

# Patientenidentifikation in medizinischen Forschungsverbänden

Klaus Pommerening

IMBEI – Universität Mainz

GMDS 2006 – Leipzig



# Patienten-Identifikation



- Behandlungszusammenhang:
  - Identitätsdaten/ persönliche Ansprache
  - künftig: elektronische Gesundheitskarte (eGK)
- Sekundärnutzung von Patientendaten (Forschung, Qualitätssicherung, ...):
  - Anonymisierung oder
  - Identitätsmanagement über Pseudonyme durch vertrauenswürdige Instanzen („Datentreuhänder“, „Trusted Third Parties“ (TTPs))



Behandlungskontext



[Primärnutzung]

Barriere: Ärztliche Schweigepflicht

[Sekundärnutzung/Forschungskontext]

klinische Forschung  
Versorgungsforschung



direkte  
Erfassung

Export erlaubt, wenn  
- anonyme Daten,  
- Einwilligung,  
- Gesetzesvorschrift

Register/  
epidemiologische Forschung

# Identitätsmanagement

**Aufgabe:** Verknüpfbarkeit (Linkability, Traceability) –  
Zuordnung sichern, wo nötig,  
Identität schützen, wo möglich.

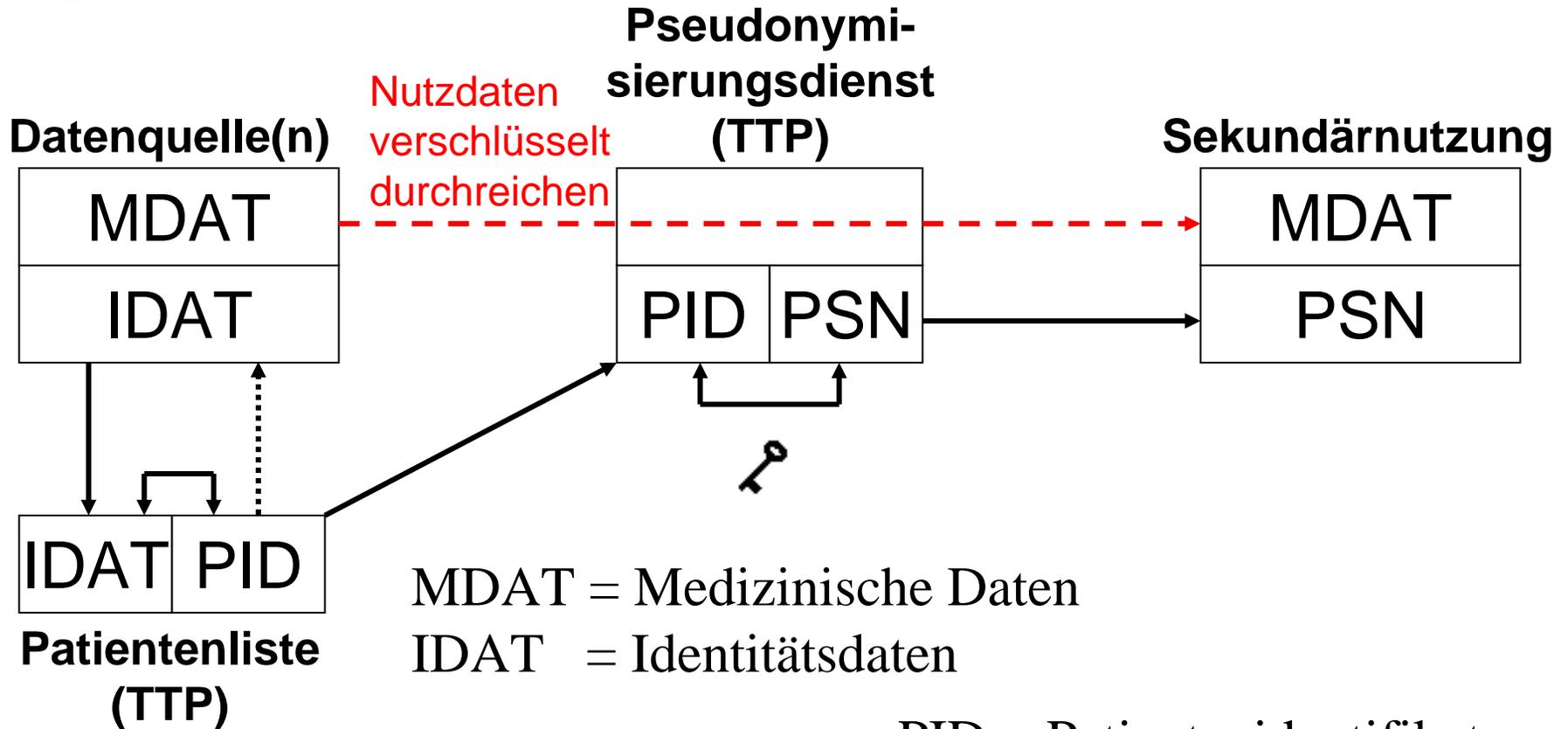
## **Ansätze:**

- Directory/ Verzeichnis [im Berechtigungskontext]
- Master Patient Index [im Behandlungskontext]
- Record Linkage [z. B. in Registern]
- Pseudonyme = kontrollierte Verknüpfbarkeit  
(eigenbestimmt oder über Treuhänder)  
[im Forschungskontext]

