Generische Datenschutzmodelle für die medizinische Forschung

Peter Debold[1], Carl-Michael Reng[2]

1 Problemstellung

Vernetzte medizinische Forschung

Die Vernetzung medizinischer Forschung wird international mit dem Ziel vorangetrieben, die Forschung auf eine breite Basis zu stellen und ihr hierzu ausreichend große Patientenkollektive verfügbar zu machen. So soll auch die wissenschaftliche Untersuchung seltener Krankheits- und Therapieformen aussagekräftiger werden. Dieses Ziel verlangt, dass Patientendaten nicht nur, wie in traditionellen klinischen Forschungsprojekten, im Rahmen dezidierter Studienprotokolle bereit gestellt werden, sondern dass sie in einem Verbund von Einzelprojekten zusammengeführt und gemeinsam genutzt werden können. Im Vergleich zu traditionellen klinischen Studien erweitert sich auch der Zeitraum der erwünschten Bereitstellung der Daten erheblich, da das Interesse der Nutzung gerade im Hinblick auf das besonders interessante Langzeit-Outcome den Zeithorizont eines Einzelprojektes übersteigt.

Die deutsche Datenschutzkultur definiert für dieses Ansinnen eindeutige Forderungen[3]: Werden Patientendaten nicht nur für die Behandlung, sondern auch für Forschung genutzt, ist das Einverständnis des Patienten zu einer derartigen Nutzung seiner Daten unverzichtbar. Dennoch ist auch ein vorliegendes Einverständnis kein „Freibrief“ zum wissenschaftlichen Datenaustausch und Datenpooling. Die Befugnisse des Behandlungsvertrags, der den Ärzten in der Regel freien Zugang zu personen- und behandlungsbezogenen Informationen innerhalb des Behandlungszusammenhanges gewährt, dürfen auch mit Genehmigung des Patienten nicht bzw. nur unter sehr eingeschränkten Bedingungen auf Dritte übertragen werden. Die einfache Anonymisierung bzw. Pseudonymisierung ist hierbei nicht ausreichend, um den für vernetzte Forschung erforderlichen Freiheitsgrad im Umgang mit klinischen Daten zu erzielen.

Telematikplattform Medizinische Forschungsnetze

Die Förderung von bundesweit agierenden Forschungsnetzen in Deutschland war mit der Einrichtung einer „Telematikplattform für medizinische Forschungsnetze“ TMF - verbunden, in der die Aktivitäten der Netze im Bereich der Informationstechnologie gebündelt und vereinheitlicht werden sollten. Die TMF ist die Interessensgemeinschaft öffentlich geförderter medizinischer Forschungsverbünde und zahlreicher Koordinierungszentren für Klinische Studien in Deutschland. Sie dient der Koordination von Interessen der Forschungsverbünde in der Entwicklung und im Auf- und Ausbau leistungsfähiger IT-Infrastrukturen für die medizinische Forschung[4]. Die Kompetenznetze für die Medizin haben hierbei die Aufgabe, über den bundesweiten Zusammenschluss von Forschungsinitiativen die Expertise in Forschung, Lehre, Entwicklung, Anwendung und Dienstleistung zu bündeln[5], die Koordinierungszentren für klinische Studien sollen vernetzte Strukturen etablieren, welche die Qualität und Effizienz klinischer Forschung verbessern helfen[6]. Besonders schwierig und aufwendig war es bisher für die „Forschungsverbünde in der Medizin“ ein gesetzeskonformes Datenschutz-Konzept zu erarbeiten, das sowohl den Interessen der an der Forschung Beteiligten, den Interessen der klinisch Behandelnden und den legitimen und vorrangigen Interessen der Patienten gerecht wird.

Die TMF entwickelte daher einen Pseudonymisierungsdienst für Forschungsdaten, die in einem eigenständigen Dokumentationsprozess gewonnen werden. Außerdem wurde in einem der Kompetenznetze[7] ein Konzept entwickelt, das die Bereitstellung von Forschungsdaten direkt aus dem Behandlungsprozess heraus zum Ziel hat.

Nachdem die Entwicklungen mit nachhaltiger Unterstützung der Datenschutzbeauftragten aus Bayern und Berlin einen gewissen Reifegrad erreicht hatten, wurde zwischen der TMF, dem Bundesministerium für Bildung und Forschung und dem Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vereinbart, dass diese Datenschutzkonzepte nicht nur als projektspezifische, sondern auch zu generischen Lösungen weiterentwickelt werden sollten. Ziel der Erstellung dieser generischen Lösungen sollte es sein, für die vernetzte medizinische Forschung allgemeingültige, beispielhafte Lösungen zu generieren. So sollte der Aufwand der datenschutzrechtlichen Konzeption für zukünftige Forschungsverbünde gering gehalten und das erforderliche datenschutzrechtliche Prüfungsverfahren schneller durchgeführt werden können.

