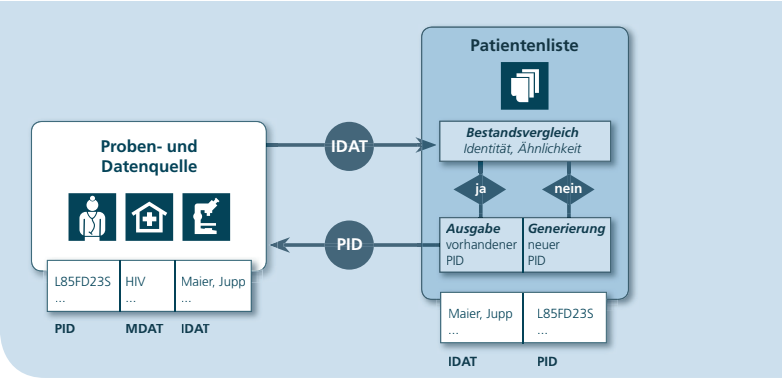
Telematikplattform für
Medizinische Forschungsnetze e. V.

Datenschutz und medizinische Forschung sind vereinbar: Konzepte, Tools und Services der TMF

PID-Generator und Pseudonymisierungsdienst sind die zentralen Komponenten für die technische Umsetzung der generischen Datenschutzkonzepte der TMF. Diese ermöglichen die langfristige Nutzung von Datensammlungen, beispielsweise in zentralen Datenbanken oder Registern, zu denen es über die Datenschutzgesetzgebung hinaus keine spezifischen gesetzlichen Bestimmungen gibt.

Gerade in medizinischen Verbundforschungsprojekten entstehen zunehmend große, qualitätsgesicherte Datenbanken, in denen Daten langfristig und damit auch für die Untersuchung heute noch unbekannter Fragestellungen gespeichert werden. Dies ist jedoch problematisch, wenn die Daten nicht anonymisiert gespeichert werden können, da Datensätze von mehreren Untersuchungszeitpunkten einander zugeordnet werden sollen, oder weil sich aus langfristig gespeicherten Daten zu einem späteren Zeitpunkt individuelle Behandlungskonsequenzen ergeben können. In solchen Fällen muss ein aufwändiges Pseudonymisierungskonzept erarbeitet und – bei verteilter Datenerhebung – oft gleichzeitig mit den verschiedenen Landesbeauftragten für den Datenschutz abgestimmt werden. Pseudonymisierungskonzepte, wie sie im Rahmen gesetzlich geregelter Registerlösungen zum Einsatz kommen, finden dabei oft keine Zustimmung der Datenschützer.

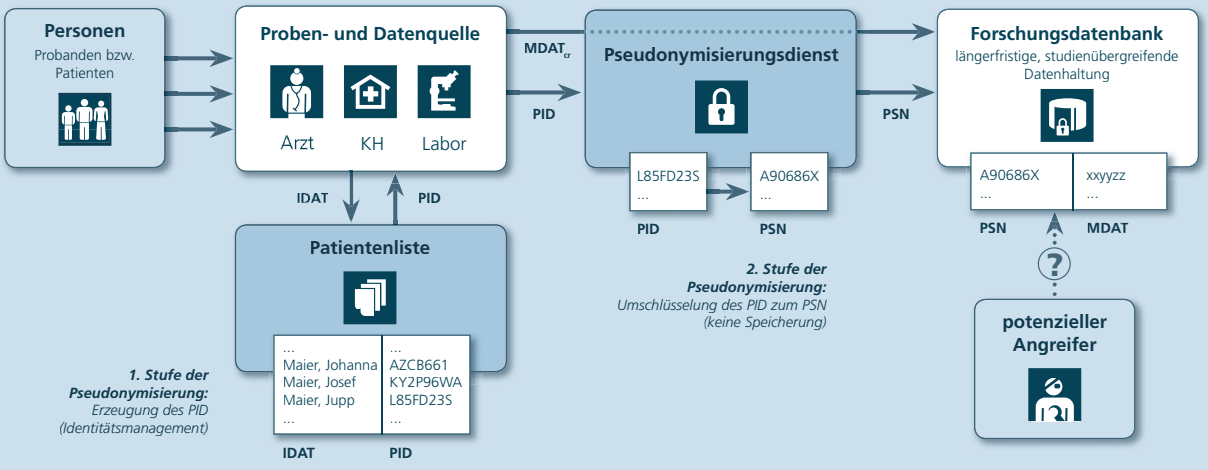


PID-Generator

Generische Datenschutzkonzepte

Die TMF als Dachorganisation für die vernetzte medizinische Forschung hat für solche Anwendungsfälle verschiedene generische Datenschutzkonzepte erarbeitet und mit den Datenschutzbeauftragten des Bundes und der Länder intensiv diskutiert und abgestimmt. Forschungsverbünde können auf dieser Basis eigene Konzepte erstellen und in deutlich vereinfachter Form schneller mit den Datenschützern abstimmen. Die Erfahrungen in der Anwendung der generischen Datenschutzkonzepte werden in der TMF gebündelt und für ihre Fortschreibung genutzt. Ein wesentliches Prinzip ist die informationelle Gewaltenteilung, die dadurch zu realisieren ist, dass der administrative Zugriff auf verschiedene Komponenten und Anteile des Datenbestandes mindestens auf unterschiedliche Organisationseinheiten ohne gemeinsame übergeordnete Weisungsbefugnis verteilt ist. Die Konzepte sind in der TMF-Schriftenreihe veröffentlicht worden (Reng et al.: Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin, Berlin 2006).