# Pseudonyme

- Ersatz der identifizierenden Merkmale durch eine (nichtsprechende) Zeichenkette
  - mit Kontrolle der Rückverknüpfung.
- Indirekter Personenbezug –
  - Selbstverwaltete Pseudonyme oder
  - *Treuhänderlösung mit Einwilligungserklärung*
  - oder gesetzliche Regelung (z. B. Krebsregister).
- In der medizinischen Forschung in der Regel nur die Treuhänderlösung sinnvoll.
  - Pseudonymisierung rechtlich *nicht* äquivalent zur Anonymisierung.
  - Verschiedene Pseudonyme in verschiedenen Kontexten nötig.
- Im eCommerce: selbstverwaltete Pseudonyme,
  - rechtssicher durch blinde Signatur (D. Chaum),
  - lüftbar im Betrugsfall.

# Identitätsmanagement im TMF-Modell B (patientenferne „Forschungsdatenbank“)



MDAT = Medizinische Daten  
IDAT = Identitätsdaten

PID = Patientenidentifikator  
PSN = Pseudonym

# Funktion der Patientenliste

... ist das eigentliche Identitätsmanagement:

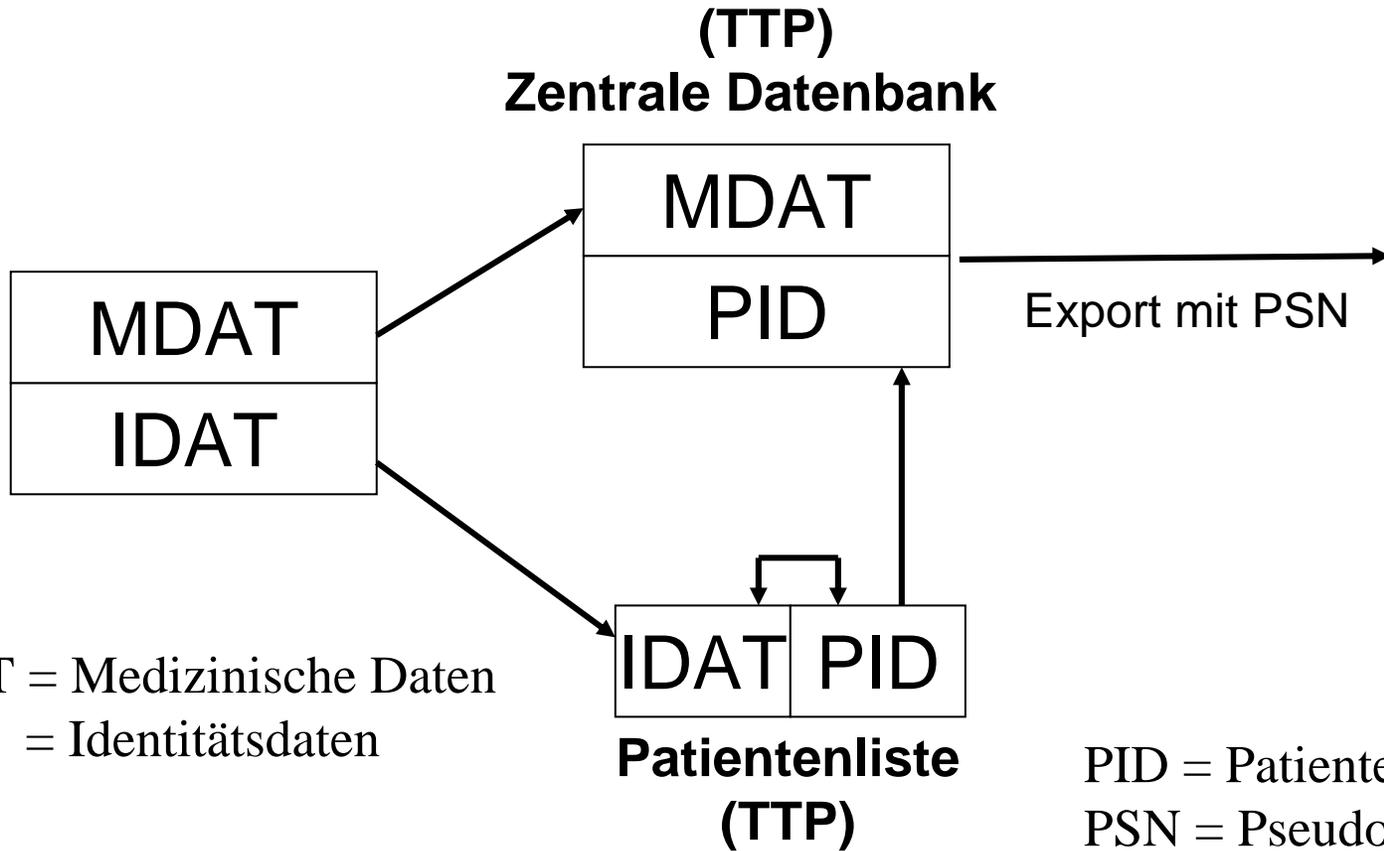
- Eindeutige fehlertolerante Zuordnung von Daten aus verschiedenen Quellen (Matchen, Record Linkage)
  - deterministische, stochastische oder „KI“ Methoden
  - Klassifikationsproblem
- Vergabe eines eindeutigen (nichtsprechenden) Identifikators PID
  - 1. Stufe der Pseudonymisierung
- Mithilfe im Falle einer nötigen Depseudonymisierung
  - z. B. bei Rückkopplung Forschung → Versorgung