Das ehrgeizige Vorhaben, Anfang 2002 gestartet, kam im März 2003 zum Abschluss. Nach intensiven Beratungen zwischen den Entwicklern, der TMF und dem AK Wissenschaft wurden zwei auf gemeinsamer Basis entwickelte Modelle verabschiedet, die nun bundesweit anerkannt sind und als Richtschnur für Projekte der vernetzten Forschung gelten können.

Autoren: Peter Debold, Carl-Michael Reng
Titel: Generische Datenschutzmodelle für die medizinische Forschung
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2004
Seite: 214-219

Kap_3_8_TMF_04 neu 214 06.02.2006, 9:38 Uhr

Besondere Rahmenbedingungen für den Datenschutz

Bei der Gestaltung des generischen Datenschutzkonzeptes waren neben vielen komplexen Problemen einige Besonderheiten zu beachten, die in bisher vorliegenden Lösungsansätzen einzelner Forschungsverbünde nur unzureichend Berücksichtigung fanden:

1. Datenschutz in Deutschland ist Ländersache, die zugehörige Gesetzgebung unterscheidet sich von Bundesland zu Bundesland. Zielführend kann daher nur ein Ansatz sein, der alle Landesbeauftragten und den Bundesbeauftragten für den Datenschutz einbindet.
2. Zur einem Datenschutz-Konzept gehören neben technischen Lösungen auch organisatorisch-logistische Lösungen. Diese müssen bereits in einem generischen Konzept bedacht werden, um seinen Nutzern sinnvolle und weitgehende Hilfestellung bieten zu können.
3. Werden medizinische Daten zu Studienzwecken erfasst, so fallen oft gleichzeitig auch Laborproben der teilnehmenden Patienten an, die in speziellen Biomaterial-Banken gelagert werden. Für den Schutz der medizinischen Daten wie auch den der zugehörigen Laborproben ist ein gemeinsames technisches, organisatorisches und logistisches Konzept erforderlich.
4. Die Erfassung von Patientendaten zu Forschungszwecken bedarf der Qualitätssicherung. Ohne die Möglichkeit einer Kontrolle der erfassten Daten auf Richtigkeit und Vollständigkeit ist der Aufbau eines Datenpools für die Wissenschaft wertlos.
5. Die medizinische Forschung kann zu einem Ergebnis führen, das für den Patienten, an dessen Daten bzw. an dessen biologischen Proben dieses Wissen gewonnen wurde, von hohem gesundheitlichem Interesse ist. Es muss möglich sein, einen Patienten über eine solche für ihn wichtige Erkenntnis zu informieren.

Früher entwickelte Datenschutzkonzepte boten besonders im Bereich der Rückführung von Forschungsergebnissen auf den mit der Forschung kooperierenden Patienten nur sehr eingeschränkte Möglichkeiten. Auch wurden Aspekte der Qualitätssicherung der Forschungsdaten und die Bedürfnisse der zur Datenerfassung herangezogenen klinisch tätigen Ärzte nur wenig berücksichtigt[8].

2 Generische Datenschutzlösung Datenfluss und organisatorische Komponenten

Die Vorarbeiten in der TMF und den beteiligten Forschungsverbünden sowie das Studium externer Forschungsstrukturen haben gezeigt, dass es zwar möglich ist, für verschiedene Forschungsszenarien einheitliche Definitionen, Strukturen und Prozeduren zu erarbeiten, dass aber in der Kombination der Prozeduren zwei Ausprägungsvarianten entwickelt werden mussten, um unterschiedlichen Bedürfnissen der Datenerhebung und -prozessierung gerecht zu werden.

In klinisch fokussierten Forschungsnetzen leisten die behandelnden Ärzte die Erhebung und Dokumentation der Forschungsdaten direkt aus dem Behandlungsprozess heraus und wollen auf diese Daten weiter in personenbezogener Form zugreifen. Die Qualitätssicherung ist in den Dokumentationsprozess integriert, so dass dort auch Änderungen bereits erhobener Daten möglich sein müssen. Ort der Dokumentation ist eine netzweit organisierte Datenbank.

In wissenschaftlich fokussierten Forschungsnetzen ist die Dokumentation der Forschungsdaten grundsätzlich unabhängig vom Behandlungsprozess organisiert. Die Qualitätssicherung ist eine zeitlich nachgeordnete Prozedur, die in der Regel von Dritten durchgeführt wird. Erst mit dem Abschluss der Qualitätssicherung werden die Daten in eine netzweit organisierte Datenbank übertragen.

