarekomponente, wie z.B. des PID-Generators der TMF. Eine solche Software hat die Aufgabe, entweder für jede einzelne Studie einen SIC entgegenzunehmen und zusammen mit den IDAT zu verwalten oder jeweils einen SIC auf Basis der IDAT selbst zu erzeugen und herauszugeben. Ein übergeordnetes ID-Management erfordert darüber hinaus die Zuordnung mehrerer SICs zu einem Patienten über ein übergeordnetes Pseudonym, den PID_S. Die Nutzung eines PID_S für eine dauerhafte Zusammenführung von Daten aus mehreren einzelnen Forschungsprojekten oder Studien ist in Kapitel 6.4 beschrieben.

Für die Nutzung in klinischen Studien nach AMG entsprechen fertig entwickelte Softwaresysteme üblicherweise hinsichtlich Funktionsumfang, Qualitätssicherung und Dokumentation den umfangreichen gesetzlichen Vorgaben bzw. den Kriterien der Good Clinical Practice (GCP). Hierzu gehört z.B. die Funktion eines umfassenden Audit-Trails, in dem alle Änderungen an Datensätzen nachvollziehbar gespeichert werden. Eigenentwicklungen oder nicht für AMG-Studien konzipierte Systeme genügen solchen Anforderungen häufig nicht. Bei Nutzung einer zusätzlichen Softwarekomponente für das zentrale ID-Management ist zu beachten, dass letzteres entsprechend den gesetzlichen Vorgaben und internationalen Regularien nur dann zu validieren ist, wenn die Softwarekomponente in das ID-Management einer einzelnen Studie eingreift. Wenn das zentrale ID-Management hingegen im Rahmen einer Studie nur vom validierten Studiensoftwaresystem generierte SICs entgegennimmt und diese nur für studienübergreifende Zwecke, wie z.B. Metaanalysen, wieder herausgibt, dann kann eine Validierung gemäß GCP für die Softwarekomponente des zentralen ID-Managements entfallen.

5.3 Forschungsmodul

Das Forschungsmodul stellt die Adaption des Modells B des bisherigen generischen Datenschutzkonzepts der TMF dar; die Einordnung in die übergeordneten Strukturen ist in Kapitel 6.1.7 beschrieben.

Die Bezeichnung als „Forschungsmodul" bedeutet *nicht*, dass in den anderen Modulen keine Forschung stattfindet, sondern bezieht sich auf das Charakteristikum, dass hier die Forschung vom direkten klinischen Bezug entkoppelt und insbesondere nicht mit der direkten Krankenversorgung verzahnt ist. Das Forschungsmodul sieht zudem primär keine eigene Datenerfassung vor, sondern übernimmt Daten aus einem Klinischen (vgl. Kap. 5.1) oder Studien-Modul (vgl. Kap. 5.2) oder einer anderen geeigneten Datenquelle.

Ein Forschungsmodul kapselt eine oder mehrere Forschungsdatenbanken mit der dazu nötigen Infrastruktur. Es können beispielsweise unterschiedliche Datentypen zu einem Patienten (z.B. Bilder, genetische Daten etc.) in unterschiedlichen Datenbanken abgelegt sein, auf die über das Forschungsmodul zugegriffen werden kann.

5.3.1 Zweck und Anwendungsbereich

Das Forschungsmodul dient dazu, medizinische Daten hoher Qualität langfristig – auch für zukünftige Forschungsprojekte – zur Verfügung zu stellen. Daraus ergibt sich, dass der Verwendungszweck sowie die Lebensdauer der Daten weniger konkret angegeben werden können, als dies für das Studienmodul, wie es in Kapitel 5.2 beschrieben ist, gilt. Die Einsatzmöglichkeiten eines Forschungsmoduls sind sehr weit gefasst. Dies können gesundheitsökonomische oder epidemiologische Studien sein, aber auch die Ermittlung von Fallzahlen bzw. von Patienten für klinische Studien kann ermöglicht werden. Im Gegensatz zum Klinischen Modul ist ein unmittelbarer Behandlungsbezug der gespeicherten Daten nicht notwendigerweise gegeben. Mit Hilfe eines Forschungsmoduls können große Kollektive abgebildet werden, die über einen längeren Zeitraum beobachtet werden, ohne dass die Vertraulichkeit der Information angetastet wird. Eine direkte Verknüpfung der Identitätsdaten mit den medizinischen Daten einer Forschungsdatenbank ist generell ausgeschlossen, da kein zur unmittelbaren Identifikation eines Patienten führendes Merkmal – wie z.B. der PID des Klinischen Moduls – als Ordnungskriterium in einer Forschungsdatenbank geführt wird. Das Forschungsmodul kann medizinische Daten zu einem Patienten aus mehreren Studien oder Systemen verwalten und bietet Forschern somit einen Datenpool, der sich zur Generierung neuer Fragestellungen oder für Sekundärauswertungen eignet.

Die medizinischen Daten des Forschungsmoduls können potenziell nicht nur den Forschern, die direkt an einer Studie beteiligt sind, zur Verfügung gestellt werden, sondern auch anderen Forschern eines Forschungsverbundes, externen Forschern oder auch der Industrie.

Je nach Aufbau des Forschungsmoduls bzw. abhängig von den Regularien eines Forschungsverbundes wird den Forschern ein direkter Zugang auf die Daten in den Datenbanken gewährt oder ein Export der Daten übermittelt. Bei einem direkten Zugriff auf die Forschungsdatenbanken können für die Sekundär-

nutzung von Daten aus der klinischen Forschung komfortable Such-, Filter- und Selektionsmechanismen zur Verfügung gestellt werden.

5.3.2 Anwendungsfälle

5.3.2.1 Probanden in das Forschungsmodul aufnehmen

Anders als bei der Aufnahme in andere Module eines Forschungsverbunds wird die Aufnahme in das Forschungsmodul im Regelfall nicht interaktiv und im Kontakt zum betroffenen Probanden oder Patienten stattfinden. Allerdings setzt auch die Übermittlung eines personenbezogenen Datensatzes in das Forschungsmodul eine informierte Einwilligung des Betroffenen (vgl. Kap. 3.2.3.1) voraus. Daher ist das Vorliegen einer ausreichenden Einwilligung, die zudem die typischerweise mit der Übermittlung in das Forschungsmodul einhergehende Zweckänderung und Langfristigkeit der Speicherung abdeckt, vor der Übermittlung zu prüfen.

