

Pseudonymisierung in der medizinischen Forschung - das generische TMF-Datenschutzkonzept

Pseudonymization in medical research - the generic data protection concept of the TMF

• Klaus Pommerening¹ • Michael Reng² • Peter Debold³ • Sebastian Semler⁴

Die Nutzung von Patientendaten in medizinischen Forschungsnetze steht im Konflikt mit den Persönlichkeitsrechten der Betroffenen, insbesondere, wenn Daten einrichtungsübergreifend und langfristig gespeichert und genutzt werden sollen. In der Telematikplattform für Medizinische Forschungsnetze (TMF) wurde ein "generisches" Datenschutzkonzept entwickelt, das in zwei Modellvarianten den Aufbau geeigneter Datenpools beschreibt. Dieses Konzept fand die Zustimmung der Datenschutzbeauftragten und dient als Grundlage individueller Konzepte für die einzelnen Netze.

Schlüsselwörter: Datenschutz, Pseudonyme, medizinische Forschungsnetze

Using patient data in medical research nets is in conflict with the patients rights on privacy, in particular when data are collected from several sources and stored in long-term registries. The TMF (Telematics Platform for Medical Research Networks) developed a "generic" data protection concept that specifies two models for building research data pools. The german data Protection Commissioners agreed with this concept which in the meantime is the basis for concretisations in several research networks.

Keywords: data protection, pseudonyms, medical research networks

1. Einleitung

Medizinische Forschung, sei sie klinisch oder epidemiologisch ausgerichtet, braucht systematisch gewonnene Daten hoher Qualität. Für einzelne Studien haben sich seit langem Vorgehensweisen etabliert, die unter anderem den Anforderungen an datenschutzgerechte Durchführung genügen. Durch überregionale Kooperation, Vernetzung und Zusammenführung von Daten-

sätzen aus verschiedenen Quellen wird die Basis für wesentlich weiter gehende Vorhaben geschaffen, es stellen sich aber auch wesentlich höhere Anforderungen an die Wahrung der Persönlichkeitsrechte von Patienten und Probanden. Kompetenznetze und andere Forschungsverbünde können nur dann die Forschung entscheidend voranbringen, wenn sie eine telematische Infrastruktur aufbauen, die ein gemeinsames Datenmanagement für die in ihrem Rahmen

¹ Institut für medizinische Biometrie, Epidemiologie und Informatik der Johannes-Gutenberg-Universität Mainz, Mainz, Deutschland

² Abteilung für Innere Medizin, Kreiskrankenhaus Bogen, Bogen, Deutschland

³ Debold & Lux GmbH, Hamburg, Deutschland

⁴ Telematikplattform für Medizinische Forschungsnetze e. V., Berlin, Deutschland

durchgeführten, meistens multizentrischen, Studien ermöglicht und darüber hinaus ein langfristiges Poolen von qualitätsgesicherten Daten sowie den Aufbau von Biomaterialbanken vorsieht. Damit eröffnen sich Möglichkeiten zur Langzeitbeobachtung chronisch kranker Patienten, zur Erforschung von Spätfolgen und Auswirkungen auf die Lebensqualität nach aggressiven Therapien, zur Gewinnung ausreichender Fallzahlen bei seltenen Erkrankungen und zur Rekrutierung geeigneter Probanden für neue Forschungsprojekte. Um diese Ziele zu verfolgen, reichen die klassischen Werkzeuge datenschutzgerechter Forschung - Anonymisierung bzw. Einwilligungserklärung - nicht mehr aus. Es sind neue Methoden nötig: Pseudonymisierung [1] und informationelle Gewaltenteilung (z. B. durch getrennte Datenhaltung oder Aufteilung von Funktionen). Hierfür hat die Telematikplattform für medizinische Forschungsnetze (TMF) [2] ein generisches Datenschutzkonzept mit Modellvarianten [3], [4] entwickelt, das den Verbänden ermöglicht, ihre Forschungsziele in rechtlich abgesicherter Weise zu verfolgen und dafür ein positives Votum der zuständigen Datenschutzbeauftragten zu erhalten. Diese Modelle wurden bereits von einer Reihe von Forschungsnetzen adaptiert; die konkrete Implementation ist dort in Arbeit, zum Teil schon im Betrieb. An der Erweiterung des Konzepts auf Biomaterialbanken wird derzeit gearbeitet. Die Integration in die künftige Architektur des Gesundheitswesens, insbesondere die Übertragung auf Vorhaben der Versorgungsforschung, wird angestrebt.

2. Pseudonyme

Ein Pseudonym ist ein Kennzeichen, das einen Datensatz einer eindeutigen Person zuordnet, ohne etwas über deren Identität zu verraten. Im Gegensatz zu einer faktischen Anonymisierung gibt es aber einen "Geheimnisträger", der in der Lage ist das Pseudonym aufzulösen, d. h., durch Depseudonymisierung den Personenbezug wieder herzustellen. Dieses wird durch Abbildung 1 veranschaulicht, die das Basismodell der Pseudonymisierung beschreibt. Für andere Personen, die nicht im Besitz des Geheimnisses sind, ist ein pseudonymisierter Datensatz dagegen genauso wenig einem Individuum zuzuordnen wie ein anonymisierter.

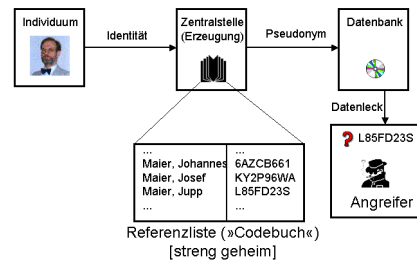


Abbildung 1: Pseudonymisierung - das Basismodell

Zweck der Pseudonymisierung - im Unterschied zur Anonymisierung - ist zum ersten, Daten zu einem Fall aus verschiedenen Quellen oder von verschiedenen Zeitpunkten zusammenführen zu können, und zum zweiten, die "Fährte zum Fall" für besondere Anlässe offen zu halten.

Pseudonymisierung erlaubt also im Gegensatz zur Anonymisierung eine Rückidentifizierung. Diese kann gewollt sein und findet dann kontrolliert durch Depseudonymisierung statt, oder sie ist unbefugt mit Hilfe von Inferenzen aus den Daten möglich, z. B. durch seltene Diagnosen oder detaillierte Beschreibungen von Wohnorten; die Möglichkeiten hierzu müssen durch eine gründliche Analyse des Rückidentifizierungsrisikos in jedem Einzelfall abgeschätzt werden.

Zu beachten ist, dass wegen der möglichen Rückidentifizierung, wie gut sie auch immer abgesichert sein mag, die Pseudonymisierung rechtlich nicht zur Anonymisierung äquivalent ist: Pseudonymisierte Daten sind personenbeziehbar und dürfen daher in der Regel nur verwendet werden, wenn die Probanden darin eingewilligt haben.

Daten von Patienten oder Probanden werden oft gezielt für ein Forschungsprojekt erhoben, kommen in der Regel aber aus einem Behandlungszusammenhang, wo sie durch die besonders hohe Hürde der ärztlichen Schweigepflicht geschützt sind, wie in Abbildung 2 illustriert. Mit einer Einwilligungserklärung kann man zwar viel Freiraum für die Nutzung der Daten erreichen; eine Einwilligungserklärung ist aber unwirksam, wenn sie zu Eingriffen in die Persönlichkeitsrechte führt, die sich durch andere Maßnahmen, wie z. B. Anonymisierung oder Pseudonymisierung, vermeiden ließen, oder wenn ihre Tragweite nicht völlig klar ist, wie es zum Beispiel bei einer Einwilligung zur völlig freien Verwendung von Daten oder zur beliebigen Weitergabe von Proben der Fall wäre.

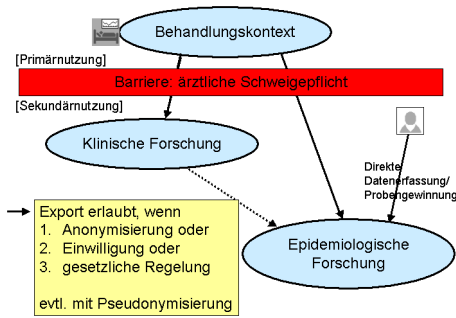


Abbildung 2: Die Barriere der ärztlichen Schweigepflicht

Daher ist es wichtig, verschiedene Modelle und Vorgehensweisen für die Anonymisierung oder Pseudonymisierung mit unterschiedlicher Tragweite und Eingriffstiefe zur Verfügung zu haben, um den spezifischen Erfordernissen in verschiedenen Forschungsszenarien gerecht werden zu können. Insbesondere für die Langzeitsammlung von Patientendaten bietet das TMF-Konzept zwei Modelle, die in den Abschnitten 3.4 und 3.5 beschrieben werden; sie unterscheiden sich darin, an welcher Stelle der gesamten Netzarchitektur der Datenpool angesiedelt ist, und wer einen Online-Zugriff auf die Datenbank erhält.