2.1 Klinisch fokussierte Forschungsnetze

In klinisch fokussierten Forschungsnetzen ist die gemeinsame Datenbank den behandelnden Ärzten zugänglich. Sie erhalten ausschließlich Zugriff auf die Daten ihrer Patienten, wobei im lesenden Zugriff auch Daten anderer behandelnder Ärzte und Laborbefunde eingesehen werden können. Bei längerfristiger Betrachtung können dabei auch durchaus Daten verfügbar werden, die nicht mehr mit dem jeweils aktuellen Behandlungsvertrag im Zusammenhang stehen. Diese Lösung kann durch eine Einwilligungserklärung des Patienten abgedeckt werden, der in jedem Fall der Nutzung seiner Daten zu Forschungszwecken zustimmen muss.

Der schreibende Zugriff wird auf die Daten begrenzt, die der behandelnde Arzt selbst einträgt; Änderungen bereits eingetragener Daten werden dokumentiert.

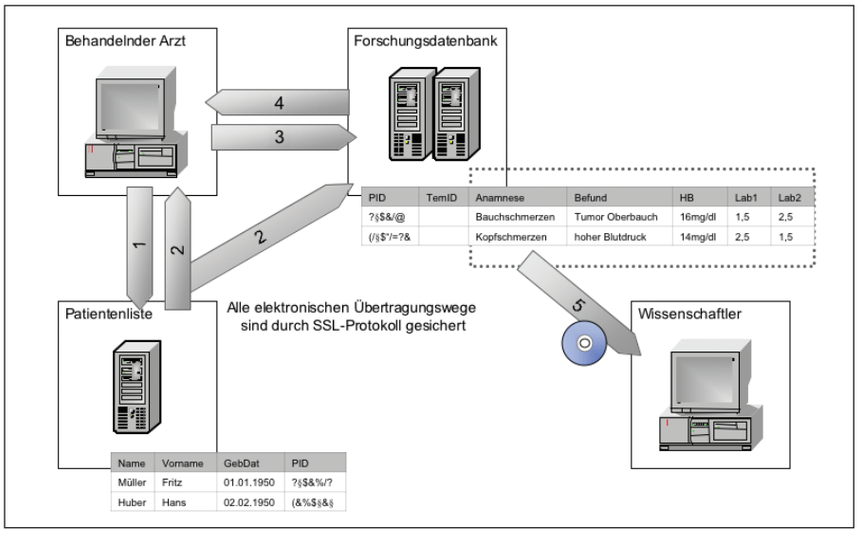

Abbildung 1: *Übersichtsschema zum Datenfluss in klinisch fokussierten Forschungsnetzen*

Kap_3_8_TMF_04 neu 215 06.02.2006, 9:38 Uhr

Die wissenschaftliche Dokumentation wird als integraler Bestandteil in den Behandlungsprozess integriert. Damit kommt die klinisch etablierte Qualitätssicherung direkt der wissenschaftlichen Dokumentation zu gute. Eine aufwendige Doppeldokumentation, die im schmalen Zeitbudget der Klinikärzte meist auch mit Qualitätsrisiken verbunden ist, wird vermieden.

Die zentrale Speicherung der Forschungsdaten mit selektiven Zugriffsrechten für die Ärzte ist so organisiert, dass das Recht des Patienten auf den zuverlässigen Schutz seiner Daten vor unberechtigtem Zugriff auf den Personenbezug in keiner Weise beeinträchtigt werden kann. Dreh- und Angelpunkt der datenschutztechnischen Lösung ist die strikte Trennung der medizinischen Daten und der die Person identifizierenden Daten in zwei Datenbanken, die an verschiedenen Standorten unter getrennter Verantwortlichkeit geführt werden.

Patientenliste

Die Identifikationsdaten der Patienten werden in der sogenannten Patientenliste verwaltet. Der behandelnde Arzt gibt die Daten bei der Erstdokumentation dort ein. Dabei wird auch eine Tabelle erweitert, die den Arzt als Behandler dem Patienten zuordnet. Ist der Patient in der Patientenliste bereits erfasst, wird die Meldung des Arztes auf den vorhandenen Datensatz abgebildet, wo nicht, wird ein neuer Identifikationsdatensatz erstellt. Für jeden Patienten besteht ein (geheimer) Patientenidentifikator PID, der nicht nach außen, sondern lediglich gegenüber der Forschungsdatenbank kommuniziert wird.

Der Zugang des Arztes zur Forschungsdatenbank wird nach Authentisierung[9] über eine Anfrage an die Patientenliste eingeleitet, indem der Arzt die Identifikationsdaten seines Patienten eingibt. Hat der Arzt Zugriffsberechtigung, erhält er eine temporäre ID (TempID), die gleichzeitig von der Patientenliste mit dem geheimen PID an die Forschungsdatenbank übermittelt wird und so den Arzt autorisiert, die Daten einzusehen.

Die in der Patientenliste gespeicherten Identifikationsdaten und der PID werden grundsätzlich nicht nach außen kommuniziert. Die einzige Ausnahme besteht, wenn ein Patient über ein Forschungsergebnis informiert werden soll. Dies bedarf der Genehmigung durch den Ausschuss Datenschutz des Forschungsnetzes. In diesem Fall werden die Identifikationsdaten vom Systembetreuer der Patientenliste dem (zuletzt) behandelnden Arzt übermittelt, der seinerseits den Kontakt mit dem Patienten aufnehmen kann.

Behandlungsdatenbank

Die medizinischen Daten des Patienten sind mit dem geheimen PID als Ordnungskriterium abgelegt. Nach Anfrage eines Arztes bei der Patientenliste wird von dort die TempID zusammen mit dem PID übermittelt; die TempID wird im Datensatz des Patienten für einen Zugriff gespeichert und nach dem Zugriff gelöscht.

Der Arzt meldet sich mit Authentisierung und der TempID bei der Forschungsdatenbank an und erhält lesenden Zugriff auf die Daten des entsprechenden Patienten, für die er eine Zugangsberechtigung besitzt. Zusätzlich erhält er schreibenden Zugriff auf die von ihm selbst erstellten Daten. Der Zugriff auf einen weiteren Patienten bedarf wieder der Autorisierung durch die Patientenliste. Der Vorgang der zweistufigen Anmeldung bei der Patientenliste und der Forschungsdatenbank kann hierbei auf dem Rechner des Arztes automatisiert sein.

Durch die Ablauforganisation, technische Maßnahmen und verpflichtende organisatorische Regelwerke ist sichergestellt, dass zu keinem Zeitpunkt an irgendeiner Stelle abseits des Rechners des behandelnden Arztes identifizierende und Behandlungsdaten gemeinsam verfügbar sind. Nur für den behandelnden Arzt sind beide Datenteile seines Patienten gemeinsam einsehbar und können erweitert und geändert werden. Im Online-Zugriff auf die Datenbank können keine Suchläufe oder Auswertungen durchgeführt werden.

Nutzung der Daten für Forschungsprojekte

Für Forschungsprojekte ist der Zugriff auf Daten aus der Forschungsdatenbank nur offline möglich. Nach einem entsprechenden Genehmigungsverfahren werden die jeweils zutreffenden Daten zu einem definierten Zeitpunkt aus der Datenbank exportiert, wobei die PID als Ordnungskriterium durch einen anderen, nicht sprechenden Identifikator ersetzt werden. Auch für die Bereitstellung von biologischen Proben wurde ein Verfahren entwickelt, das die Weitergabe des geheimen PID und von Identifikationsdaten unnötig macht und sicher verhindert.

2.2 Wissenschaftlich fokussierte Forschungsnetze

Die Lösung für wissenschaftlich fokussierte Forschungsnetze ist zunächst am Beispiel des Kompetenznetzes Rheuma[10] entwickelt und nach der Aufforderung der TMF und des AK Wissenschaft der Datenschutzbeauftragten verallgemeinert worden. Sie sieht ebenfalls die strikte Trennung der Identifikationsdaten in der Patientenliste und der medizinischen Daten in der Forschungsdatenbank vor. Auf der Basis der gleichen Komponenten musste jedoch eine erweiterte Ablauforganisation zugrunde gelegt werden.

Vor Beginn der Dokumentation ist der Patient zunächst mit der Klinik- oder PraxisID in der Patientenliste anzumelden. Zurückgemeldet wird ein Patientenidentifikator (PID), der nicht geheim ist, sondern in der Dokumentation als Ordnungskriterium verwendet werden soll. Die Dokumentation wird mit dem PID, aber ohne Identifikationsdaten der Qualitätssicherung übergeben. Der PID dient hier dazu, zwischen Qualitätssicherung und dokumentierender Stelle den notwendigen Informationsaustausch zu ermöglichen.

Nach Abschluss der Qualitätssicherung werden die Daten von einem weiteren unabhängigen zentralen Dienst pseudonymisiert und von ihm ohne PID an die Forschungsdatenbank übermittelt.

