Identitätsmanagement für Patienten in medizinischen Forschungsverbünden

Klaus Pommerening, Krister Helbing, Thomas Ganslandt, Johannes Drepper

Institut für Medizinische Biometrie, Epidemiologie und Informatik
Universitätsmedizin der Johannes-Gutenberg-Universität
55131 Mainz
pommeren@uni-mainz.de
khelbing@med.uni-goettingen.de
thomas.ganslandt@uk-erlangen.de
johannes.drepper@tmf-ev.de

Abstract: Die Integration von medizinischer Versorgung und Forschung ist eine zentrale Herausforderung des Gesundheitswesens. Die rechtlichen und ethischen Rahmenbedingungen erfordern dabei effektive Maßnahmen zum Datenschutz. Insbesondere soll außerhalb des direkten Behandlungskontextes die Identität eines Patienten nirgends erkennbar sein. Um das zu erreichen, benötigt man ein Identitätsmanagement für Patienten. Die hauptsächlichen Methoden hierzu sind Pseudonymisierung und eine darauf aufbauende informationelle Gewaltenteilung. Das Identitätsmanagement ist auch gekoppelt mit einem Kontakt- und Einwilligungsmanagement. Dieser Artikel beschreibt das generische TMF-Datenschutzkonzept für medizinische Forschungsverbünde und die zugehörigen Werkzeuge zum Identitätsmanagement sowie deren Weiterentwicklungsbedarf. Das Konzept und die Werkzeuge sind in verschiedenen Szenarien des verteilten Gesundheitswesens anwendbar.

1 Einleitung

Medizinische Forschungsverbünde, wie etwa die Kompetenznetze in der Medizin [KN], haben die Integration von qualitativ hochwertiger Versorgung und aktueller Forschung zum Ziel. Sie sind meist krankheitsspezifisch ausgerichtet, bieten eine verteilte Versorgung unter der Mitwirkung der führenden, oft auch internationalen, Experten des jeweiligen Fachs, und sie führen klinische, epidemiologische und translationale Forschungsprojekte durch. Dazu benötigen sie Daten und Biomaterialien, die hauptsächlich bei der Behandlung von Patienten gewonnen werden und oft über große Zeiträume, vielleicht sogar lebenslang, aufbewahrt werden müssen.

Dieses Zusammenspiel von Patientenversorgung und medizinischer Forschung effektiv und rechtlich einwandfrei zu gestalten, ist eine der zentralen Herausforderungen des Gesundheitswesens. Dazu benötigen Versorgung und Forschung eine gemeinsame Infrastruktur, die einen Daten-, Informations- und Materialfluss in beiden Richtungen unter-

stützt, aber dabei auch die vom Gesetzgeber errichteten Schranken zwischen Versorgungs- und Forschungskontext respektiert; insbesondere sind die hohen Anforderungen an den Schutz von persönlichen Patientendaten zu erfüllen. Dies ist in großen Forschungsverbünden eine komplexe Aufgabe und erfordert u. a. die Etablierung eines wirkungsvollen Identitätsmanagements.

Die TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. – ist eine Dachorganisation für die medizinischen Forschungsverbünde [TMF]. Ihre Aufgabe ist, Rahmenbedingungen und Infrastruktur der medizinischen Forschung zu verbessern. Sie unterstützt die Wissenschaftler dabei, gemeinsame Probleme rechtlicher, organisatorischer, methodischer und technischer Natur zu erkennen und zu lösen.

Insbesondere wurden in der TMF auf der Grundlage umfangreicher Rechtsgutachten und im Benehmen mit den Datenschutzbeauftragten Datenschutzkonzepte für eine Vielfalt von Szenarien in medizinischer Versorgung und Forschung entwickelt [Po08, Re06] und dazu technische Werkzeuge, die die Implementation dieser Konzepte in der Praxis unterstützen. Diese Bottom-Up-Entwicklung hatte zum Ziel, konkrete Netze zeitnah und direkt zu unterstützen, resultierte allerdings in einem gewissen Wildwuchs. Die mehrjährige Erfahrung hiermit motivierte eine größere Revision der Datenschutzkonzepte und einer Vereinheitlichung in Form eines modular aufgebauten gesamten „generischen" Datenschutzkonzepts für die medizinische Forschung. Im Anschluss daran sind auch Verbesserungen und Erweiterungen der Werkzeuge zum Identitätsmanagement erforderlich [He10].

2 Material: Datenbanken und Module

Medizinische Forschungsverbünde decken eine große Vielfalt von Anwendungsszenarien aus verteilter Versorgung, Telemedizin, assistierender Technik, translationaler, klinischer und epidemiologischer Forschung über Volkskrankheiten bis hin zu seltenen Erkrankungen ab.

Damit einher gehen verschiedene Datensammlungen: elektronische Patientenakten, klinische und epidemiologische Register, Bilddatenbanken, Biobanken. Das bringt ethische und rechtliche Probleme mit sich, denn medizinische Daten sind kaum wirksam zu anonymisieren. Insbesondere medizinische Bilddaten, genetische Daten und Daten aus Assistenzumgebungen sind extrem detailliert und hochgradig charakteristisch für den individuellen Patienten, zu dessen Identifikation sie leicht missbraucht werden können [Go06, MS04]. Für das Reidentifizierungspotenzial medizinischer Bilder kann man etwa an Hautanomalien oder Skelettfehlbildungen denken.

Daten und Proben werden oft über lange Zeiträume hinweg benötigt. Ihre primäre Nutzung im Behandlungszusammenhang wird durch die strikten Regelungen der ärztlichen Schweigepflicht und entsprechende Sicherheitsmaßnahmen in Krankenhaus- und Arztpraxissystemen geschützt; entsprechende Konzepte für die von der Gesundheitstelematik angestrebte Vernetzung sind seit Jahren in der öffentlichen Diskussion. Die Langzeitauf-

bewahrung und die Sekundärnutzung für Forschungszwecke erfordern allerdings sorgfältig konzipierte weiterreichende Datenschutzmaßnahmen.

Obwohl medizinische Versorgung und Forschung oft eng verzahnt und Ärzte in Personalunion in beiden Bereichen tätig sind, bedeutet die Nutzung von Patientendaten für die Forschung eine Zweckänderung. Daher definieren die rechtlichen Rahmenbedingungen eine strikte Trennlinie zwischen Behandlung und Forschung, beschränken die Datenflüsse und führen sogar dazu, dass Datensammlungen und Forschungsprozesse modular auf verschiedene Kontexte verteilt werden müssen, siehe Abb.1, in denen jeweils unterschiedliche Regularien zu beachten sind. Ein solches Modul kann eine oder mehrere gleichartige Datenbanken enthalten. Die verschiedenen Module benötigen unterschiedliche Ansätze, um Datenspeicherung und Datenzugriffe datenschutzkonform zu gestalten:

- Im klinischen Modul und im Studienmodul ist die pseudonyme Speicherung vorgeschrieben, aber der Zugriff für autorisierte Nutzer – das sind behandelnde Ärzte und ihre Mitarbeiter, die auch an Forschungsprojekten beteiligt sind – personenbezogen erforderlich und erlaubt. Dieses Prinzip, „pseudonyme Speicherung, personenbezogener Zugriff", ist übrigens auch im Versorgungskontext für einrichtungsübergreifende Patientenakten angemessen.

- Im Forschungsmodul und im Biobank-Modul sollten sowohl die Speicherung als auch der Zugriff nur über Pseudonyme möglich sein.