Die hier verwendeten Pseudonyme sind technisch gesehen kryptographisch verschlüsselte Patientenidentifikatoren. Die in anderen Kontexten von Chaum [5] vorgeschlagenen Methoden der Pseudonymisierung beruhen auf blinder digitaler Signatur und bewirken, dass der Eigner des Pseudonyms selbst der Geheimnisträger ist und dadurch dessen Gebrauch steuert; dieses Vorgehen ist im Kontext der medizinischen Forschung nicht geeignet, schon deshalb, weil die Kommunikation mit dem Patienten nur über die Vertrauensperson "behandelnder Arzt" stattfinden darf.

3. Modelle der Pseudonymisierung

Es werden fünf Szenarien wachsender Komplexität beschrieben. Die ersten drei beziehen sich auf die einmalige Nutzung von Daten zu einem vorher bestimmten Forschungszweck; hier kann der Schutz der Persönlichkeitsrechte durch ziemlich einfache Maßnahmen in ausreichendem Maße sichergestellt werden. Die letzten beiden Szenarien sind die im generischen TMF-Datenschutzkonzept ausführlich beschriebenen; sie werden beim Aufbau von Forschungsnetzen mit Langzeitdatenspeicherung für vorher nicht notwendig bekannte Fragestellungen relevant. Für den Aufbau solcher langfristigen Forschungsinfrastrukturen ist die vereinfachte Sicht, bei der nur zwischen Behandlungs- und Forschungskontext unterschieden wird, nicht mehr ausreichend; es sind kompliziertere Modelle nötig, bei denen bis zu vier Bereiche voneinander abgegrenzt werden: der Behandlungszusammenhang, die lokale

Sammlung von Forschungsdaten, zentrale Datenpools für ein Forschungsnetz und die Nutzung von Daten aus diesen Pools als Datenbasis für konkrete Auswertungen oder zur Rekrutierung von Fällen für neue Studien. Die Grenzen zwischen diesen Bereichen werden immer auch durch einen Pseudonymisierungsschritt markiert. Dadurch entstehen komplexe Prozessmodelle, deren Beschreibungen notwendigerweise umfangreich sind, weil sie darstellen, was durch organisatorische und technische Maßnahmen, insbesondere durch geeignete Software, umgesetzt werden soll. Diese Komplexität wird aber durch die Systemarchitektur mit Unterstützung geeigneter, bereits verfügbarer Software-Werkzeuge vor dem Anwender verborgen. Die Teilnehmer an einem solchen Netz, seien sie Datenlieferanten oder auswertende Forscher, sollen von der Komplexität dieser Modelle nicht bei ihrer Arbeit behindert werden.

• 3.1 Einzelne Datenquelle, Einmalnutzung der Daten

Dieses ist der typische Anwendungsfall für die Anonymisierung. Als Beispiel kann man sich eine einfache statistische Auswertung von Patientendaten vorstellen. Wegen der Anonymisierung ist hier nicht einmal die Einwilligung der betroffenen Patienten nötig.

• 3.2 Mehrere überlappende Datenquellen mit Einmalnutzung

Hierbei müssen Daten aus verschiedene Quellen zusammengeführt werden. Als Beispiel kann man an die Auswertung von Follow-Up-Daten denken. Die gewünschte Nutzung lässt sich mit Einweg-Pseudonymen erreichen. Wesentliche Voraussetzung ist, dass die verschiedenen Datenquellen einen einheitlichen eindeutigen Patientenidentifikator (PID) zur Verfügung haben. Die Pseudonymisierung besteht dann aus einer kryptographischen Einweg-Verschlüsselung des PID. Diese sollte von einer unabhängigen Stelle ausgeführt werden. In einem größeren Forschungsverbund ist dafür ein vertrauenswürdiger zentraler Dienst einzurichten ("Trusted Third Party" - TTP) und in die Netzarchitektur einzubinden. Dieser Pseudonymisierungsdienst sollte im Sinne der informationellen Gewaltenteilung die begleitenden medizinischen Daten gar nicht zu Gesicht bekommen. Dies kann man erreichen, indem nach dem Prinzip der asymmetrischen Verschlüsselung die medizinischen Daten bei den Datenquellen mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und in dieser Form durch den Pseudonymisierungsdienst "durchgereicht" werden. Der Datenfluss wird in Abbildung 3 veranschaulicht; hier steht MDAT für die medizinischen Daten, IDAT für die Identitätsdaten und PSN für das Pseudonym.

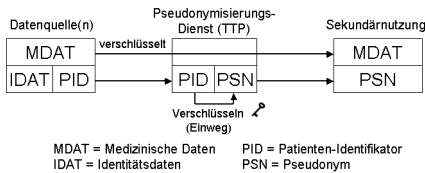


Abbildung 3: Pseudonymisierung für einmalige Sekundärnutzung

Der Pseudonymisierungsdienst speichert die Zuordnung zwischen Patientenidentifikatoren und Pseudonymen nicht und kann auch die Verschlüsselung nicht umkehren. Daher ist es unproblematisch, bei den Datenquellen PID und Identitätsdaten zusammen zu speichern; als PID kann auch ein allgemein verfügbarer Identifikator verwendet werden, wie er etwa mit der künftigen Patienten- bzw. Gesundheitskarte eingeführt werden soll. Es muss in diesem Modell nur sicher gestellt sein, dass der Pseudonymisierungsdienst über einen geeigneten Zugriffsschutz die "Probeverschlüsselung" durch Unbefugte wirksam verhindert.

Dieses Modell wurde in einem TMF-Projekt [6] zur Versorgungsforschung implementiert und ist dort seit 2002 im Routinebetrieb.

• 3.3 Einmalnutzung mit möglicher Rückidentifizierung

Bei größeren Forschungsvorhaben kann die Notwendigkeit zur Rückidentifizierung von Probanden entstehen. Ein möglicher, auch im Interesse des Betroffenen liegender Grund ist etwa die Rückmeldung entdeckter genetischer Prädispositionen; Gründe sind aber auch die Rekrutierung von geeigneten Fällen und Einholung der Einwilligung für weitergehende Studien oder die Auflösung nachträglich entdeckter Unstimmigkeiten in den Daten.

In dem konzeptuell einfachsten Modell der Pseudonymisierung mit möglicher Rückidentifizierung führt ein zentraler Pseudonymisierungsdienst eine Referenzliste für die Zuordnung zwischen Identitätsdaten und Pseudonymen. Eine solche, potenziell riesengroße, Liste wie in Abbildung 1 wäre natürlich ein herausgehobenes Angriffsziel und damit eine sensible Stelle im Sicherheitskonzept. Die Referenzliste beim Pseudonymisierungsdienst entspricht nicht dem Stand der Technik; sie wird hier nur als Vorstufe erwähnt, um die Vorgänge zu veranschaulichen.

Besser geeignet ist ein Modell, das wie in 3.2 funktioniert, aber eine umkehrbare Verschlüsselung vorsieht. Hierfür sollte dann aber kein allgemein verfügbarer PID verwendet werden, sondern ein speziell für dieses Projekt erzeugter. Dafür braucht man eine weitere unabhängige Instanz, den PID-Dienst, der in der Ter-

minologie des TMF-Konzepts auch als "Patientenliste" bezeichnet wird. Dieser speichert dann tatsächlich eine Referenzliste, aber ein unbefugter Zugriff auf diese führt selbst bei unbefugtem Zugriff auf die exportierten Forschungsdaten zu keinem Erkenntnisgewinn, da der Zusammenhang zwischen PID und Pseudonym verborgen bleibt. Der Forderung nach Redundanz in Sicherheitsmaßnahmen wird hier also durch eine zusätzliche Datentrennung - informationelle Gewaltenteilung - mit einem zweistufigen Pseudonymisierungsverfahren (PID und PSN) Rechnung getragen. Der Datenfluss in diesem Modell wird durch Abbildung 4 veranschaulicht. Der Pseudonymisierungsdienst braucht sich hier nicht einmal die Datenquellen zu merken; im Falle einer nötigen Rückidentifizierung werden der Pseudonymisierungsdienst und der PID-Dienst hinzugezogen.

