Das TMF-Datenschutzkonzept für medizinische Datensammlungen und Biobanken

Klaus Pommerening, Johannes Drepper, Thomas Ganslandt, Krister Helbing, Thomas Müller, Ulrich Sax, Sebastian Semler, Ronald Speer

Institut für Medizinische Biometrie, Epidemiologie und Informatik
Universitätsmedizin Mainz, 55101 Mainz
pom@imbei.uni-mainz.de

Medizinische Forschung dient der Weiterentwicklung diagnostischen und therapeutischen Wissens und nützt den Patienten durch Verbesserung der Behandlungsqualität. Nötig dafür sind oft große Mengen an Daten, zunehmend auch Proben und genetische Daten. Allerdings gehören medizinische Daten und Proben zu den sensibelsten persönlichen Informationen und müssen sorgfältig geschützt werden; sie können nicht einfach für Forschungsprojekte zur Verfügung gestellt werden. Besonders hoch sind die rechtlichen Hürden in Fällen, wo ohne Aufbau langfristiger Datensammlungen kaum medizinischer Fortschritt zu erwarten ist, wie z. B. bei seltenen Erkrankungen.

Um zu zeigen, wie medizinische Forschung mit diesen Randbedingungen vereinbar ist, entwickelte die Telematikplattform für medizinische Forschungsnetze (TMF) ein generisches Datenschutzkonzept für die Prozessierung von Daten und Proben in medizinischen Netzen und Biobanken. Die wichtigsten Methoden dafür sind informationelle Gewaltenteilung durch eine verteilte Netzarchitektur, Datentreuhänderdienste, ein auf Pseudonymen basierendes Identitätsmanagement sowie ein organisatorisches Rahmenwerk, das auch Mustervorlagen für Einwilligungserklärungen, Policies und Verträge umfasst. Selbstverständlich sind Datenbanken und Netzkommunikation durch IT-Sicherheitstechnik und kryptographische Verfahren nach dem Stand der Technik zu schützen.

Eine gründliche Revision des Konzepts auf Grund der bisherigen Erfahrungen aus abgeschlossenen und versuchten Implementationen ist zurzeit in Arbeit. Es gruppiert verschiedene Module – Versorgungsmodul, Studienmodul, Forschungsmodul, Biobank – um ein zentrales Identitätsmanagement. Durch diese modulare Netzarchitektur werden insbesondere Komponenten gekapselt, die gleichen rechtlichen Rahmenbedingungen unterliegen. Jeder der Module verwendet eigene Pseudonyme, deren Zusammenführung nur unter kontrollierten Umständen über das Identitätsmanagement möglich ist. Diese Kontrolle wird soweit wie möglich durch technische Verfahren erzwungen; da die technischen Möglichkeiten dafür aber limitiert sind, müssen sie durch weitere Maßnahmen im organisatorischen Bereich ergänzt werden. Insbesondere erfordert das – durch die Detailliertheit der medizinischen Daten bedingte und auch durch noch so gute Pseudonymisierungsverfahren verbleibende – Restrisiko einer Rückidentifizierung Betroffener, dass auch der Zugang zu pseudonymisierten Daten unter Kontrolle bleibt.