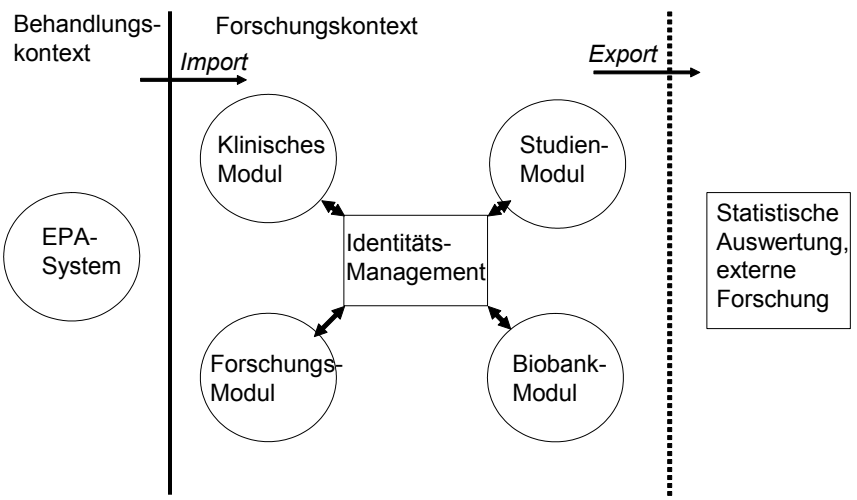

Abbildung 1: Module eines medizinischen Forschungsverbunds; neben dem Identitätsmanagement sind auch andere zentrale Dienste nötig, etwa Rechtemanagement oder Datenqualitätsmanagement.

Im klinischen Modul und im Studienmodul müssen Pseudonyme allerdings etwas unterschiedlich eingesetzt werden: Im Studienmodul finden die klinischen Studien statt, die

besonderen gesetzlichen Regularien unterliegen, siehe 2.2, und diese legen u. a. fest, dass die Prüfärzte die Pseudonyme ihrer eigenen Patienten kennen. Das klinische Modul bündelt alle übrigen patientennahen Forschungsprojekte, siehe 2.3. Hier sollte – zumindest bei einrichtungsübergreifenden Projekten – nur ein Treuhänder die Pseudonyme zuordnen können.

2.1 Elektronische Patientenakte (EPA)

Im direkten Behandlungszusammenhang ist der Patient persönlich bekannt; die Benutzung seines echten Namens ist üblich und erlaubt, und wird von ihm auch erwartet.

Die Nutzung einer elektronischen Patientenakte erfordert allerdings schon eine einfache Form des Identitätsmanagements, das für behandelnde Ärzte und deren berufliches Personal einen personenbezogenen Zugriff erlaubt, aber ansonsten die Identitätsdaten verbirgt, selbst vor Datenbank-Dienstleistern; hier ist also das Prinzip „pseudonyme Speicherung, personenbezogener Zugriff“ angemessen. Erst recht gilt das für einrichtungsübergreifende Patientenakten, wozu auch die konzernweiten Patientenakten großer Krankenhauskonzerne zu rechnen sind.

Die EPA ist Gegenstand der Gesundheitstelematik und dabei massiven politischen Konflikten ausgesetzt, die ihre flächendeckende Einführung bisher verzögert haben. Im Fokus der TMF, die die Forschungsinfrastruktur adressiert, ist sie nur am Rande. Auf viele ihrer Prozesse passen Teile des TMF-Datenschutzkonzepts aber sehr gut, und die darin beschriebenen Ansätze und Werkzeuge sind genauso nützlich und anwendbar.

2.2 Studienmodul

Klinische Studien zur Arzneimittelprüfung oder zur Funktion und zum Nutzen von Medizinprodukten unterliegen spezialgesetzlichen Regelungen, vor allem dem Arzneimittelgesetz (AMG) oder Medizinproduktegesetz (MPG) und den Richtlinien zur guten klinischen Praxis (GCP). Darin sind die Prozesse und der Umgang mit den Daten recht genau vorgegeben, unter anderem die Nutzung eines Pseudonyms, das hier SIC (Subject Identification Code) genannt wird und dem Prüfarzt, der hier gleichzeitig auch Behandler ist, bekannt ist. Ein aus Datenschutzsicht wichtiger Aspekt des Studienmoduls ist auch, dass der Zweck der Datenverarbeitung und der Nutzerkreis von vornherein feststehen. Die Überlappung mit dem Behandlungskontext ist groß; aus der Sicht des Patienten ist seine Teilnahme an einer klinischen Studie mit seiner Behandlung weitgehend identisch, außer dass die experimentellen Elemente der Therapie präzise definiert sind und nach einem vorgegebenen Studienprotokoll systematisch ausgewertet werden.