5.3.2.2 Datenqualität sichern

Wird das Forschungsmodul mit anderen Modulen (z.B. dem Studienmodul oder Klinischen Modul) gekoppelt, so können schon vorhandene Daten eines Patienten aus dem Forschungsmodul zum Zwecke der Qualitätssicherung genutzt werden. Eine genaue Beschreibung befindet sich im Kapitel 6.3 zum kombinierten Einsatz von Studien- und Forschungsmodul.

5.3.2.3 Daten mit externen Quellen abgleichen

Im Zuge eines Forschungsvorhabens können neben dem Datenbestand der Forschungsdatenbank auch Informationen aus externen Datenquellen z.B. dem Melderegister oder Daten der Gesundheitsämter herangezogen werden. Dies können beispielsweise Anfragen an die Einwohnermeldeämter sein, ob die in einem Forschungsvorhaben betrachteten Personen noch leben. Bei einem Datenabgleich sind die datenschutzrechtlichen Bestimmungen der datenliefernden Stelle zu berücksichtigen. Zusätzlich muss der Datenabgleich durch das Forschungsvorhaben gut begründet sein. Gegebenenfalls muss entschieden werden, ob das Interesse der Allgemeinheit an diesem Forschungsvorhaben das Recht der einzelnen Person auf informationelle Selbstbestimmung überwiegt. Auf die rechtlichen Rahmenbedingungen zum Abgleich mit externen Datenbeständen wird im Kapitel 4.3.4 genauer eingegangen.

5.3.2.4 Machbarkeit einer Studie prüfen

Um die Machbarkeit einer Studie prüfen zu können, müssen Indizien dazu ausgewertet werden, wie viele den spezifizierten Ein- und Ausschlusskriterien entsprechende Patienten innerhalb einer bestimmten Zeitspanne zu erwarten sind. Die Information, ob die Patienten eingewilligt haben, über weitere Stu-

dien informiert zu werden, kann bei der Machbarkeitsprüfung einer Studie ggf. mit berücksichtigt werden.

Die Machbarkeitsprüfung einer Studie auf Grundlage der Daten des Forschungsmoduls, kann durch drei unterschiedliche Verfahren realisiert werden:

- Der Forscher erhält direkten Zugriff auf die Forschungsdatenbank und kann durch Abfragen der Ein- und Ausschlusskriterien entsprechend aggregierte Informationen über das zu erwartende Patientenkollektiv bekommen.
- Der Forscher erhält einen Export und verfährt dann wie bei (1).
- Der Betreiber bzw. Verantwortliche der Forschungsdatenbank erhält bestimmte Anfragen eines Forschers (z.B. die Ein- und Ausschlusskriterien einer Studie) und liefert dem Forscher als Ergebnis eine Anzahl geeigneter Patienten zurück.

Bei diesen Abfragen müssen geeignete Mechanismen verhindern, dass einzelne Patienten durch gezieltes Abfragen identifiziert werden können. Z.B. kann bei Abfragen, die eine bestimmte Anzahl von Patienten unterschreiten, nicht mehr die genaue Patientenanzahl ausgegeben werden, sondern nur noch der Hinweis, dass das Mindestmaß an Patienten unterschritten ist. Bei einer Datenbereitstellung als Export müssen geeignete Maßnahmen zur Anonymisierung der Rohdaten getroffen werden (vgl. Kap. 5.3.2.9).

5.3.2.5 Rekrutierung unterstützen

Patienten, die bereits an einem früheren Forschungsprojekt teilgenommen haben, können mit Hilfe des Forschungsmoduls auch effektiv für weitere Studien rekrutiert werden. Dies kann insbesondere bei chronischen Erkrankungen von Interesse sein. Anders als bei der Überprüfung der Machbarkeit wird hierfür eine Depseudonymisierung der Datensätze ausgelöst werden müssen, die den gesuchten Ein- und Ausschlusskriterien entsprechen. Das Verfahren der Depseudonymisierung wird im Kapitel 6.1 zum Identitätsmanagement genauer beschrieben. Idealerweise sollten die hinterlegten Einwilligungserklärungen der ausgewählten Patienten eine direkte Ansprache aus dem Forschungsverbund heraus erlauben. Andernfalls könnte auch eine Ansprache über die aktuell behandelnde Einrichtung geregelt sein.

5.3.2.6 Auskunft geben

Wünscht ein Patient Auskunft über die in dem Forschungsmodul über ihn gespeicherten Daten, wird die Auskunftserteilung in geeigneter Form geprüft und über das Identitätsmanagement an das Forschungsmodul weitergeleitet. Im Forschungsmodul werden die medizinischen Daten des Patienten ggf. aus mehreren Datenbanken selektiert und an das Identitätsmanagement zurückgeschickt. Bei diesem Vorgang muss durch geeignete Mechanismen verhindert werden, dass das im Forschungsmodul verwendete Pseudonym (PSN) des Pa-

tienten Unbefugten offenbart wird (s. hierzu Kap. 6.1 Identitätsmanagement und Kap. 6.4 Studienmodul und Forschungsmodul).

5.3.2.7 Daten auswerten

Die Daten des Forschungsmoduls können, je nach Aufbau der Infrastruktur und der organisatorischen Regelungen, sowohl im Sinne einer Erstauswertung (z.B. bei epidemiologischen Registern) als auch im Rahmen einer Sekundärauswertung (z.B. für eine retrospektive Studie) genutzt werden. Die Zugriffe auf die Daten können online oder auch in Form eines Exports erfolgen.

5.3.2.8 Daten an Forscher weitergeben (auf Basis einer Einwilligung)

Bei Vorliegen einer entsprechenden Einwilligung kann einem Forscher nach Antrag und entsprechender Bewilligung ein direkter Zugriff auf einen bestimmten Ausschnitt (z.B. eine Studie) des Forschungsmoduls gewährt werden. Alternativ werden die entsprechenden Daten als Export bereitgestellt. Die Einwilligung für die Weitergabe für ein bestimmtes Forschungsprojekt kann zum Zeitpunkt der Datenerhebung durch eine den Zweck des Forschungsprojekts mit umfassende Formulierung erfolgt sein, ggf. auch im Rahmen einer abgestuften Einwilligung (vgl. Kap. 4.2.2). Alternativ kann in bestimmten Fällen auch die spätere Einholung einer separaten Einwilligung für ein konkretes Forschungsprojekt möglich und nötig sein.