# Funktion des Pseudonymisierungsdiensts

- Umwandlung PID zu Pseudonym PSN (kryptographische Transformation)
- Sichere Verwahrung des zugehörigen Schlüssels
- Mithilfe im Falle einer nötigen Depseudonymisierung

*Die Depseudonymisierung wird also technisch durch zwei unabhängige vertrauenswürdige Stellen kontrolliert.*

# Identitätsmanagement im TMF-Modell A (patientennahe „klinische Datenbank“)



# Modell A

- Das Identitätsmanagement dient zur kontextsensitiven Zugriffsregelung.
  - PID nur in Datenbank und TTP bekannt,
  - wird als Pseudonym behandelt.
  - Zugriff über Einmal-Token gesteuert.
- Auch geeignet zur Verbesserung des Datenschutzes bei gemeinsamer Datenhaltung für
  - integrierte Versorgung,
  - multizentrische klinische Studien,
  - Vernetzung von Versorgung und Forschung.

# Stand der Umsetzung

- PID-Generator in
  - Kompetenznetz POH seit 2002 (ca 47 000 PIDs)
  - einigen anderen Netzen in Einführungsphase
- Anwenderworkshop Ende September
- Kompetenznetz Parkinson und CAPnet mit externem Datentreuhänderdienst für Identitätsmanagement
  - Kosten, Aufwand, Verhältnismäßigkeit
  - evtl. zentraler Service durch TMF geplant

# Ausblick und Diskussion

- Das Modell „pseudonyme Datenbank + Identitätsmanagement durch unabhängige TTP“
  - ermöglicht den Aufbau mehrseitig nutzbarer Datenpools,
  - sorgt für ausreichenden Schutz der Patientenrechte.
- Nach eGK-Einführung könnte man als PID verschlüsselte Patientenummer nehmen.
  - Das Problem des Record Linkage bleibt trotzdem.
  - Einheitliches Identitätsmanagement für verschiedene Sekundärkontexte weiterhin nicht erlaubt.
- Revision des generischen TMF-Datenschutzkonzepts in Arbeit –
  - u. a. auch Verzahnung Versorgung/Forschung besser zu berücksichtigen.

# Probleme des Identitätsmanagements

Elektronische Stellvertretung:

- Repräsentant eines Handelnden (oder andere Delegationsbeziehung)
- Eltern für Kind (oder andere Vormundschaftsbeziehung)

Noch keine praktizierten Lösungen für dieses Problem.

- Vollmacht und Widerruf technisch abbilden,
- Notfallregelung.