2.3 Klinisches Modul

Hier werden alle Arten klinischer Forschung zusammengefasst, die nicht den Spezialregelungen von 2.2 unterliegen. Das können Langzeit-Beobachtungsstudien, z. B. bei seltenen Erkrankungen sein, die im Sinne eines Data-Mining erst zu einer Hypothesen-

bildung führen sollen. In dieses Modul gehören auch klinische Register, z. B. Krebsregister, in denen für bestimmte Erkrankungen möglichst von allen Patienten regional oder auch überregional Daten zusammengetragen werden. Typisch für das klinische Modul ist, dass die Daten – im Gegensatz zu einer klinischen Studie – nicht für eine ganz konkrete Zweckbestimmung gesammelt werden, sondern sozusagen als Rohmaterial, auf dem künftige Forschungsprojekte aufbauen können. Typisch ist andererseits, dass ein direkter Patientenkontakt erforderlich ist.

Auch hier sind Ärzte im Behandlungszusammenhang beteiligt, sie melden ihre Daten an das Register oder die zentrale Datenbank und können durch direkten patientenbezogenen Zugriff auch Unterstützung bei der Behandlung finden. Z. B. ist es bei seltenen Erkrankungen durchaus üblich, dass Fälle in einem Expertenforum diskutiert werden. Alle Zugriffe außer durch den direkt behandelnden Arzt, sei es eine simple Benchmark-Auswertung oder die Langzeit-Auswertung einer Beobachtungsstudie, gehören aber in den Forschungskontext und müssen daher frei vom Bezug zum konkreten Patienten sein. Daher ist eine pseudonyme Speicherung vorzusehen, wobei die Pseudonyme im Grundsatz extern bei einem zentralen vertrauenswürdigen Dienst treuhänderisch verwaltet werden; wenn Patienten ihre behandelnde Stelle während der Laufzeit des Projekts nicht wechseln, kann eine Pseudonymverwaltung an der Datenquelle aber auch angemessen sein.

2.4 Forschungsmodul

In dieses Modul gehören alle Datensammlungen und -verarbeitungsprozesse, die nicht den direkten Patientenkontakt erfordern und damit deutlich von der Behandlung abgekoppelt sind. Typische Beispiele sind epidemiologische Projekte wie bevölkerungsbezogene Register, z. B. Landeskrebsregister, oder Kohortenstudien, bei denen von einer definierten Teilmenge der Bevölkerung immer wieder Daten erfasst werden. Hier ist kein direkter persönlicher Bezug nötig, aber Daten von verschiedenen Zeitpunkten oder aus verschiedenen Quellen müssen richtig zugeordnet werden können – der typische Anwendungsfall der Pseudonymisierung.

2.5 Biobankmodul

Eine Biobank sammelt Biomaterial, Proben und aus Proben gewonnene Derivate, mit dem Ziel genetischer Analysen für alle möglichen Arten medizinischer Forschung, sei es Grundlagenforschung oder translationale, klinische oder epidemiologische Forschung. Zu einer Biobank gehören Datenbanken für das Management der Proben, für klinische Begleitdaten („Annotationsdaten“) und für die Ergebnisse genetischer Analysen. Neben den datenschutzrechtlichen Anforderungen sind in diesem Modul auch eigentumsrechtliche Gesichtspunkte sowie besonders hoch gewichtete Persönlichkeitsrechte zu berücksichtigen [Si06]. Zum Betrieb einer Biobank mit allen ihren Komponenten werden verschiedene Pseudonyme eingesetzt. Zunächst werden Proben mit einer – nach Möglichkeit nichtsprechenden, also pseudonymen – Probenkennung LabID markiert. Proben enthalten aber umfangreiche genetische Informationen über ihren Spender und somit genetische Fingerabdrücke, die als Identifikatoren geeignet sind. Da der Wert

einer Biobank aber erst durch zugeordnete medizinische Daten – „klinische Annotation“, mindestens eine Diagnose – entsteht, setzen sie diese zugeordneten Daten einem hohen Reidentifizierungsrisiko aus. Daher sollte der Bezug zwischen Proben und Daten ebenfalls durch einen Pseudonymisierungsschritt geschützt sein, etwa indem die medizinischen Daten nur einen kryptographisch verschlüsselten Verweis $LabID_{tr}$ auf die zugehörigen Proben enthalten, wie in Abb. 2 dargestellt; selbstverständlich können einer Person mehrere Proben zugeordnet sein. Daten aus Probenanalysen, die ja jederzeit wieder aus der Probe gewonnen werden können, gehören dagegen im Allgemeinen zur Probe und nicht in die Annotationsdatenbank.