Datenschutzkonzept der TMF: Eine zweistufig verschlüsselte ID und die getrennte Haltung von Identifikationsdaten (IDAT) und medizinischen Daten (MDAT) sorgen für größtmögliche Sicherheit bei der Nutzung der Forschungsdatenbank. (PID = einfach verschlüsselter Patientenidentifidator, PSN = Pseudonym, zweifach verschlüsselter Patientenidentifikator)



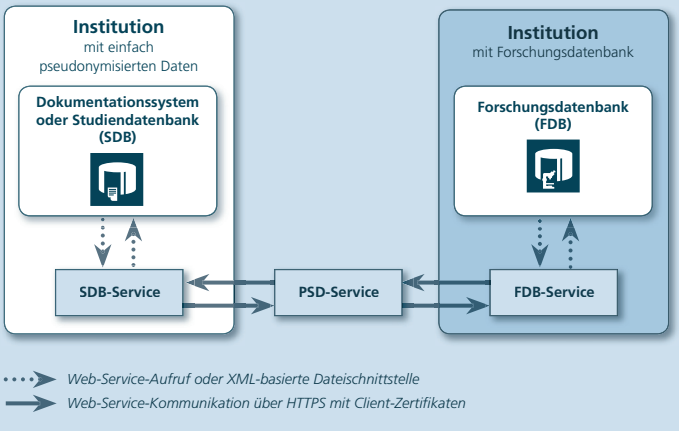
Tools und Services

Wie die generischen Konzepte müssen auch die entsprechenden Tools und Services zur Umsetzung der Konzepte in unterschiedlichen Infrastrukturen einsetzbar sein. Dies erfordert eine modulare Konzeption der technischen Komponenten. Die TMF hat sich für das Paradigma der Service Oriented Architecture (SOA) entschieden. Dies spiegelt auch die umfangreiche Erfahrung der TMF wider: Be stimmte generische Komponenten und damit verbundene Funktionen kommen in verschiedenen Anwendungsfällen und Einrichtungen in gleicher Form, aber unterschiedlichen Konstellationen und Prozessabbildungen zum Einsatz.

PID-Generator

Der PID-Generator ist als erste wichtige Komponente im Gesamtprozess für das Identitätsmanagement zuständig. Hier werden identifizierende Daten der Probanden und Patienten (IDAT) zentral verwaltet, und nichttriviale Pseudonyme erster Ordnung werden generiert und herausgegeben. Um Patientendaten auch bei fehlerhaften Eingaben in unterschiedlichen Softwaresystemen korrekt zuordnen zu können, wurde ein fehlertolerantes Matchingverfahren realisiert, das optimalerweise auf der phonetischen Repräsentation der Daten basiert. All dies bietet der PID-Generator der TMF mit wenigen und einfach nutzbaren Web-Services für unterschiedliche Infrastrukturen und Softwaresysteme. (s. Abb. S. 1, oben)

Pseudonymisierungsdienst der TMF: Es werden spezielle Komponenten (Services) bereit gestellt, die die Signierung und asymmetrische Ver- und Entschlüsselung der medizinischen Daten, wie auch die Absicherung der gesamten Kommunikation übernehmen. Diese Komponenten lassen sich in bestehende Infrastrukturen einfach einbinden: Sowohl der Aufruf einfacher und generischer Web-Services wie auch die Nutzung einer XML-basierten Dateischnittstelle wird unterstützt.



Pseudonymisierungsdienst

Aus Sicht des Datenschutzes ist für langfristig gespeicherte Daten eine zweite Stufe der Pseudonymisierung notwendig. Hierzu dient der eigentliche Pseudonymisierungsdienst (PSD) der TMF, der zwischen einstufig und zweistufig pseudonymisierten Datenbeständen vermittelt. Die zweistufige Pseudonymisierung wird durch eine kartenbasierte, sichere symmetrische Verschlüsselung des einstufigen Pseudonyms erreicht. Die zugehörigen medizinischen Daten (MDAT) werden asymmetrisch verschlüsselt und ohne Entschlüsselungsmöglichkeit für den Pseudonymisierungsdienst selbst durchgereicht. Die datenschutzgerechte Realisierung dieser sensiblen und komplexen Kommunikationsanforderung wird durch das Zusammenspiel von drei Komponenten erreicht. Jede der drei Komponenten stellt die benötigten Funktionen als Web-Services zur Verfügung. Auf der Seite der einstufig pseudonymisierten Datenbestände sind dies z. B. Funktionen zum Abrufen, Pseudonymisieren, Anonymisieren oder Löschen von medizinischen Daten. Wichtig ist, dass alle Komponenten und Funktionen so generisch angelegt sind, dass die eigentlichen medizinischen Daten in beliebigem Format (XML, ASCII, binär) und in beliebiger inhaltlicher Struktur (z. B. CDISC-ODM, -SDTM, HL7) übermittelt werden können.

KONTAKT
Geschäftsstelle TMF e.V.
Neustädtische Kirchstr. 6
10117 Berlin

Telefon +49 (0)30 / 31 01 19 50
E-Mail info@tmf-ev.de
Internet www.tmf-ev.de

Ihre Ansprechpartner:

Johannes Drepper
Telefon +49 (0)30 / 31 01 19 53
E-Mail johannes.drepper@tmf-ev.de

Sebastian Claudius Semler
Telefon +49 (0)30 / 31 01 19 50
E-Mail sebastian.semler@tmf-ev.de

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung