

V039-03 Fortschreibung der generischen Datenschutzkonzepte der TMF

TMF-AG „Datenschutz“ + GMDS-AG DGI

Berlin, 24. März 2011

Prof. Dr. Klaus Pommerening

Universitätsmedizin Mainz, IMBEI

KN Pädiatrische Onkologie und Hämatologie

TMF-AG Datenschutz

GMDS-AG DGI

- „1 Einführung“ und „2 Datenschutzkonzepte der TMF“
in redaktioneller Überarbeitung
- „3 Anwendungsszenarien“:
technische Beschreibung i. w. komplett,
nicht-technische Beschreibung in Überarbeitung.
- „4 Rechtliche und ethische Rahmenbedingungen“ i. w. komplett.
- „5 Module des Datenschutzkonzepts“ fertig.
- „6 Organisatorisches und technisches Konzept
für Forschungsverbünde“ fertig.
- „7 Aspekte der Realisierung“: i. w. komplett.
- „8 Glossar“ i. w. komplett.
- „9 Literatur“ in redaktioneller Überarbeitung
- „10 Anhang“ i. w. komplett.

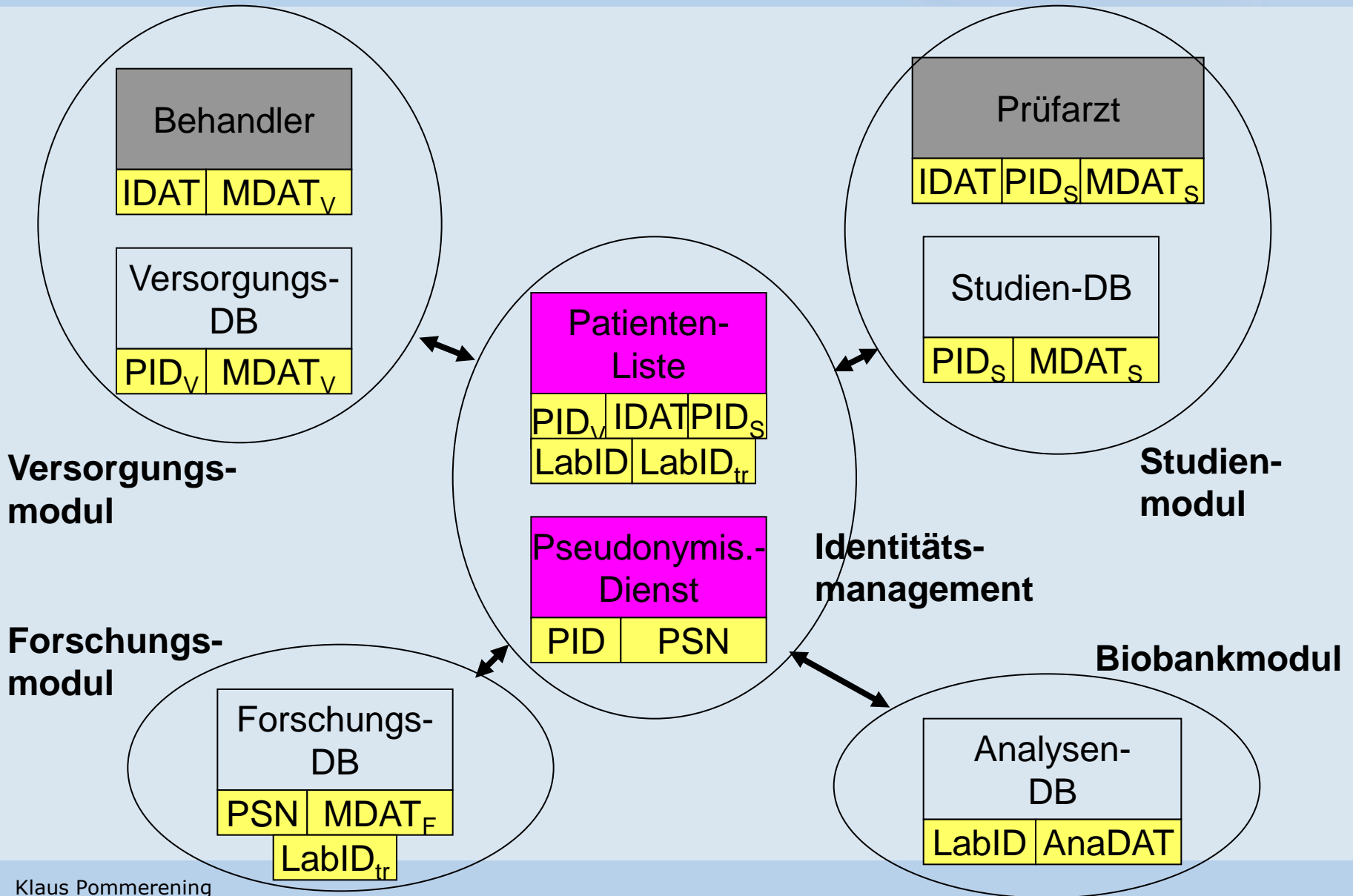
23. 2. 2011 Telefonkonferenz

23. 3. 2011 Besprechung in Berlin

Aktueller Stand: Redaktionelle Überarbeitung

Abstimmung mit AK Wissenschaft anschließend,
noch kein Termin.
Ziel: in 2011.

Revidiertes Datenschutzkonzept: → Neue Strukturen



- ↪ Versorgungsmodul (\approx altes Konzept A)
- ↪ Studienmodul (neu)
- ↪ Forschungsmodul (\approx altes Konzept B)
- ↪ Biobankmodul (= vorhandenes Konzept BMB)

Alle Module verwenden eigene Pseudonyme
(PID_V , PID_S oder SIC, PSN, LabID).

Zentrale Komponenten (auf logischer Ebene):

- ↪ Identitätsmanagement
- ↪ Probandenmanagement (CRM-System)
mit Einwilligungsmanagement
- ↪ Rechtemanagement



Patient-Arzt-Verhältnis

[Behandlungskontext]

[ePA/eGA]

Barriere: Ärztliche Schweigepflicht/ SGB V §291a

[Forschungskontext]



[TMF-Konzepte]

klinische Register,
Versorgungsforschung

klinische Studien

direkte
Erfassung

Register/
epidemiologische Forschung/
Biobanken

- ... bündelt Versorgungsdatenbanken und klinische Register,
- ... enthält Daten, die für die Versorgung des Patienten relevant sind,
- ... steht auch im unmittelbaren Behandlungskontext,
- ... ist aber einrichtungsübergreifend
- ... und wird daher pseudonym (PID) geführt.

Behandler haben einen personenbezogenen Zugriff auf die Daten ihrer Patienten (lesend und schreibend).

Der Zugriff geschieht mit Hilfe der Patientenliste (ID-Management für Patienten) und mit Hilfe eines Verzeichnisdienstes (ID-Management für Benutzer) und Rechtemanagements.

... kann Teil einer ePA-Struktur sein (*Cave*: rechtliche Probleme!),
... kann aber auch unabhängig eine vom Netz geführte
krankheitsspezifische „Teil-ePA“ umsetzen (*Cave*: Aufwand!),
... oder als forschungsorientierte „klinische Datenbank“ im Sinne
des alten Modells A betrieben werden.

An der technischen Umsetzung ändert diese Unterscheidung
wenig.

(Unterschied im Zugriff durch den Patienten selbst bzw. in der
direkten Nutzung der Daten.)



bündelt Studiendatenbanken, die

... zur Durchführung einer (oder mehrerer) klinischer Studien nach den Regularien des AMG und der guten klinischen Praxis (GCP) dienen.

... Daten zum Patienten, die für die Studie relevant sind, enthalten (Überschneidung mit den Daten der Versorgung).

... im unmittelbaren Behandlungskontext stehen, soweit es um Zugriffe durch den Prüfarzt geht;

... im Forschungskontext stehen, wenn es um Zugriffe durch den Sponsor oder Studienleiter geht.