Bei einem direkten Zugriff auf die Datenbank muss sichergestellt sein, dass die Summe der zu einem Patienten verfügbar gemachten medizinischen Daten (ggf. aus mehreren Datenbanken zusammengeführt) nicht zu einem relevanten Reidentifizierungsrisiko führt. Zudem sollte das als dauerhaftes Ordnungskriterium in der Datenbank genutzte Pseudonym den zugreifenden Forschern verborgen bleiben.

Wenn Daten des Forschungsmoduls in Form eines Exports für weitere Auswertungen benötigt werden, muss der hierfür zuständige Wissenschaftler einen entsprechenden Antrag auf einen Datenexport stellen. Hierfür ist zu spezifizieren, welche Daten benötigt werden und ob im Rahmen der Auswertung möglicherweise mit relevanten Ergebnissen für einzelne Patienten zu rechnen ist und eine solche Rückmeldung im Vorfeld vereinbart wurde. Wenn keine relevante individuelle Rückmeldung der Ergebnisse an die Patienten zu erwarten ist, werden die Daten für den Export anonymisiert, andernfalls werden die Daten mit einem neuen Pseudonym versehen und exportiert. Wenn Daten aus mehreren Forschungsdatenbanken innerhalb des Forschungsmoduls für eine Auswertung zusammengeführt werden, muss sichergestellt sein, dass dadurch keine Reidentifizierung des Patienten ermöglicht wird. Sowohl bei anonymisierten wie auch pseudonymisierten Exporten ist darauf zu achten, dass sich die Sortierreihenfolge der exportierten Datensätze nicht nach dem langfristigen Pseudonym PSN im Forschungsmodul

richtet, sondern z.B. nach den neu erzeugten anonymen oder pseudonymen IDs.

5.3.2.9 Daten an Forscher weitergeben (unabhängig von einer Einwilligung)

Externen Forschern, für deren Zugriff keine Einwilligung der Probanden vorliegt, können Daten in Form eines Online-Zugriffes sowie als Export zur Verfügung gestellt werden. Das Vorgehen bei den Zugriffen auf die Forschungsdaten für externe Forscher ist angelehnt an die Regelungen der Forschungsdatenzentren der statistischen Ämter des Bundes und der Länder[22]. Daraus ergibt sich, dass für externe Forscher der Zugriff auf die Daten des Forschungsmoduls in der Regel faktisch anonymisiert erfolgen kann.

Bei einem Online-Zugriff werden zwei Möglichkeiten vorgeschlagen, die beide ein möglichst geringes Reidentifizierungsrisiko für die Patienten mit sich bringen:

- Den Forschern werden spezielle PC-Arbeitsplätze bereitgestellt an denen sie arbeiten können. Bei diesen Arbeitsplätzen gibt es eine spezielle Regulierung des Datenzugangs, die die Reidentifizierung des Patienten verhindert. Durch diese Mechanismen können den externen Forschern die Daten faktisch anonymisiert zur Verfügung gestellt werden.
- Die Forscher bekommen Zugriff auf Dummy-Daten, die in Aufbau und Merkmalsausprägungen dem Originalmaterial gleichen. Mit Hilfe dieser Dummy-Dateien können die Forscher, entsprechend ihrer Fragestellung, spezielle Abfragen erstellen. Diese Abfragen werden anschließend von den Verantwortlichen für die Forschungsdatenbank (z.B. Biometrie-Einheit) auf den Originaldaten angewendet. Die Forscher erhalten nach einer notwendigen Geheimhaltungsprüfung schließlich die Ergebnisse dieser Auswertung. Dieses Vorgehen ermöglicht die Arbeit mit absolut anonymisierten Daten.

Neben dem Online-Zugriff können externen Forschern auch absolute bzw. faktisch anonymisierte Exporte zur Verfügung gestellt werden. Bei den faktisch anonymisierten Exporten handelt es sich um sogenannte Scientific-Use-Files, die wissenschaftlichen Institutionen zur Verfügung gestellt werden. Vertragliche Vereinbarungen zur Nutzung und Weitergabe der Daten können ein evtl. noch vorhandenes Reidentifizierungsrisiko begrenzen. Für die Bereitstellung von Daten für die breite Öffentlichkeit können absolut anonymisierte Exporte (Public-Use-Files) bereitgestellt werden, die nur ausgewählte oder vergröberte Merkmale enthalten. Um ein Reidentifizierungsrisiko für die einzelnen Patienten auszuschließen, sollte bei der Auswahl der Merkmale das Prinzip der *k*-Anonymität berücksichtigt werden, wobei die Größe von *k* geeignet zu wählen ist. Auch bei diesen Exporten ist auf eine Sortierung unab-

22 http://www.forschungsdatenzentrum.de/datenzugang.asp

hängig vom langfristig genutzten Pseudonym zu achten [34]. Weitere Hinweise und Hilfestellungen für die Bereitstellung anonymer Daten, gerade auch in internationalen Projekten, finden sich in [35].

5.3.2.10 Ergebnisse mitteilen

Im Falle, dass ein Patient über Forschungsergebnisse benachrichtigt werden soll, ist dieser Vorgang in jedem Einzelfall von Antrag und Bewilligung durch den Ausschuss Datenschutz des Forschungsverbundes abhängig. Das Verfahren ist so einzurichten, dass es erst nach aktueller Prüfung der Genehmigung durch den Verantwortlichen manuell gestartet werden kann. In diesen Fällen geht der Vorgang von der Forschungsdatenbank aus. Die Identifizierung und Benachrichtigung des Patienten über das Identitätsmanagement erfolgt analog zu dem Verfahren, wie es beim Erteilen der Auskunft vorgesehen ist (s.a. Kap. 6.1.2 zur Mitteilung von Ergebnissen).

5.3.3 Daten und Datenflüsse

Die Forschungsdatenbanken des Forschungsmoduls enthalten ausschließlich medizinische Daten, die mit einem Pseudonym (PSN) versehen sind, das außerhalb des Forschungsmoduls nicht offenbart werden darf. Neben den Administratoren können zusätzlich speziell autorisierte Services, die mit dem Identitätsmanagement kommunizieren, auf die Forschungsdatenbanken des Forschungsmoduls zugreifen (s.a. Kap. 6.1.6.2).

Aus den oben genannten Anwendungsfällen lassen sich folgende Datenflüsse in Bezug auf die Forschungsdatenbanken des Forschungsmoduls ableiten:

5.3.3.1 Transfer medizinischer Daten in eine Forschungsdatenbank

Bevor medizinische Daten eines Patienten in eine Forschungsdatenbank eines Forschungsverbundes transferiert und dort gespeichert werden können, ist sicherzustellen, dass diese mit einem Pseudonym (PSN) versehen werden, das an keiner Stelle zusammen mit identifizierenden Daten des Patienten gespeichert werden darf. Somit wird eine eindeutige Zuordnung der Daten zum richtigen Patienten vor der Pseudonymisierung vorausgesetzt. Dies ist eine Aufgabe des im Kapitel 6.1 beschriebenen Identitätsmanagements.

Das Pseudonym wird von einer für das Identitätsmanagement legitimierten Institution des Forschungsverbundes erzeugt und zusammen mit den medizinischen Daten an eine Forschungsdatenbank weitergeleitet. Dort dient das PSN als Zuordnungskriterium für die Speicherung und die Zusammenführung der Daten und für alle fallbezogenen Auswertungen, die daraus abgeleitet werden. Die Kennungen der medizinischen Einrichtungen oder der individuellen Ärzte – so genannte organisatorische Daten (OrgDAT), wie sie im Kapitel zum Maximalmodell (s. Kap. 6.5) beschrieben sind – können in den For-

schungsdaten im Klartext oder ebenfalls pseudonymisiert gespeichert werden. Bei einer Speicherung solcher Daten im Klartext muss gewährleistet sein, dass hierdurch kein relevantes Reidentifizierungsrisiko für Patienten entsteht. Des Weiteren muss bei der Zusammenführung der medizinischen Daten eines Patienten aus verschiedenen Quellen in einer Datenbank (z.B. unterschiedlichen Studien) sichergestellt werden, dass durch diese Zusammenführung das Reidentifizierungsrisiko nicht zu groß wird.

Die medizinischen Daten können sowohl aus der direkten Versorgung (Klinisches Modul, Kap. 5.1), aus klinischen Studien (Studienmodul, Kap. 5.2) oder aus anderen Datenbanken (z.B. Registern) des Forschungsverbundes stammen oder auch direkt für das Forschungsmodul erfasst worden sein, wie z.B. Daten von Kontrollpersonen bei epidemiologischen Kohortenstudien. Sollten schon Daten zu einem PSN vorhanden sein, können diese zusammengeführt werden. Die Übertragung von Daten aus einer Studiendatenbank in eine Forschungsdatenbank wird im Kapitel 6.4 (Studien- und Forschungsmodul) detailliert beschrieben.

5.3.3.2 Ändern medizinischer Daten in einer Forschungsdatenbank

Es kann die Notwendigkeit bestehen, medizinische Daten, die sich schon in einer Forschungsdatenbank befinden, zu ändern. Dies kann z.B. im Rahmen einer Qualitätssicherung notwendig sein, wie sie im Kapitel 6.4 (Studien und Forschungsmodul) beschrieben wird. Es können aber auch bei der sekundären Auswertung Fehler entdeckt werden, die dann ebenfalls im Datenbestand des Forschungsmoduls geändert werden sollten. Für die Änderungen eines Datensatzes wird dieser anhand seines PSN selektiert und geändert bzw. überschrieben. Aus Sicht des Datenschutzes kann es dem Betreiber der Forschungsdatenbank überlassen werden, ob er die Änderung in Form einer Versionierung oder mit Hilfe eines Audit-Trails nachvollziehbar macht. Im Sinne einer hohen Datenqualität sind aber Funktionen, die eine Nachvollziehbarkeit aller Änderungen gewährleisten, auf jeden Fall zu empfehlen.

5.3.3.3 Anonymisieren bzw. Löschen medizinischer Daten in der Forschungsdatenbank

Ein Patient hat jederzeit das Recht, seine Einwilligungserklärung für die Speicherung medizinischer Daten im Rahmen eines Forschungsvorhabens zurückzuziehen. Des Weiteren dürfen medizinische Daten je nach Forschungsvorhaben nur für eine bestimmte Dauer in pseudonymisierter Form gespeichert werden; dies ist im Regelwerk des Forschungsverbunds zu definieren und muss durch die jeweilige Einwilligungserklärung abgedeckt sein. Ein weiterer Grund für die Anonymisierung bzw. Löschung der Daten eines Patienten ist dessen Versterben.

In diesen Fällen bedeutet dies für den Betreiber einer Forschungsdatenbank, dass er die medizinischen Daten eines Patienten anonymisieren oder löschen

können muss. Bei der Anonymisierung müssen die ggf. extern, z.B. in einer Patientenliste, gespeicherten identifizierenden Daten (IDAT) gelöscht und das Pseudonym als Ordnungskriterium in der Forschungsdatenbank durch eine anonyme Kennung ersetzt werden (s. Anwendungsfall Widerruf in Kap. 6.1.2). Bei der Erzeugung anonymer Kennungen ist zu beachten, dass diese nicht mit schon bestehenden anonymen oder pseudonymen Kennungen in der Forschungsdatenbank übereinstimmen dürfen. Das Löschen der Daten aus einer Forschungsdatenbank erfordert ebenso wie das Anonymisieren auch ein Löschen der ggf. extern gespeicherten IDAT. Die Anonymisierung kann im Einzelfall und nach Abschätzung des Reidentifizierungsrisikos auch erfordern, dass einzelne charakteristische Merkmale des Falls gelöscht oder vergröbert werden. Genauere Details, wie dies im Zusammenhang mit einem Identitätsmanagement erfolgen kann, sind im Kapitel 6.4 (Studien- und Forschungsmodul) beschrieben.

5.3.3.4 Austausch der Pseudonyme einer Forschungsdatenbank

Der Austausch der Pseudonyme einer Forschungsdatenbank kann aus unterschiedlichen Gründen notwendig werden: Z.B. bei Verlust oder Kompromittierung einer zur Pseudonymisierung genutzten SmartCard oder bei drohender Kompromittierung des verwendeten Verschlüsselungsalgorithmus. Liegt die Notwendigkeit eines Austausches der Pseudonyme vor, so muss dieser durch das Identitätsmanagement durchgeführt werden. Hierbei muss durch geeignete Verfahren sichergestellt werden, dass die neuen Pseudonyme dem richtigen Patienten bzw. Datensatz zugewiesen werden (Kap. 6.1.2 Umpseudonymisierung).

5.3.4 Nutzer, Rollen und Rechte

Der Zugriff auf die Forschungsdatenbank kann durch den Administrator sowie durch einen autorisierten internen bzw. externen Forscher erfolgen.

Der Administrator hat vollen Zugriff auf die Datenbank und kann entsprechende Selektionen und Exporte veranlassen.

Der interne Forscher kann seinem Antrag entsprechend bestimmte Teile der Forschungsdatenbank einsehen. Auch hier ist bei einem studienübergreifenden Zugang wieder das Reidentifizierungsrisiko der einzelnen Patienten abzuschätzen. Während der Administrator die PSN in der Forschungsdatenbank sehen darf, bleiben diese dem Forscher verborgen.

Der externe Forscher hat in der Regel nur anonymisierten Zugriff auf die Daten. Dieser kann sowohl online als auch in Form eines Exportes erfolgen.

Hat ein behandelnder Arzt auch in der Rolle eines Forschers Zugriff auf Daten eines seiner Patienten, so sollte sichergestellt werden, dass er diesem keine weiteren medizinischen Daten zuordnen kann, die ihm im Rahmen der Behandlung verborgen geblieben wären (z.B. genetische Informationen, s.a. Kap. 6.2.3.3).

5.3.5 Verantwortlichkeiten

Da ein Forschungsmodul der Bereitstellung von Daten für die Forschung über einen langen Zeitraum dient, muss auch die Verantwortlichkeit für die Datenverarbeitung langfristig geregelt und für die Patienten transparent dargestellt werden. Hierfür ist auch die Auswahl oder ggf. Etablierung einer rechtsfähigen Einrichtung bzw. eines Forschungsverbunds als juristischer Person notwendig. Der Zugriff auf die Daten der Forschungsdatenbank muss über den von der verantwortlichen Stelle eingerichteten Ausschuss Datenschutz bewilligt werden. Forscher erhalten ein Zugriffsrecht auf die Daten, wenn dies vom Ausschuss Datenschutz nach Prüfung des Forschungsansatzes und des dafür benötigten Datensatzes bewilligt wird.

Der Betrieb und die Administration des Forschungsmoduls sollten möglichst räumlich und organisatorisch getrennt von anderen Modulen, wie z.B. dem Identitätsmanagement, erfolgen. Für die Erstellung und Einhaltung der Regeln bezüglich des Umganges mit den Forschungsdaten bzw. der Kontaktierung des Patienten ist das Management des Forschungsverbundes zuständig bzw. ein vom Management beauftragter Dienstleister.

5.3.6 Aspekte der Realisierung

Im Gegensatz zu den Studiendatenbanken, die sich in den letzten Jahren immer mehr als „Standardprodukte" etabliert haben, gibt es relativ wenige IT-Lösungen für die Anforderungen einer Forschungsdatenbank. Mit dem Pseudonymisierungsdienst der TMF sind zwar schon die Anforderungen für das Identitätsmanagement (Pseudonymisierung, Depseudonymisierung, Findingmanagement etc.) abgedeckt, jedoch fehlt es noch an nationalen IT-Lösungen für die Umsetzung der oben beschriebenen Anwendungsfälle. Der Pseudonymisierungsdienst der TMF könnte auch eingesetzt werden, um Exporte aus einer Forschungsdatenbank mit projektindividuellen, bei Bedarf reidentifizierbaren Pseudonymen zu versehen (vgl. Kap. 6.1.1.2).

Als internationale Lösung wäre das Projekt I2B2 (Informatics for Integrating Biology and the Bedside) zu nennen [36]. I2B2 ist ein von der NIH gefördertes Projekt in den USA, welches u.a. ein Open Source Tool entwickelt, mit dem die Zusammenführung klinischer Datenbestände und die Abfrage medizinischer Datenbestände ermöglicht werden. Somit können u.a. Machbarkeitsanalysen für neue Studien realisiert werden.

Auch wenn das I2B2-Tool eine gute Grundlage für eine Forschungsdatenbank darstellt, sind noch einige Anpassungen bezüglich des Datenschutzes sowie einige Verbesserungen bezüglich der Funktionalität zu realisieren. Ein Punkt ist der Ausbau des Rechte- und Rollenmanagements (alle Nutzer können momentan den gesamten Datenbestand einsehen). Als weiterer Punkt ist der Im- und Export der Daten zu nennen. Hier bedarf es ebenfalls einiger Erwei-

terungen, da momentan noch keine Schnittstellen für gängige Datenstandards wie CDISC, HL7 etc. vorhanden sind. Im Rahmen eines TMF-Projekts[23] wurde 2012 jedoch ein Toolkit auf Basis der I2B2-Plattform und mit Hilfe einer frei verfügbaren Version der Software Talend Open Studio[24] erstellt, welches standardisierte Importe für eine Reihe von Formaten ermöglicht.

Für die Bereitstellung anonymer Exporte aus Forschungsdatenbanken stellt die TMF kostenfrei eine Softwarekomponente zur Verfügung, die vorhandene Daten in verschiedenen Formaten nach umfangreicher Parametrierung unter möglichst geringem Informationsverlust zuverlässig k-anonymisiert.[25]

5.4 Biobankenmodul

Für Biobanken (oder Biomaterialbanken) hat die TMF bereits die bisherigen generischen Datenschutzkonzepte aus dem Jahre 2003 erweitert und 2006 ein angepasstes und mit den Datenschützern auf nationaler Ebene abgestimmtes Datenschutzkonzept vorgestellt [2]. Dieses bleibt weiterhin gültig und ist nicht Gegenstand dieser Revision. Es ist dann einschlägig, wenn der Biobank-Betrieb der eigentliche Gegenstand eines Datenschutzkonzepts ist; seine Einordnung in die neue umfassende Struktur wird in Kapitel 6.1.7 beschrieben.

