Patientenidentifikation in medizinischen Forschungsverbünden

Pommerening K
Institut für Medizinische Biometrie, Epidemiologie und Informatik, Johannes-Gutenberg-Universität Mainz, Deutschland
pommerening@imbei.uni-mainz.de

Einleitung und Fragestellung Die Identifikation eines Patienten im Behandlungsbereich ist – abgesehen von Betrugsversuchen – unproblematisch: In dem auf Vertrauen begründeten Patienten-Arzt-Verhältnis sind die namentliche Identifikation und eine persönliche Ansprache selbstverständlich und werden auch im zugehörigen Informationssystem verwendet. Sobald Daten des Patienten den engen Behandlungskontext verlassen, entsteht das Problem des Identitätsmanagements für Patienten. So ist im Forschungsbereich der direkte Personenbezug in aller Regel nicht nötig und nicht ohne weiteres erlaubt, der Weg zum Patienten muss aber aus mancherlei Gründen offen gehalten werden. Das schließt die Anonymisierung aus, ist aber durch Pseudonymisierung lösbar. Vergleichbar damit sind andere Arten der Sekundärnutzung der Patientendaten von der Abrechnung erbrachter Leistungen bis hin zur Qualitätssicherung. Die Barrieren, die den Bezug zur Identität des Patienten verhindern sollen, sind die ärztliche Schweigepflicht und die Datenschutzregelungen. Diese können durch Gesetze oder Einwilligungserklärungen überwunden werden, in der Regel aber nur um den Preis zusätzlicher Maßnahmen, wie etwa im Absatz (34) der Präambel der EU-Datenschutzrichtlinie [1] festgelegt.
Material und Methoden Im Behandlungskontext wird die elektronische Gesundheitskarte mit der eindeutigen Versichertennummer künftig als flächendeckendes Identifikationsinstrument dienen. Für den Forschungskontext und andere Arten der Sekundärnutzung von Patientendaten und Proben sind Pseudonyme das geeignete Werkzeug. Damit stellen sich aber organisatorische und logistische Probleme für ein funktionierendes und effizientes Identitätsmanagement. Die Lösungen der TMF für medizinische Forschungsverbünde [2, 3] sehen hierfür zwei vertrauenswürdige Stellen (Trusted Third Parties, TTPs) als organisatorische Einheiten und Teile der Netzarchitektur vor: Den PID-Dienst [4] zur Erzeugung eines Patientenidentifikators (PID) mit Patientenliste für das eigentliche Identitätsmanagement sowie den Pseudonymisierungsdienst, der einen PID durch eine kryptographische Transformation in ein Pseudonym umwandelt, das nirgends sonst auf die Person bezogen werden kann. Das Identitätsmanagement (für Patienten als Datenobjekte, aber auch für IT-Nutzer als Handelnde) ist auch Grundlage für kontextsensitive Zugriffsregelungen, z. B. im Modell A des generischen TMF-Datenschutzkonzepts; letzteres könnte auch die Datenschutzproblematik einer zentralen Datenspeicherung im Rahmen integrierter Versorgungskonzepte oder multizentrischer klinischer Studien mildern, wo die Grenzen zwischen Versorgung und Forschung oft unscharf sind. Ein zusätzliches Problem tritt im Forschungskontext auf, falls keine exakte Identifizierung vorliegt, etwa bei der Zusammenführung von Daten aus verschiedenen Quellen: Hierfür werden Record-Linkage-Methoden eingesetzt, die auch bei fehlerhaften Daten noch eine korrekte Zuordnung ermöglichen können. Neben dem bisher im TMF-PID-Dienst verwendeten deterministischen Algorithmus stehen hierfür auch stochastische Verfahren und andere Methoden des Soft-Computing [5] zur Verfügung. Die TTP-Dienste ermöglichen auch die Rückkopplung aus dem Forschungs- in den Versorgungsbereich durch kontrollierte Depseudonymisierung sowie die Zusammenführung von Daten aus verschiedenen Bereichen.
Ergebnisse Die TMF-Datenschutzkonzepte für medizinische Forschungsnetze [2] und Biomaterialbanken [3] wurden vom Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder positiv beurteilt. Damit stehen datenschutzgerechte Methoden für das Identitätsmanagement von Patienten zur Verfügung, die überall dort eingesetzt werden können, wo der direkte Behandlungsbezug nicht mehr gegeben ist. Diese Methoden wurden in mehreren medizinischen Forschungsnetzen bereits implementiert oder stehen kurz vor der Einführung. Das Kompetenznetz Pädiatrische Onkologie und Hämatologie nutzt den PID-Dienst schon seit 2002, auch zur pseudonymen Kommunikation im Rahmen der multizentrischen Therapieoptimierungsstudien. Inzwischen sind dort fast 47000 Patienten erfasst; die einzigen nennenswerten Probleme waren ca. 20 fälschlicherweise, meistens durch Fehleingaben, erzeugte Synonyme, die durch Eingriff des Systemadministrators aufgelöst werden mussten. Homonyme traten bisher keine auf. Das Kompetenznetz Chronisch-Entzündliche Darmerkrankungen nutzt den PID-Dienst zur patientenabhängigen Zugriffssteuerung in einer pseudonym geführten zentralen Datenbank. Dieses Modell soll bei der bereits begonnenen Revision des generischen Datenschutzkonzepts auch für das zentrale Datenmanagement in multizentrischen klinischen Studien vorgeschlagen werden. In beiden Netzen wird der PID-Dienst organisatorisch unabhängig in einem Klinikrechenzentrum betrieben. Die Kompetenznetze Parkinson und CAPnet nutzen für das Identitätsmanagement (in Form einer Patientenliste) und den Pseudonymisierungsdienst einen Notar als externen Treuhänder. Da dieses mit Kosten und Aufwand verbunden ist, wird immer wieder die Frage nach der Verhältnismäßigkeit solcher Maßnahmen gestellt; sie wird im Datenschutzkonzept für Biomaterialbanken ausführlich behandelt und mit einem Kriterienkatalog versehen und soll auch in bei der Revision des generischen Datenschutzkonzepts entsprechend ausgearbeitet werden.
Diskussion Künftig werden Versorgung und Forschung, insbesondere klinische Forschung und Versorgungsforschung, immer enger verzahnt; auch die TMF und die in ihr vertretenen Forschungsverbünde arbeiten intensiv an diesem Thema. Möglicherweise wird das Identititätsmanagement dann auch insofern vereinfacht, als Pseudonyme durch Verschlüsselung der Versichertennummer erzeugt werden können – je nach Anwendungskontext mit unterschiedlichen Schlüsseln. Allerdings werden die Methoden des Record Linkage ihre Bedeutung nicht vollständig verlieren, da Patienten nicht an allen beteiligten Stellen persönlich mit ihrer Karte erscheinen. Andere Methoden des Identitätsmanagements werden für die medizinische Forschung hinsichtlich der Identifikation von Patienten auch in Zukunft keine Rolle spielen:

- Identitätsmanagement in der Hand der Betroffenen in Form von durch blinde Signatur erzeugten Pseudonymen [6] ist im Kontext medizinischer Anwendungen nicht praktikabel, aber auch nicht erforderlich. Im Abrechnungskontext wurde allerdings von der GMDS-Arbeitsgruppe Datenschutz schon in den Neunziger-Jahren ein pseudonymisiertes Verfahren vorgeschlagen [7], das auf einem Konzept von B. Struif zum elektronischen Rezept beruhte.
- Biometrische Methoden (Fingerabdruck, Gesichtserkennung) dienen eher zur Authentisierung von Teilnehmern an IT-Systemen und sind für Patienten, deren Daten und Proben in Forschungsverbünden verarbeitet werden, nicht nutzbar. Ein Identitätsmanagement durch genetische Fingerabdrücke, die in Forschungsverbünden, zumindest wenn sie auch Biomaterialbanken betreiben, relativ leicht verfügbar sind, kommt aus Datenschutzgründen nicht in Frage, da ein Abgleich mit externen Datenbeständen auf kaum kontrollierbare Weise erleichtert würde.

Als Fazit ist festzuhalten, dass das Modell „pseudonyme Datenbank + separates Identitätsmanagement über organisatorisch unabhängige TTP-Dienste“ für die Zukunft eine bessere Integration von Versorgung und Forschung ermöglichen kann, dabei für ausreichenden Schutz des Patientenrechts auf Vertraulichkeit sorgt und somit ein wesentliches Werkzeug zum Aufbau überregionaler und mehrseitig nutzbarer Informationssysteme mit Patientendaten definiert.
Danksagung Diese Arbeit entstand aus Projekten für die vernetzte medizinische Forschung im Namen der TMF. Diese wurden gefördert vom Bundesministerium für Bildung und Forschung (BMBF). Der Autor nimmt daran als Vertreter des Kompetenznetzes „Pädiatrische Onkologie und Hämatologie“ (KPOH) teil.

Literatur

[1] EU Data Protection Directive. Online: http://www.cdt.org/privacy/eudirective/EU_Directive_.html
[2] Reng CM, Debold P, Specker C, Pommerening K. Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin. München: MWV; 2006.
[3] Becker R et al. Ein generisches Datenschutzkonzept für Biomaterialbanken. TMF 2006, im Druck.
[4] Glock J, Herold R, Pommerening K. Personal identifiers in medical research networks: Evaluation of the personal identifier generator in the Competence Network Pediatric Oncology and Haematology. Submitted for publiction.
[5] Schnell R, Bachteler T, Bender S. A toolbox for record linkage. Austrian J Stat 2004; 33: 125-133.
[6] Chaum D. Security without identification: Transaction systems to make Big Brother obsolete. Communications of the ACM 1985; 28: 1030-1045.
[7] Bleumer G, Schunter M. Datenschutzorientierte Abrechnung medizinischer Leistungen. Datenschutz und Datensicherheit 1997; 21: 88-97.