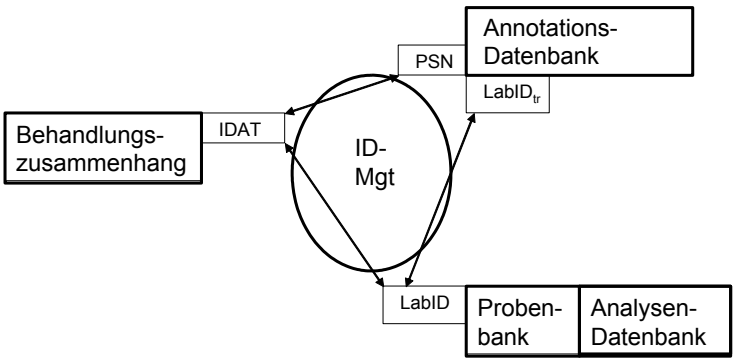

Abbildung 2: In den Annotationsdaten einer Biobank sind die Verweise auf den Patienten und auf die zugehörigen Proben pseudonymisiert. (IDAT = Identitätsdaten, PSN = Pseudonym)

Im Forschungsverbund nach Abbildung 1 sind die klinischen Annotationsdaten am besten im Forschungsmodul aufgehoben.

3 Methoden: Identitätsmanagement – Was wird benötigt?

In vielen Situationen findet die medizinische Forschung weit entfernt vom Patienten statt. Die unmittelbare Kontrolle und Steuerung des Datenzugriffs durch die Patienten selbst – wie sie in der Gesundheitstelematik für die Behandlung, soweit sinnvoll, vorgesehen ist – ist für die Forschung keine realistische Option, wenn Patienten nicht für jeden Datenzugriff einbestellt werden sollen. Darüber hinaus haben die Patienten ja sogar ein Recht auf Nichtwissen hinsichtlich medizinischer oder genetischer Informationen. Daher kann die Verantwortung für die Vertraulichkeit der Daten und für das Identitätsmanagement nicht den Patienten selbst auferlegt werden, sondern es werden dafür vertrauenswürdige Dritte eingeschaltet (Datentreuhänder, Trusted Third Parties = TTPs).

Sobald die Daten (oder Proben) eines Patienten den Behandlungszusammenhang für eine sekundäre Nutzung verlassen, sei es für eine einfache statistische Auswertung oder für ein komplexes Forschungsprojekt, spielt die Identität des Patienten überhaupt keine

Rolle mehr und muss daher verborgen werden [PR04]. Die erste Option zum Schutz der Vertraulichkeit ist die Anonymisierung der Daten. Diese ist für einfache Auswertungsszenarien geeignet. Die Multidimensionalität medizinischer Daten – besonders von genetischen Daten oder Daten aus Assistenzumgebungen – verhindert aber meistens eine effektive Anonymisierung [G06, MS04]. Anonymisierung scheidet auch aus, wenn Daten aus verschiedenen Quellen oder von verschiedenen Zeitpunkten zusammengeführt werden müssen. Für manche Anwendungsfälle muss sogar der Weg zurück zum Patienten offen gehalten werden, etwa um einen lebenswichtigen Zufallsbefund zurückzumelden oder um geeignete Probanden für eine neue klinische Studie zu „rekrutieren"; in epidemiologischen Studien – etwa zur Lebensqualität nach einer bestimmten Therapie – müssen oft Daten durch Befragung nacherhoben werden. Daher ist in der Regel für medizinische Forschungsprojekte eine Pseudonymisierung der Anonymisierung vorzuziehen; hierbei werden die Identitätsdaten durch eine zufällige Zeichenkette ersetzt, die nur von einem Treuhänder (TTP) aufgelöst werden kann, der somit auch als Teil des Kontaktmanagements mitwirkt.