In diesem Kapitel werden die dortigen Ausführungen soweit wiederholt, wie es nötig ist, um die Einpassung von Biobanken in das modulare Konzept für medizinische Forschungsverbünde beschreiben zu können. Die Abgrenzung eines Biobankenmoduls von weiteren im Forschungsverbund existierenden Modulen spiegelt einerseits die technisch und organisatorisch unterschiedliche Handhabung von Biomaterialien wider, andererseits die besondere Sensibilität von genetischen Daten, die aus der Analyse der Materialien entstehen und in der Regel von anderen Daten getrennt gespeichert werden sollten.

5.4.1 Zweck und Anwendungsbereich

Ein Biobankenmodul enthält eine oder mehrere Probenbanken zusammen mit organisatorischen oder administrativen Daten (OrgDAT) zu den Proben oder Biomaterialien, die in einer direkt bei der Probenbank angesiedelten Datenbank verwaltet werden. Auch eine Datenbank für die aus den Proben gewonnenen Analysedaten (AnaDAT, im BMB-Konzept etwas missverständlich als ProbDAT bezeichnet) gehört in der Regel in das Biobankenmodul. Zu einer Biobank gehören immer auch Komponenten zum Identitätsmanagement (s. Kap. 6.1), die mehr oder weniger zentral betrieben werden, und eine Daten-

23 siehe www.tmf-ev.de/idrt
24 siehe www.talend.com
25 siehe www.tmf-ev.de/produkte/P100201

bank mit klinischen Annotationen, die im modularen Aufbau eines Verbunds im Forschungsmodul (s. Kap. 5.3) oder Klinischen Modul (s. Kap. 5.1) angesiedelt, also vom Typ her eine Klinische Datenbank (KDB) oder Forschungsdatenbank (FDB) ist; sie wird im Kontext dieses Kapitels als Annotationsdatenbank bezeichnet.

Aufgabe der Probenbank ist die Aufbewahrung von Proben. In der Regel ist sie an einem Labor oder einem biomedizinischen Institut angesiedelt. Die Probenbank erhält die Probe direkt von der Daten erhebenden Stelle bzw. von einem weiteren Labor, in dem gegebenenfalls die Probenaufarbeitung oder eine Aliquotierung in Unterproben erfolgt. Die Probe wird in der Probenbank eingelagert; entsprechende organisatorische Daten (OrgDAT, z.B. Probennummer, Probenaufenthalt, Probencharakterisierungen) werden dokumentiert. Ist die Probenbank an ein geeignet ausgestattetes Institut angeschlossen, so können in der Probenbank auch direkt Analysen der Probe vorgenommen werden. Je nach Organisationsform des Forschungsverbunds geschieht dies im Zuge der Behandlung des Patienten, für ein konkretes Forschungsprojekt oder allgemein für Forschungszwecke. Analysen können auch durch andere Einrichtungen durchgeführt werden, wozu die Probe entsprechend zugeliefert werden muss, in der Regel nur von einem minimalen Satz organisatorischer Daten begleitet.

Zweck des Biobankenmoduls ist die medizinische Forschung mit Proben, Analyseergebnissen und Annotationsdaten. Dazu tritt in der Regel ein Forschungsprojekt mit einer bestimmten Anforderung (Spezifikation der Erkrankung, Randparameter wie Alter und Komorbiditäten, genetische Parameter, Anforderungen an die Probe bzw. deren Analyse) an den Forschungsverbund heran und erhält im Gegenzug Daten, eventuell auch Proben, die gemäß den Richtlinien des Forschungsverbundes bereitgestellt werden.

Biomaterialien werden oft auch im Rahmen einer klinischen Studie gesammelt. Solange sie an die Zweckbestimmung der Studie gebunden bleiben und überschüssige Reste spätestens bei Beendigung der Studie vernichtet werden, gelten hierfür die Regeln der Studie, die allgemein im AMG und den GCP-Richtlinien, im Speziellen in der Einwilligungserklärung festgeschrieben sind (vgl. Kap. 5.2, Studienmodul). Die Proben können im Rahmen der Studie direkt den Daten zugeordnet werden, so dass keine weiteren Anforderungen an das Identitätsmanagement (Kap. 6.1) entstehen. Sollen Proben über das Studienende hinaus langfristig aufbewahrt werden, so sind sie spätestens dann in ein eigenständiges Biobankenmodul zu überführen und unterliegen von da an den in diesem Kapitel beschriebenen Regeln. All dies kann natürlich nur auf der Grundlage einer ausreichenden Einwilligung geschehen. Gleiches gilt, wenn die Proben zwar für die Studie erhoben, aber direkt in einer Biobank aufbewahrt werden sollen; die Studie kann für ihre Zwecke wie jedes andere Forschungsprojekt Analysen und Auswertungen anfordern (s. o.). Auch die aus der Studie entstandenen Annotationsdaten sind spätestens bei Studienende in eine geeignete Annotationsdatenbank zu überführen.

5.4.2 Anwendungsfälle

Da die relevanten Anwendungsfälle bereits in dem generischen Datenschutzkonzept für Biobanken aus dem Jahr 2006 [2] beschrieben wurden, wenn auch anders strukturiert als für die anderen hier beschriebenen Module, wird an dieser Stelle auf eine wiederholende Beschreibung verzichtet. Tabelle 1 bietet eine Übersicht über die relevanten Anwendungsfälle, die der Strukturierungsvorgabe für Anwendungsfälle aus diesem Leitfaden folgt. Zu jedem Anwendungsfall sind die Verweise zu den entsprechenden Kapiteln des bereits veröffentlichten Konzepts für Biobanken aufgeführt. Ergänzend sind Verweise zu relevanten analogen Anwendungsfällen oder übergreifenden Kapiteln aus diesem Konzept aufgeführt.

Tab. 1 Anwendungsfälle im Biobankenmodul

Anwendungsfall	Relevante Kapitel im generischen Datenschutzkonzept für Biobanken	Vergleichbare Kapitel in diesem Leitfaden
Probenspender in eine Biobank aufnehmen	Kap. 4.2.2: Gewinnung und Anmeldung einer Probe *siehe auch:* Kap. 4.4.5: Probenmanagement	Kap. 5.1.2.1 Kap. 5.2.2.1
Daten auswerten	Kap. 1.1.2: Kennzeichnungen und Datentypen Kap. 4.4.5: Probenmanagement	
Ergebnisse mitteilen	Kap. 3.4: Wissen/Nichtwissen, Mitteilungspflichten	Kap. 5.3.2.8
Auskunft geben	Kap. 4.4.6: Auskunft an den Probanden	Kap. 5.3.2.6
Daten an Forscher weitergeben	Kap. 4.2.3: Erzeugung und Verschlüsselung der LabID Kap. 4.4.4: Bereitstellung von Daten *siehe auch:* Kap. 4.1.1: Aufgabe des Datenschutzkonzepts Kap. 4.4.5: Probenmanagement Kap. 3.3.3: Einwilligungserklärung – Weitergabe an Dritte	
Machbarkeit einer Studie prüfen	*nicht behandelt*	Kap. 5.1.2.9 Kap. 5.3.2.4
Rekrutierung unterstützen	Kap. 4.4.3: Pseudonymisierungsdienst *(für den Aspekt der Depseudonymisierung)* Kap. 3.8: Zusatzerhebung *(für den Aspekt der erneuten Kontaktierung)*	Kap. 5.1.2.10 Kap. 5.3.2.5
Proben und Daten sperren, anonymisieren, löschen oder vernichten	Kap. 3.7: Widerruf und Löschung Kap. 4.2.7: Widerruf einer Einwilligung Kap. 4.2.6: Anonymisierung Kap. 3.3.2: Nutzungsdauer, Sterbefall *(für die Aspekte der Aufklärung und Einwilligung)*	Kap. 5.2.2.11 Kap. 5.1.2.8 Kap. 5.2.2.11

5.4.3 Daten und Datenflüsse

Personendaten oder identifizierende Stammdaten (IDAT), Pseudonyme (PID und PSN) sowie medizinische Daten (als Annotationsdaten) kommen im Biobankenmodul in der gleichen Bedeutung wie in den anderen Modulen vor (s. Kap. 4.2 zum allgemeinen Datenmanagement in [2]). Daneben gibt es auch noch die folgenden Biobank-spezifischen Daten:

Probennummer (LabID): LabID bezeichnet die ursprüngliche Nummer der Probe, die entweder von der Proben gewinnenden Stelle oder von der Probenbank vergeben wird, in der Regel auch als Barcode-Aufkleber (Details in Kap. 4.2 zum allgemeinen Datenmanagement in [2]). Die LabID wird entweder durch die Proben gewinnende Stelle oder durch das verarbeitende bzw. analysierende Labor an die Annotationsdatenbank (vom Typ KDB oder FDB) gemeldet. Dort wird evtl. statt der LabID eine kryptographisch transformierte $LabID_{tr}$ gespeichert, um eine direkte Zuordnung von Datensatz und Probe zu vermeiden (s. Kap. 4.2.3 zur Erzeugung und Verschlüsselung der LabID in [2]). Diese Transformation ist logisch eine Funktion des Identitätsmanagements; wo sie tatsächlich durchgeführt wird, hängt von den konkreten Gegebenheiten des Forschungsverbunds ab (s. Kap. 4.2.3 in [2] und Kap. 6.1.3.1 in diesem Leitfaden). Dabei spielen auch Überlegungen zur Verhältnismäßigkeit eine Rolle (s. Kap. 4.6 in [2] und Kap. 6.7 in diesem Leitfaden).

Organisatorische Daten (OrgDAT): OrgDAT sind Begleitdaten einer Probe, die an unterschiedlichen Stellen entstehen und verwendet werden. So erfasst z.B. die Proben gewinnende Stelle die Probenart und gegebenenfalls die Informationen zu Probenentnahme und Präanalytik. In der Probenbank werden die Begleitdaten einer Probe mit weiteren Informationen wie z.B. den Umständen von Konservierung, Lagerung und Qualität gespeichert. OrgDAT zu einer Probe werden an verschiedenen Stellen benötigt und dann zur Unterscheidung durch unterschiedliche Indizes gekennzeichnet. Eine ausführliche Darstellung findet sich in den Kapiteln 1.1.2 (Kennzeichnungen und Datentypen) und 4.2.4 (Grundsätzliche Verteilung der Daten) in [2] sowie in Kapitel 6.5.2.4 in diesem Leitfaden.

Probenanalysedaten (AnaDAT oder ProbDAT): Die mit AnaDAT bezeichneten Ergebnisse der Probenanalyse werden in einer Analysendatenbank gespeichert, die im Biobankenmodul angesiedelt ist. Sie werden nach Bedarf für Anfragen verwendet oder an anfragende Forscher übermittelt (s. Kap. 1.1.2 in [2]). Die ihnen zu Grunde liegenden Analysen können sowohl von den der Probenbank angeschlossenen Laboren als auch von kooperierenden Einrichtungen durchgeführt werden. AnaDAT können potenziell rückbeziehbare Größen darstellen wie z.B. im Fall von Genotypen. Ihre Speicherung sollte daher separat von den Annotationsdaten und eventuellen anderen Datenbeständen des Forschungsverbundes im Biobankenmodul selbst erfolgen.

Insgesamt sind im Grundmodell eines Biobankenmoduls zumindest die folgenden Datenarten unter getrennter Verantwortung zu speichern:

- IDAT,
- MDAT,
- Probe (+ zugehörige OrgDAT) und AnaDAT.

Für die Zuordnung dieser getrennten Teildatenbestände werden die Kennungen

- PID,
- PSN,
- LabID,
- $LabID_{tr}$

als Pseudonyme verwendet, die jeweils nur unter genau definierten Bedingungen miteinander verknüpfbar sind, siehe auch Kapitel 6.1 (Identitätsmanagement) und Abbildung 7.

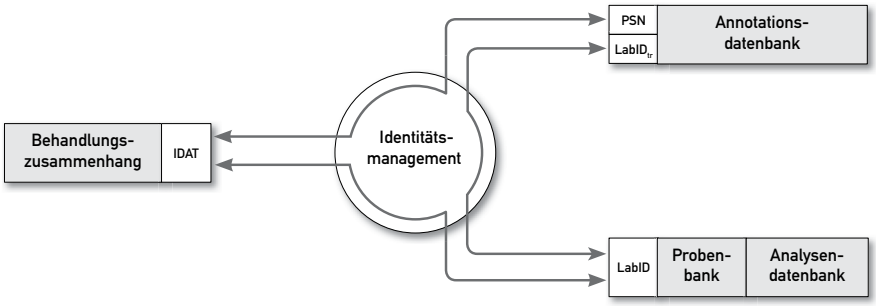

Abb. 7 In den Annotationsdaten einer Biobank sind die Verweise auf den Patienten und auf die zugehörigen Proben pseudonymisiert.