Patientenliste

Die Patientenliste ist ein zentraler Dienst für ein Forschungsnetz, der räumlich, organisatorisch und technisch unabhängig von anderen zentralen Diensten der Gesamtlösung geführt wird. Ein spezifisches Instrument wurde eingeführt, um mit möglichst hoher Sicherheit zu erreichen, dass Patienten, die durch verschiedene behandelnde Stellen gemeldet

Kap_3_8_TMF_04 neu 216 06.02.2006, 9:38 Uhr

werden, auch bei Schreibfehlern, Vornamenvertauschung etc. auf den gleichen Ursprungsdatensatz abgebildet werden und immer der identische PID zurückgemeldet wird. Dieses Instrument wird PID-Generator genannt, der in hoher Komplexität und Funktionstüchtigkeit vom Institut für Medizinische Biometrie, Epidemiologie und Informatik -IMBEI- der Johannes-Gutenberg-Universität, Mainz, unter Prof. Pommerening entwickelt wurde[11].

Der Patient wird dort von der dokumentierenden Stelle nach Authentifikation mit seinen Identifikationsdaten angemeldet; die Patientenliste liefert den PID zurück, ohne dass Informationen übermittelt werden, ob für den Patient bereits ein Datensatz besteht oder neu angelegt wurde.

Es werden grundsätzlich keine Identifikationsdaten nach außen vermittelt; die dokumentierenden Stellen können keine Anfrage stellen. Ausnahmen bestehen nur, wenn nach Genehmigungsverfahren ein Patient über Forschungsergebnisse informiert werden soll oder eine Patientengruppe mit spezifischen Merkmalsausprägungen um die Mitarbeit an weiteren Studien gebeten werden soll. Dafür erhält die Patientenliste eine Liste von PIDs über den Pseudonymisierungsdienst, deren Pseudonyme in der Forschungsdatenbank ermittelt wurden.

Qualitätssicherung

Die Qualitätssicherung ist der zweite zentrale Dienst für ein Forschungsnetz, der räumlich, organisatorisch und technisch unabhängig von anderen zentralen Diensten der Gesamtlösung geführt wird. Die dokumentierende Stelle übergibt die Daten nach Authentifizierung an die Qualitätssicherung. Die Qualitätssicherung prüft zunächst die interne Plausibilität der Daten, hat aber auch die Möglichkeit, aus der Forschungsdatenbank für die betroffenen Patienten zeitlich begrenzt früher erhobene Daten als Kontext für die Plausibilitätsprüfung zu übernehmen. Nach Abschluss der Qualitätssicherung werden die neuen medizinischen Daten dem zentralen Pseudonymisierungsdienst übergeben, der die PID in Pseudonyme umwandelt und die so pseudonymisierten Daten an die Forschungsdatenbank übermittelt. Anschließend werden die neu dokumentierten und die Kontextdaten bei der Qualitätssicherung gelöscht.

Pseudonymisierungsdienst

Der Pseudonymisierungsdienst ist der dritte zentrale Dienst für ein Forschungsnetz, der räumlich, organisatorisch und technisch unabhängig von anderen zentralen Diensten der Gesamtlösung geführt wird. Er übernimmt die qualitätsgesicherten Daten, hat aber nur Zugriff auf den PID in jedem Datensatz, da die medizinischen Daten auf den Empfänger hin – die Forschungsdatenbank – verschlüsselt sind. Der PID wird kryptografisch in ein Pseudonym transformiert und gelöscht, die Daten werden an die Forschungsdatenbank übermittelt.

In Verfahren, die einer Genehmigung bedürfen, findet auch eine Depseudonymisierung statt: Diese Genehmigung gilt mit Sicherheitsauflagen für die Übermittlung von Kontextdaten an die Qualitätssicherung generell, für die Kontaktaufnahme mit Patienten (siehe unten) muss sie im Einzelfall gesondert genehmigt und die Autorisierung in jedem Prozessschritt geprüft werden.

Abgesehen von diesen Prüfungen vor der Einleitung der Depseudonymisierung ist der Pseudonymisierungsdienst eine reine Maschinenfunktion mit hohen Sicherheitsauflagen an die Aufbewahrung des geheimen Schlüssels.

Forschungsdatenbank

Die Forschungsdatenbank, ebenfalls unabhängig von den anderen Diensten geführt, übernimmt die qualitätsgesicherten Daten, entschlüsselt die medizinischen Daten und speichert sie unter dem Pseudonym als Ordnungskriterium.

Sobald nach Empfangsbestätigung die Daten der Qualitätssicherung gelöscht sind, gibt es nur noch die mit dem PID versehenen Daten bei der dokumentierenden Stelle und die pseudonymisierten Daten in der Forschungsdatenbank. Ein Rückbezug von Datensätzen aus der Forschungsdatenbank auf Identifikationsdaten ist nur nach Genehmigungsverfahren und im Einzelfall möglich, z.B. wenn ein Patient über Forschungsergebnisse informiert werden soll. Der direkte Kontakt zum Patienten darf hierbei nur vom behandelnden Arzt aufgenommen werden; Forscher erhalten in keinem Falle Einblick in Identifikationsdaten.

Die Nutzung der Datenbank für die Forschung kann auf verschiedene Weise organisiert werden:

- In der Regel wird die Forschungsdatenbank von Wissenschaftlern betreut, die selbst Auswertungen machen und auch einzelne Datensätze einsehen. Ihnen bleibt das Pseudonym verborgen.
- Externe Wissenschaftler erhalten die Nutzungsmöglichkeit von Daten nur

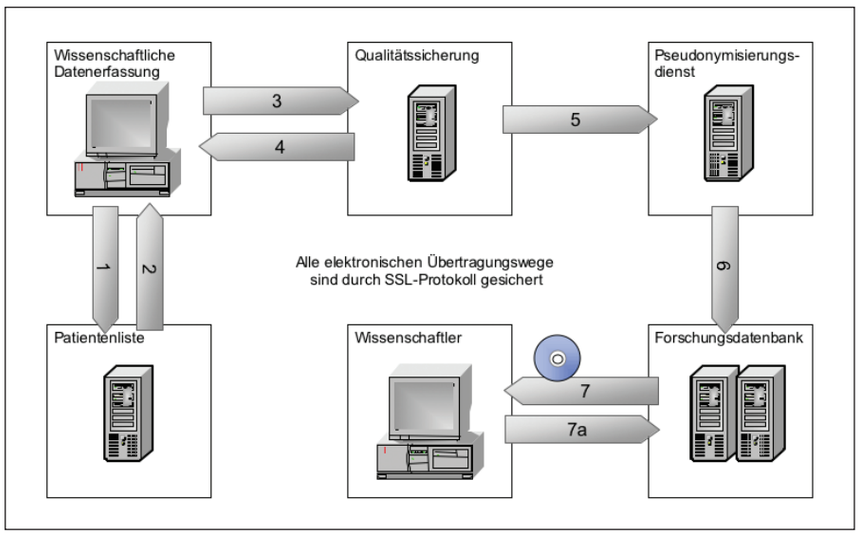

Abbildung 2: *Übersichtsschema zum Datenfluss in wissenschaftlich fokussierten Forschungsnetzen*

Kap_3_8_TMF_04 neu 217 06.02.2006, 9:38 Uhr

nach einem Genehmigungsverfahren. Danach können die zutreffenden Daten entweder exportiert und offline verfügbar gemacht werden, oder die Forscher können Online-Zugriff auf die Forschungsdatenbank erhalten, sofern die Datenbank nach Datenfeldern und Datensätzen differenzierte Zugriffsrechte verwalten kann. In solchen Fällen darf für Forscher keine Möglichkeit bestehen, auf die Pseudonyme zuzugreifen.

3 Gemeinsame Aspekte

3.1 Technischer Datenschutz

Beide generische Lösungen nutzen gemeinsame Komponenten und Verfahren, um die Anforderungen des Datenschutzes von der technischen Seite her sicherzustellen:

Die Datenbanken sollen auf jeweils eigenen, dedizierten Industrie-Standard-Datenbankrechnern liegen. Die originären Sicherheitstechnologien dieser Datenbanken sollen eingesetzt werden, um differenzierte Zugriffsrechte einzurichten und, zusammen mit Firewalls und Intrusion-Detection-Systemen, unbefugten Zugriff zu verhindern. Eigenständige Programmierungen im Sicherheitsbereich sollen völlig vermieden werden.

Jede Kommunikation zur Übertragung von Daten wird ausschließlich mit sicheren Protokollen aufgebaut: SSL oder gleichwertige Protokolle für die Authentifizierung der Kommunikationspartner und die Verschlüsselung der kommunizierten Inhalte (128 Bit und höher). Dies gilt auch für Serververbindungen mit Ein- und Ausgabe-Clients. Eine Migration zu einem höheren Sicherheitsniveau durch die Nutzung von Chipkarten auf der Client-Seite ist grundsätzlich möglich und wird im Kompetenznetz Rheuma, welches die generische Lösung nach 2.2 als erster Forschungsverbund übernimmt, praktisch erprobt werden.

Werden medizinische Daten mit Stellen kommuniziert, die sie nicht selbst verarbeiten müssen, werden zusätzlich zur Transportsicherung diese Teildaten auf den Endempfänger hin asymmetrisch kryptografisch verschlüsselt. Dies ist z.B. der Fall, wenn der Pseudonymisierungsdienst medizinische Daten mit dem PID erhält, aber nur die Aufgabe hat, den PID in ein Pseudonym zu transformieren.

3.2 Rechtliche und organisatorische Regelwerke

Zur Konkretisierung der datenschutzrechtlichen Vorschriften, des Strafgesetzbuches, der Berufsordnung und der sonstigen berufsethischen Normen sind Regelwerke zu schaffen, auf die alle Beteiligten vertrauen können, und woran das medizinisch behandelnde und forschende Personal in der Nutzung der Systeme rechtsverbindlich gebunden wird.

Für eine rechtssichere Umsetzung der Regeln für Datenschutz und Datensicherheit ist es unerlässlich, dass sich ein Forschungsverbund den Status einer juristischen Person gibt. Dies geschieht am Einfachsten durch die Gründung eines Vereins. In dieser Eigenschaft kann er für zentrale Dienste Aufträge vergeben und mit Nutzungsordnungen verbinden, welche die organisatorisch und datenschutzrechtlich relevanten Regelwerke darstellen.

Zur weiteren Konkretisierung bedarf es der Einsetzung eines Ausschusses Datenschutz des jeweiligen Forschungsverbundes, der die Regelung aller mit dem Datenaustausch und dem Datenzugang zusammenhängenden Fragen verantwortet. Diesem Rat kommen folgende fachlichen Aufgaben zu:

1. Bewertung und Bewilligung der Anträge von Wissenschaftlern auf Bereitstellung von Forschungsdaten, welche Ziel, Weg und Datenbedarf darstellen. Mit der Bewilligung ist zu definieren
   - der auf die Forschungsaufgabe zugeschnittene Datensatz,
   - die anzuwendenden Selektionsfilter,
   - der Zugang zu pseudonymisierten oder anonymisierten Daten.
2. Bewertung und Bewilligung von Anträgen auf Übermittlung von Forschungsergebnissen an Patienten durch deren behandelnde Ärzte.
3. Die Beauftragung der zentralen Dienste und die Verabschiedung der Nutzungsordnungen für diese zentralen Dienste, welche die für Datenschutz und Datensicherheit relevanten Regeln enthalten.

Der Verein des Forschungsnetzes schließt Verträge, um die Beteiligten an die Regelwerke zu binden:

1. Mit den dokumentierenden Ärzten und ihren Mitarbeitern zur Festlegung der Anforderung an die Forschungsdaten und ihre Überlassung an den Verein.
2. Mit den Wissenschaftlern zu den Verfahren, die ihnen Zugang zu den Forschungsdaten verschaffen und sie an die regelgerechte Verwendung von Daten und biologischen Proben bindet.
3. Mit den zentralen Diensten zur Regelung der Aufgaben und Pflichten, die mit dem Auftrag zur Datenverarbeitung verbunden sind. In den Verträgen soll auch die Unabhängigkeit von Datenbank-Administratoren vom forschenden Personal sichergestellt werden.

Als weitere Grundlage rechtssicherer Einbindung der datenschutzrechtlich relevanten Vorschriften sind juristische und organisatorische Regelwerke zu schaffen. Sie können in einem Policy-Dokument zusammengefasst werden und betreffen:

- die Satzung des Forschungsverbundes e.V. und seiner Organe, insbesondere des Ausschusses Datenschutz
- die mit den dokumentierenden Ärzten und den Forschern ab zu schließenden Verträge
- die Patienteninformation und Einwilligungserklärung
- die Nutzungsordnungen der zentralen Dienste, mit denen das Sicherheitspotential der technischen Instrumente organisatorisch verankert wird. Für folgende klinikübergreifende Dienste sind die Auftragsbedingungen und Nutzungsordnungen festzulegen, welche die in den vorausgegangenen Kapiteln dargestellten Grundzüge der Maßnahmen zum Datenschutz konkretisieren:
  - Teilnehmerservice zur Beantragung und Verteilung von Zugangskennungen oder SmartCards für die Authentifizierung
  - zentrale Patientenliste
  - Qualitätssicherungs-Service (nur für 2.2)
- Pseudonymisierungsdienst (nur für 2.2)

Kap_3_8_TMF_04 neu 218 06.02.2006, 9:38 Uhr

- Bereitstellung von biologischen Proben
- Führung der Forschungsdatenbank.

Die konkreten Ausprägungen der Regelwerke sollen mit der Einrichtung eines Projekts in einem Forschungsnetz zur Implementation einer Datenschutzlösung detailliert ausgearbeitet werden. Eine „generische" Formulierung ist hier kaum möglich, da die Regeln jeweils auf spezifische organisatorische Bedingungen abgestimmt sein müssen und für die einzelnen Aufgaben konkrete Verantwortliche zu nennen sind. Die Regelwerke, die in diesem Zusammenhang an anderer Stelle für die Kompetenznetze Chronisch Entzündliche Darmerkrankungen und Rheuma entwickelt worden sind, liefern aber eine inhaltliche und methodische Basis . Sie können mit relativ geringem Aufwand an die spezifischen Anforderungen eines anderen Forschungsverbundes angepasst werden.

4 Ausblick

Die vorliegenden generischen Konzepte für den Datenschutz in medizinischen Forschungsnetzen sind von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Arbeitskreis Wissenschaft und im Arbeitskreis Gesundheit und Soziales angenommen worden. Die Landes- und Bundesbeauftragten für den Datenschutz sehen beide Modelle als datenschutzgerechte Konzeptionen an.

Sowohl der AK Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wie auch der Koordinierungsrat der TMF haben Empfehlungen für die Nutzung der generischen Lösungen formuliert. Danach sind die Mitglieder der TMF gehalten, ihre Datenschutzkonzepte, soweit sie noch nicht bewilligt sind, an den generischen Lösungen auszurichten.

Zunächst ist über das Grundkonzept (2.1 oder 2.2) zu entscheiden, das entsprechend den spezifischen Bedingungen des Forschungsnetzes zu wählen ist. Erfordert die Umsetzung der generischen Lösung in die konkreten Strukturen und Möglichkeiten der Organisation der Datenflüsse eines Forschungsnetzes Abweichungen und Ergänzungen, so sind diese Abweichungen zu identifizieren und zu begründen.

In dieser Form soll das Konzept der Arbeitsgruppe Datenschutz der TMF vorgelegt werden. Erst nach positivem Votum der AG Datenschutz soll das Konzept dem zuständigen Landesdatenschutzbeauftragten[12] zur Begutachtung vorgelegt werden. Vernetzte Forschungsvorhaben in der Medizin sollen durch die Verfügbarkeit der generischen DS-Konzepte nachhaltig unterstützt werden. Das langwierige Einarbeiten in die Materie, das oft wenig erfolgreiche Suchen nach geeigneten Lösungsansätzen und die technische und administrative Umsetzung der vernetzten Daten- und Probenprozessierung sollen durch den Einsatz dieser Musterlösungen erheblich verkürzt werden. Mit der TMF steht darüber hinaus eine Organisation zur Verfügung, die in diesen Bereichen der medizinischen Forschung das geeignete Know-how vermitteln und Hilfesuchenden ggf. auch außerhalb der in der TMF organisierten Verbünde beratend beistehen kann, will und soll.

Die generischen Lösungen können mit adäquaten Anpassungen auch in die privatwirtschaftlich organisierte medizinische Forschung übertragen werden. Schließlich birgt vor allem die Lösung für klinisch orientierte Forschungsnetze bei geeigneter Modifikation auch das Potenzial, im Bereich der Regelversorgung die hier ebenso drängenden Datenschutzprobleme lösen zu helfen.

Referenzadressen

Dr. Peter Debold, Debold & Lux
Beratungsgesellschaft für
Informationssysteme und Organisation
im Gesundheitswesen mbH
Reinbeker Weg 61
21029 Hamburg
Tel. 040/7242027
info@debold-lux.com
www.debold-lux.com

Dr. Carl-Michael Reng
Klinik und Poliklinik für Innere Medizin I,
Universität Regensburg
F.-J.-Strauß-Allee 11
93042 Regensburg
michael.reng@medicdat.de

Fußnoten

1 Debold & Lux – Beratungsgesellschaft für Informationssysteme und Organisation im Gesundheitswesen, Hamburg
2 Klinik und Poliklinik für Innere Medizin I, Universität Regensburg
3 M. Bultmann, R. Wellbrock et al., Datenschutz und Telemedizin, Anforderungen an Medizinnetze, 2002
R. Metschke, R. Wellbrock, Datenschutz in Wissenschaft und Forschung, 2. Auflage, 2002 http://www.datenschutz-berlin.de/infomat/heft28/dswi_f_c.htm
4 www.tmf-net.de: Telematikplattform für medizinische Forschungsnetze
5 www.kompetenznetze-medizin.de: Kompetenznetze für die Medizin
6 www.kks-info.de: Koordinierungszentren für klinische Studien
7 Kompetenznetz Chronisch Entzündliche Darmerkrankungen: www.kompetenznetz-ced.de
8 Schulte J, Wehrmann R, Wellbrock R (2002) Das Datenschutzkonzept des Kompetenznetzes Parkinson. Datenschutz und Datensicherheit 26: 605-610
9 jegliche Kommunikation erfolgt geschützt über das SSL-Protokoll oder gleichwertiges
10 www.rheumanet.org
11 http://www.uni-mainz.de/~pommeren/PID/PIDkonzept.html
12 Zuständig ist in der Regel primär derjenige Datenschutzbeauftragte, in dessen Land der Forschungsverbund e.V. bzw. die jeweils verantwortliche juristische Person ihren Sitz hat.

Kap_3_8_TMF_04 neu 219 06.02.2006, 9:38 Uhr