Die informationelle Gewaltenteilung, aber auch die Verschiedenheit der rechtlichen Rahmenbedingungen, wird am besten durch den Gebrauch verschiedener Pseudonyme in den einzelnen Modulen eines Forschungsverbunds berücksichtigt. Aus dem historischen „Wildwuchs" und den in anderen Kontexten bereits etablierten Nomenklaturen resultieren leider unterschiedlich aufgebaute Bezeichnungen und Akronyme für die verschiedenen Pseudonyme; diese sind

- PID im klinischen Modul („Pseudonymer Patientenidentifikator").
- SIC im Studienmodul („Subject Identification Code"). Falls in verschiedenen Studien, etwa bedingt durch die eingesetzte Studiensoftware, verschiedene SIC-Schemata verwendet werden, wird für das Studienmodul noch ein übergeordnetes gemeinsames Pseudonym benötigt, das dann als PID_S bezeichnet wird und nicht mit dem PID des klinischen Moduls identisch ist.
- LabID im Biobankmodul („Laboridentifikationsnummer").
- PSN („Pseudonym") und $LabID_{tr}$ im Forschungsmodul.

Das Identitätsmanagement muss alle diese Pseudonyme und ihre Zuordnung zur wahren Identität verwalten und schützen. Dazu benötigt es Werkzeuge und Schnittstellen.

Neben Pseudonymisierungswerkzeugen wird für Datenexporte auch ein Anonymisierungsfilter benötigt. Dieser sollte auch die Möglichkeit bieten, das Reidentifizierungsrisiko der Daten durch Hinzufügen von Fehlern („Rauschen") zu verringern, sowie Suchanfragen mit zu kleinen Ergebnismengen zurückzuweisen. Da das Reidentifizierungspotentenzial medizinischer Daten hoch und oft schwer einschätzbar ist, sollten im Allgemeinen aber zumindest keine „Public-Use"-Daten exportiert werden. Da effektiv anonymisierte Daten für eine wissenschaftliche Verwendung in aller Regel zu grob sind, sollte ein verbindlicher organisatorischer und vertraglicher Rahmen für die Empfänger der Daten geschaffen werden.

4 Ergebnisse: Identitätsmanagement – Was ist vorhanden?

Die TMF hat für die unterschiedlichen Module jeweils einzeln ein Datenschutzkonzept erarbeitet, zusammen mit den jeweils passenden Identitätsmanagement-Prozeduren und -Werkzeugen. Diese Konzepte wurden mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt [Re06, Po07]. Die vorhandenen Werkzeuge zum Identitätsmanagement sind:

- Der PID-Generator. Er verwaltet eine Liste von im Forschungsverbund registrierten Patienten und erzeugt pseudonyme Identifikatoren (oder gibt vorhandene heraus), die als PID bezeichnet werden. Er hat eine eingebaute Fehlertoleranz für Identitätsdaten, die mit den Methoden des Record Linkage, insbesondere mit phonetischen Vergleichen, arbeitet und weitgehend konfigurierbar ist. Ein solcher PID ist zur Verwendung im klinischen Modul, in ähnlicher Form auch im Studienmodul als SIC oder PID_S, bestimmt.

- Der Pseudonymisierungsdienst. Er nimmt einen eindeutigen Identifikator entgegen – im Normalfall einen PID – und transformiert diesen kryptographisch in ein Pseudonym „zweiter Stufe“, als PSN bezeichnet. Ein solches PSN wird im Forschungsmodul, auch in der Annotationsdatenbank einer Biobank eingesetzt.

Diese beiden Werkzeuge können als Web-Dienste implementiert werden und sollten von (im allgemeinen unterschiedlichen) TTPs betrieben werden; die genaue Realisierung hängt unter Berücksichtigung des Verhältnismäßigkeitsprinzips u. a. von der Größe des Forschungsverbunds, seinen organisatorischen Rahmenbedingungen und der Sensibilität der Daten ab.

Beide Werkzeuge werden in verschiedenen Forschungsverbünden eingesetzt [He10] und haben sich in der Praxis bewährt. Allerdings haben die praktischen Erfahrungen auch einige Unzulänglichkeiten im Detail aufgedeckt, wie z. B. die fehlende Unterstützung fremdländischer Namen im PID-Generator, die Beherrschung nur eines einzigen Pseudonymschemas oder unhandliche Schnittstellen zu vorhandenen, insbesondere kommerziellen, Datenerfassungssystemen (EDC-Systemen = „Electronic Data Capture“), die in der Regel im Studienmodul eingesetzt werden.

5 Ausblick – Was kommt als Nächstes?

Die einzelnen, heterogenen Datenschutzkonzepte für die Module wurden in der Zwischenzeit von der TMF zu einem vereinheitlichten Datenschutzkonzept weiterentwickelt, das alle vier Arten von Modulen nach Abb. 1 umfasst und auch die Schnittstellen und Datenflüsse zwischen diesen berücksichtigt. Die Abstimmung mit den Datenschutzbeauftragten steht für diese Weiterentwicklung allerdings noch aus. Das revidierte und erweiterte Konzept und auch die mittlerweile zutage getretenen Schwächen der existierenden Werkzeuge erfordern eine gründliche Überarbeitung und teilweise Neukonzeption der Komponenten des Identitätsmanagements. Die weiterentwickelten Werkzeuge sollen dann als Leistungen anbieten:

- Erzeugung und Verwaltung unterschiedlicher Pseudonyme für denselben Patienten zur Nutzung in den unterschiedlichen Modulen.

- Verbindung mit einem Patienten-Management-System nach der Art eines in der Wirtschaft üblichen Customer-Relationship-Managements (CRM-System), das bei Bedarf die Kontaktierung unter Schutz der Pseudonyme und Wahrung der Vertraulichkeit ermöglicht und dabei auch unterschiedliche Vereinbarungen der Patienteneinwilligung korrekt berücksichtigt (Einwilligungsmanagement).

- Standardisierte Schnittstellen zu EDC-Systemen und Datenbanken, die in den unterschiedlichen Modulen eingesetzt werden.

- Schnittstellen zu lokalen und verbundweiten Rechteverwaltungs- und Zugangskontrollsystemen.

Darüber hinaus sollen die Werkzeuge vielfältige Anpassungs- und Konfigurationsoptionen bieten, so dass sie in der sehr variationsreichen Landschaft der medizinischen Forschungsverbünde überall nutzbar sind.

6 Zusammenfassung und Diskussion

Das Identitätsmanagement von Patienten in medizinischen Forschungsverbünden erfordert den Umgang mit verschiedenen Pseudonymen zur selben Person. Die vorhandenen Werkzeuge dazu, der PID-Generator und der Pseudonymisierungsdienst, haben sich zur Erfüllung von Datenschutzanforderungen in der medizinischen Forschung bewährt, müssen aber an erweiterte Anforderungen angepasst werden. Nach der in die Wege geleiteten Überarbeitung und Erweiterung werden sie für das revidierte Datenschutzkonzept der TMF und auch für internationale Projekte einsetzbar sein.

Literaturverzeichnis

[Go06] Golle, P.: Revisiting the uniqueness of simple demographics in the US population. WPES ’06, October 30, 2006, Alexandria VA, USA.

[He10] Helbing, K. et al.: Review of a data protection scheme for medical research networks after 5 years of operation. Meth. Inf. Med. 49 (2010), 601-607.

[KN] http://kompetenznetze-medizin.de/

[MS04] Malin, B., Sweeney, L.: How (not) to protect genomic data in a distributed network. J. Biomed. Inform. 37 (2004), 179-192.

[PR04] Pommerening, K; Reng, M.: Secondary use of the Electronic Health Record via pseudonymisation. In Box L. et al. (Hrsg.): Medical Care Compunetics 1, IOS Press, Amsterdam 2004; S. 441-446.

[Po07] Pommerening, K.: Das Datenschutzkonzept der TMF für Biomaterialbanken. it – Information Technology 49 (2007), 352–359.

[Po08] Pommerening, K. et al.: Integrating eHealth and medical research: The TMF data protection scheme. In Blobel, B. et al. (Hrsg.): eHealth: Combining Health Telematics, Tele-

medicine, Biomedical Engineering and Bioinformatics to the Edge, Aka Berlin 2008; S. 5-10.

[Re06] Reng, C. M.; Debold, P., Specker, C., Pommerening, K.: Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin. Medizinisch Wissenschaftliche Verlagsgesellschaft, München, 2006.

[Si06] Simon, J. et al.: Biomaterialbanken – Rechtliche Rahmenbedingungen. Medizinisch Wissenschaftliche Verlagsgesellschaft, München, 2006.

[TMF] http://www.tmf-ev.de/