Für die Datenflüsse sei auf das Kapitel 4.2 zum allgemeinen Datenmanagement von [2] verwiesen.

5.4.4 Nutzer, Rollen und Rechte

Das Biobankenmodul betrachtet überwiegend die Rollen des Proben gewinnenden Arztes (dies können auch mehrere Ärzte für jeden einzelnen Spender sein) und des Wissenschaftlers, dazu verschiedene Systemadministratoren.

Probengewinnender Arzt: Übermittelt die Probe, ggf. über ein zwischengeschaltetes Labor, an die Probenbank und die Annotationsdaten an die Annotationsdatenbank. Weitere Zugriffe auf die Daten des Falls sind für den Proben gewinnenden Arzt im Rahmen des Biobankenmoduls nicht notwendig; ist das Biobankenmodul aber Teil eines Forschungsverbunds, der die Annotationsdaten in einer Klinischen, Studien- oder Forschungsdatenbank speichert, sind die dort (Kap. 5.1 bzw. 5.2 bzw. 5.3) vorgesehenen Zugriffsrechte zu gewähren.

Laborarzt: Analysiert eine Probe im Behandlungszusammenhang und übermittelt die Ergebnisse sowohl an die Analysendatenbank als auch an den Proben gewinnenden Arzt im Rahmen der Labordiagnostik des Behandlungsfalls oder der klinischen Studie.

Analysierender Wissenschaftler: Analysiert eine Probe außerhalb des Behandlungszusammenhangs für die Nutzung in der Biobank und übermittelt die Ergebnisse an die Analysendatenbank. Für den Patienten relevante Ergebnisse werden gemäß der Regularien der Biobank bzw. des Forschungsverbunds an den Proben gewinnenden Arzt übermittelt.

Auswertender Wissenschaftler: Tritt an die Biobank mit einem Projektvorschlag heran und erhält Daten, evtl. auch Proben, wie in Kapitel 5.4.1 beschrieben.

Systemverwalter: Wird für die Probensammlung, die OrgDAT-Datenbank, die Analysendatenbank, die Annotationsdatenbank wie in Kapitel 5.1.4.5 (Klinisches Modul – Administrator für eine Klinische Datenbank) bzw. Kapitel 5.3.4 (Forschungsdatenbank – Nutzer, Rollen und Rechte) und die Komponenten des Identitätsmanagements (wie in Kap. 6.1.4.1 und 6.1.4.2) benötigt. Er hat bei den jeweils anderen Datenbanken keinerlei Rechte.

Auditor: Überprüft den ordnungsgemäßen Ablauf aller Prozesse im Biobankenmodul. Ein Zugriff auf IDAT ist dazu nicht notwendig.

Doppelrolle Arzt/Forscher: siehe Kapitel 4.1.1 (Aufgabe des Datenschutzkonzepts – Doppelrolle Arzt/Forscher) von [2] und die analogen Ausführungen in Kapitel 5.3.4 (Forschungsdatenbank – Nutzer, Rollen und Rechte) und Kapitel 6.2.3.3 (Rechtemanagement – Mögliche Rollenkonflikte).

5.4.5 Verantwortlichkeiten

Die Verantwortlichkeiten im Biobankenmodul sind in den Kapiteln 4.3–4.5 (Realisierung – Organisation der Biomaterialbank, Dienste, Verträge und Regelungsbedarf) von [2] abgehandelt. Allgemeine Aussagen, die für alle Forschungsverbünde gelten, sind in Kapitel 6.6 (Organisatorische Regelungen) zusammengefasst.

5.4.6 Besondere Aspekte der Realisierung

Für verschiedene Organisationsmodelle eines Biobankenmoduls siehe die Kapitel 2.1 (Trägerschaft der Biomaterialbank) und 4.3 (Realisierung – Organisation der Biomaterialbank) von [2]; für Überlegungen zur Verhältnismäßigkeit siehe das dortige Kapitel 4.6 (Überlegungen zur Verhältnismäßigkeit) sowie Kapitel 6.7 (Kriterien der Verhältnismäßigkeit) unten.

Das Betreiben eines Biobankenmoduls erfordert besondere Erweiterungen der Aufklärung und Einwilligung; diese sind im Kapitel 3 von [2] zur Einwilligungserklärung beschrieben.

Im Zusammenhang mit klinischen Studien sind drei Szenarien zu unterscheiden, siehe Kapitel 5.4.1 oben:

1. Probenverwendung direkt und nur im Studienkontext: Hier sollte, soweit vorhanden, ein in die Studiensoftware integriertes Probenmanagement genutzt werden.
2. Probenverwaltung in einer auch unabhängig von der Studie existierenden Biobank: Hier ist die Studie als Forschungsprojekt zu betrachten, das die Dienste der Biobank nutzt.
3. Übergabe von überschüssigen Proben an eine Biobank nach Beendigung der Studie: Hier ist die Studie in der Rolle eines Probenzulieferers zu sehen.

In den Fällen 2 und 3 sind die Prozesse des Identitätsmanagements nach den Regeln der Biobank einzuhalten.

Die Handhabung von LabID und $LabID_{tr}$ ist im BMB-Konzept [2] auf spezielle Weise beschrieben; ist das Biobankenmodul in einen größeren Forschungsverbund eingegliedert, kann die Verwaltung dieser beiden Pseudonyme alternativ auch an geeigneten Stellen des zentralen ID-Managements angesiedelt sein.

Der Markt für Biobank-Software ist noch nicht konsolidiert; Biobank-Verwaltungsfunktionen sind z.T. auch in Labor-Software oder Studiensoftware integriert. Die TMF unterstützt mit ihren Arbeitsgruppen den Erfahrungsaustausch hierzu. Insbesondere in den Arbeitsgruppen IT-Infrastruktur und Qualitätsmanagement sowie Biomaterialbanken werden konkrete Fragen der Realisierung und nötiger Hardware- und Softwareausstattung umfangreich diskutiert. Den Kontakt zu den Arbeitsgruppen vermittelt die TMF-Geschäftsstelle.