... einrichtungsübergreifend sind

... und daher pseudonym (SIC bzw. PID_S) geführt werden.

Prüfärzte haben einen personenbezogenen Zugriff auf die Daten ihrer Patienten (lesend und schreibend).

... bündelt Forschungsdatenbanken/ epidemiologische Register,
... dient zur Langzeitspeicherung pseudonymisierter medizinischer Daten für spätere Forschungsprojekte

- ↳ direkt zur epidemiologischen Forschung,
- ↳ zur Rekrutierung geeigneter Fälle für neue klinische oder epidemiologische Forschung,
- ↳ zur klinischen Annotation für Biobanken.

... bietet den nochmals pseudonymisierten Export geeigneter Daten

(evtl. je nach Beurteilung des RI-Risikos einen Direktzugriff für Forscher → geplantes Projekt Anonymisierungswerkzeug).

- ↪ Proben werden in Probenbanken gelagert
(mit Proben-Management-DB, organisatorische Daten).
- ↪ Probenanalysedaten in Analysen-DB.
Achtung: Reidentifizierung durch ca. 70 SNPs.
- ↪ klinische Annotation separat (möglichst im Forschungsmodul).

- ↪ Verwaltung der Pseudonyme,
- ↪ Möglichkeit zur Zuordnung zur Identität.
- ↪ Unterstützung des Probanden-/Patienten-Managements (CRM) mit Einwilligungsmanagement.
- ↪ Schnittstellen zu den Modulen, zum Rechtemanagement.

Projektantrag ID-Tools

[Bei Implementation zwischen logischer und physischer Ebene unterscheiden/ Verhältnismäßigkeit]

Redundanz ist wichtiges Grundprinzip bei Sicherheitskonzepten
(**Mehrfachabsicherung**):

Was passiert, wenn eine Sicherheitskomponente ausfällt?

Was passiert, wenn ein Teilnehmer nicht regelkonform agiert?

Verhältnismäßigkeit:

(bedeutet selten: Anpassung eines kontinuierlichen Parameters, sondern meistens ...)

Verzicht auf einige Redundanzen
oder Ersetzung durch „einfachere“ Vorkehrungen

Beispiel: Verlass auf ärztliche Schweigepflicht im Behandlungszusammenhang statt Einsatz einer unabhängigen TTP, wenn „vor Ort“ pseudonymisiert wird.



Größe und Komplexität der Datenbank oder des Netzes,

Dauer der Aufbewahrung,

Brisanz der Daten- oder Biomaterialbank,

↳ z. B. stigmatisierende Krankheit,

Stringenz der Organisation,

↳ z. B. Policies, SOPs, etabliertes Monitoring,

Z. B. notarielle Führung der Patientenliste

↳ bei sehr großem Patientenbestand,

↳ wenn Daten oder Proben attraktiv für Rückidentifizierungsversuche.

↳ Sonst reicht organisatorische Unabhängigkeit.

↳ Unter Umständen reicht auch dezentrale Patientenliste („an der Quelle“) bei getrennter Datenbank-Administration.

Aber: Mangelnde IT-Ressourcen sind kein Verhältnismäßigkeitskriterium.

Netze seltener Erkrankungen:

- ↪ nur Versorgungsmodul,
- ↪ oft mit Biomaterialbank.
- ↪ Beispiele: Skelettdysplasien, Epidermolysis Bullosa.

Große Netze mit allen Modulen:

- ↪ KN Angeborene Herzfehler,
- ↪ KN Pädiatrische Onkologie und Hämatologie,
- ↪ KN Parkinson.

Aufbau eines klinischen „Data Warehouse“,

- ↪ z. Z. aktuelles Thema an vielen Kliniken –
- ↪ eine „Versorgungs-“ (evtl. Forschungs-?) Datenbank, kliniks-
aber nicht abteilungsintern.
- ↪ Einwilligung? Nutzung?