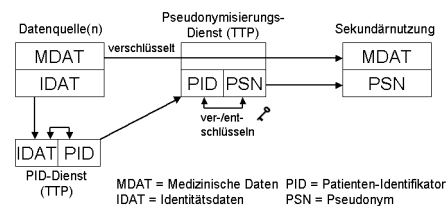


Abbildung 4: Pseudonymisierung mit möglicher Rückidentifizierung

• 3.4 Die pseudonymisierte Forschungsdatenbank

Ist auf der Seite der Datenverwendung nicht nur eine einmalige Nutzung, sondern der Aufbau einer längerfristig bestehenden Forschungsdatenbank, etwa eines krankheitsspezifischen Registers, geplant, so wird ein neues Niveau von Anforderungen an den Schutz von Persönlichkeitsrechten der Probanden erreicht. Bei der hier vorgeschlagenen Lösung ist der Datenfluss prinzipiell der gleiche wie in 3.3; allerdings werden die Daten auf der Nutzungsseite langfristig, auch für noch nicht definierte künftige Studien gesammelt. Hier ist der Zielkonflikt zwischen den Grundrechten auf Schutz der Persönlichkeit und auf Forschungsfreiheit aufzulösen. Dabei besteht ein Handlungsspielraum, der rechtliche Abwägungen und Kompromisse erfordert. Das Werkzeug der Einwilligungserklärung stößt an seine Grenzen, da eine solche sich immer nur auf eine definierte Datenverwendung und eine begrenzte Aufbewahrungsdauer beziehen kann. Ein freierer Umgang mit den Daten kann aber unter Umständen rechtlich vertreten werden, wenn zur Kompensation zusätzliche technische und organisatorische Schutzmaßnahmen vorgesehen werden; als Kompensation geeignet ist unter Umständen auch eine Abstufung der Einwilligungserklärung, die dem Patienten Wahlmöglichkeiten anbietet. Ein solcher gangbarer Weg zum Aufbau einer pseudonymisierten Datenbank wird durch das Modell

B des generischen TMF-Datenschutzkonzepts beschrieben.

In diesem Kontext ist das Problem der Qualitätssicherung der Daten besonders zu beachten; hierauf soll an dieser Stelle aber nicht weiter eingegangen werden.

• 3.5 Die zentrale klinische Datenbank

Das alternative Modell A des TMF-Konzepts folgt einem etwas anderen Ansatz, der besser auf die Erfordernisse von Forschungsnetzen mit "klinischem Fokus" zugeschnitten ist; es unterstützt die Langzeitbeobachtung chronisch kranker Patienten, das gemeinsame Datenmanagement verschiedener klinischer Studien oder die individuelle Rückmeldung von Forschungsergebnissen an den Patienten über den behandelnden Arzt ohne die Notwendigkeit, erst einen Depseudonymisierungsprozess anzustoßen. Im Zentrum dieses Modells steht eine Datenbank für die Langzeitspeicherung, auf die die teilnehmenden Kliniker direkten Zugriff haben; diese sind auch für die Qualität der Daten verantwortlich. Eine solche Datenbank im Online-Zugriff bedeutet einen relativ starken Eingriff in die Persönlichkeitsrechte; diese wird neben anderen Sicherheitsmaßnahmen auch dadurch kompensiert, dass die Datenbank keine Identitätsdaten enthält, sondern nur einen PID als Referenz. Dieser PID ist nur in der Datenbank und der Patientenliste des PID-Dienstes sichtbar und somit selbst schon ein echtes Pseudonym. Im Falle eines autorisierten Zugriffs wird diese Referenz mit Hilfe der Patientenliste aufgelöst und der Zugriff über ein ad hoc generiertes Token (TempID) gewährt. Zusätzliche Quellen, z. B. Sammlungen von Laborproben, werden über zusätzlich Referenzen (LabID) erschlossen. All diese Referenz-IDs bilden zusammen ein komplexes mehrstufiges Pseudonymisierungsverfahren. Wenn Daten aus der zentralen Datenbank für ein Forschungsprojekt benötigt werden, wird niemals ein Direktzugriff gewährt, sondern es wird ein geeigneter Auszug aus der Datenbank mit einem weiteren ad hoc erzeugten Pseudonym exportiert. Abbildung 5 zeigt die wesentlichen Komponenten des Datenflusses.

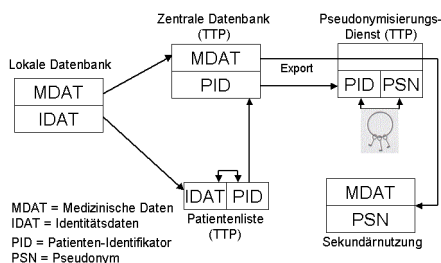


Abbildung 5: Die zentrale klinische Datenbank

Dieses Modell A erfordert, wie man sieht, die Implementierung von komplexen Kommunikationsbeziehungen.

Diese Komplexität wird allerdings durch die Automatisierung vieler Vorgänge zumindest vor den teilnehmenden Klinikern verborgen.

4. Ergebnisse

Das generische TMF-Konzept mit den Modellen A und B wurde in mehreren Projekten der TMF-Arbeitsgruppe Datenschutz entwickelt und nahm in einigen Sitzungen mit dem Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder eine konsensfähige Form an. Die endgültige Fassung fand auch die Zustimmung des Arbeitskreises Gesundheit der Datenschutzbeauftragten.

Die beschriebenen technischen Komponenten der beiden Modelle werden durch eine Sicherheitsinfrastruktur sowie durch organisatorische Maßnahmen ergänzt wie z. B. der Bildung eines "Ausschusses Datenschutz" für ein Forschungsnetz oder - im Falle besonders sensibler Krankheitsbilder - der Bestellung eines gegen Beschlagnahme geschützten Datentreuhänders. Eine simple Datenschutzkonzeption "von der Stange" kann auch das generische Konzept der TMF nicht verfügbar machen. Zu unterschiedlich sind die Datenstrukturen, Bedürfnisse und Anforderungen in der vernetzten medizinischen Forschung.

Die TMF-Arbeitsgruppe Datenschutz unterstützt medizinische Forschungsverbände bei der Adaption des generischen Datenschutzkonzepts für die eigenen Bedürfnisse. Das ist in einer Reihe von Fällen (15 Netze nach Stand März 2005) schon geschehen, in einigen Fällen ist die Implementation fortgeschritten oder schon im Betrieb. Zur Unterstützung der Implementation bietet die TMF geeignete Software-Bausteine an. Darüber hinaus stellt die TMF Policies (Verfahrensrichtlinien), Nutzungsordnungen, Vertragswerke und Einwilligungserklärungen als Muster zur Verfügung.

Mit den Datenschutzbeauftragten wurde für die Beurteilung eines konkreten Datenschutzkonzepts das folgende Verfahren vereinbart: Ein Forschungsverbund soll sich sein Konzept auf der Basis eines der Modelle A oder B erstellen und zunächst mit der TMF-Arbeitsgruppe Datenschutz diskutieren. Dabei sind Spezifika im nötigen Umfang zu beschreiben und nötige Abweichungen vom generischen Datenschutzkonzept zu begründen. Kommt die AG zu einem positiven Votum, wird dies dem für die Zentrale des Verbundes zuständigen Datenschutzbeauftragten schriftlich mitgeteilt; dieser stimmt sein Votum intern mit den anderen betroffenen Datenschutzbeauftragten ab. Dieses standardisierte Vorgehen bedeutet sowohl für den Forschungsverbund als auch für die Datenschutzbeauftragten eine erhebliche Erleichterung.

Schließlich bildet ein solchermaßen abgesichertes Datenschutzkonzept auch eine gute Basis, das Vertrauen von Patienten und mitwirkenden Ärzten in ein Forschungsnetz zu gewinnen - eine unabdingbare Voraussetzung, genügend viele "Datenspender" zu finden.

5. Diskussion

Das generische Datenschutzkonzept der TMF mit seinen zwei Modellvarianten A und B für die Netzarchitektur bietet einen Ansatz, medizinische Netze und zentrale Datensammlungen aufzubauen, der mit den deutschen und europäischen Datenschutzregelungen verträglich ist, die Persönlichkeitsrechte der Patienten und Probanden respektiert und unterschiedliche Situationen und Anforderungen abdeckt. Die Übertragung auf vergleichbare Situationen im Gesundheitswesen ist möglich und wünschenswert. Schließlich kommt man mit schnittstellenfähigen, datenschutzkonformen Lösungen dieser Art der Vision näher, Primärdaten aus der im Rahmen der Patientenversorgung anfallenden medizinischen Dokumentation - oder aus einer künftigen elektronischen Gesundheitsakte - direkt einer Sekundärnutzung für wissenschaftliche Zwecke oder für Zwecke der Evaluation im Gesundheitswesen zuzuführen.

Die Komplexität der Modellvarianten erscheint zunächst hoch, wird aber durch geeignete Implementations, unterstützt durch vorhandene Systemkomponenten, auf ein überschaubares Maß reduziert und vor den Teilnehmern des Forschungsnetzes verborgen.

Bei großen Datenbeständen ist es nicht völlig auszuschließen, dass selbst anonymisierte Patientendaten oder Laborproben anhand einer typischen Konstellation von Einzelwerten auf einzelne Patienten zurückgeführt werden können. Daher ist das Rückidentifizierungsrisiko unabhängig in jedem Einzelfall zu bewerten. Auch kann bereits das Wissen über die Mitwirkung eines Patienten in einem bestimmten Forschungsnetz Aufschluss über dessen - schützenswerte - Diagnose geben. Dieses geringe restliche Missbrauchspotenzial wird durch strikte Zugangskontrolle auch zu Forschungsdaten und durch organisatorische Regelungen im Konzept minimiert.

Der beschriebene Ansatz kann nicht für alle Zeiten festgeschrieben sein. Bei der Umsetzung entstehen praktische Erfahrungen und es kommen Rückmeldungen aus den Netzen; aber auch die Rahmenbedingun-

gen im Gesundheitswesen und der medizinischen Forschung ändern sich ständig. Im Bereich der genetischen Forschung sind neue gesetzliche Regelungen zu erwarten. Daher muss das generische TMF-Datenschutzkonzept kontinuierlich fortgeschrieben werden, um neuen Herausforderungen gerecht zu werden. Momentan konzentriert sich die Arbeit in der TMF auf die Einbeziehung von Biomaterialbanken in das Konzept; hier ist bis Ende 2005 mit vergleichbaren Ergebnissen zu rechnen.

Danksagung

Diese Arbeit wurde vom BMBF gefördert als Teilprojekt der TMF sowie der Kompetenznetze Pädiatrische Onkologie und Hämatologie, Chronisch-Entzündliche Darmerkrankungen, Systemisch-Entzündliche Rheumatische Erkrankungen und Akute und Chronische Leukämie.

Korrespondenzadresse:

• Prof. Dr. Klaus Pommerening, Institut für medizinische Biometrie, Epidemiologie und Informatik der Johannes-Gutenberg-Universität Mainz, 55101 Mainz
pommerening@imbei.uni-mainz.de

Literatur:

- [1] Pommerening K. Pseudonyme - ein Kompromiß zwischen Anonymisierung und Personenbezug. In: Trampisch HJ, Lange S, Hrsg. Medizinische Forschung - Ärztliches Handeln, 40. München: MMV Medizin-Verlag; 1995. p. 329-33.
- [2] TMF [homepage on the internet]. Berlin: Telematikplattform für die medizinischen Forschungsnetze e. V.; c2004-05 [updated 2005 April 10; cited 2005 April 10]. Available from: <http://www.tmf-ev.de/>
- [3] Reng M, Debold P, Adelhard K, Pommerening K. Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin. Im Druck.
- [4] Semler SC, Lux A, Dolle W, Pommerening K. Pseudonymisierung für Forschungsdatenbanken und Register. In: Jäckel A, Hrsg. Telemedizinführer Deutschland 2005. Ober-Mörlen: Medizin Forum; 2004. p. 209-14.
- [5] Chaum D. Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM*. 1985;28:1030-44.
- [6] Ihle P. Implementierung eines Pseudonymisierungsdienstes für versichertenbezogene Daten der gesetzlichen Krankenversicherung. *Informatik, Biometrie und Epidemiologie in Medizin und Biologie*. 2002;33:350-1.