

Identität und Pseudonym (für Patienten in der medizinischen Forschung)

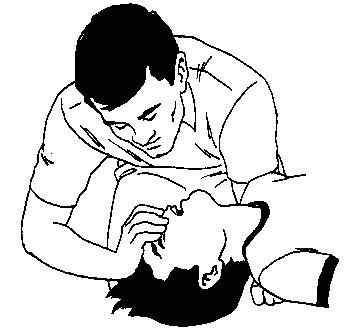
Klaus Pommerening
IMBEI – Universität Mainz
GMDS 2007 – Leipzig



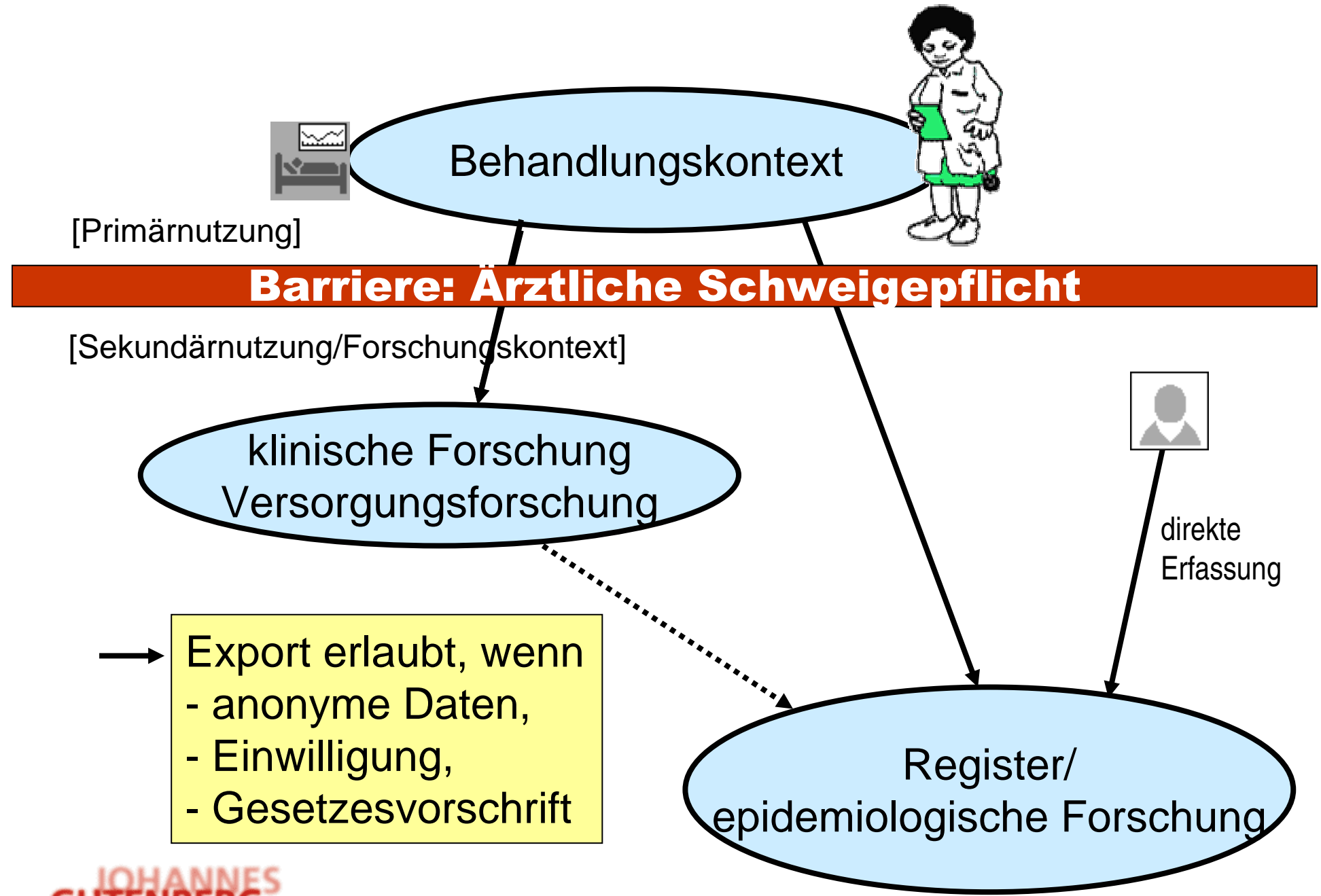
Gefördert vom

Bundesministerium
für Bildung
und Forschung

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))



Identitätsmanagement

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

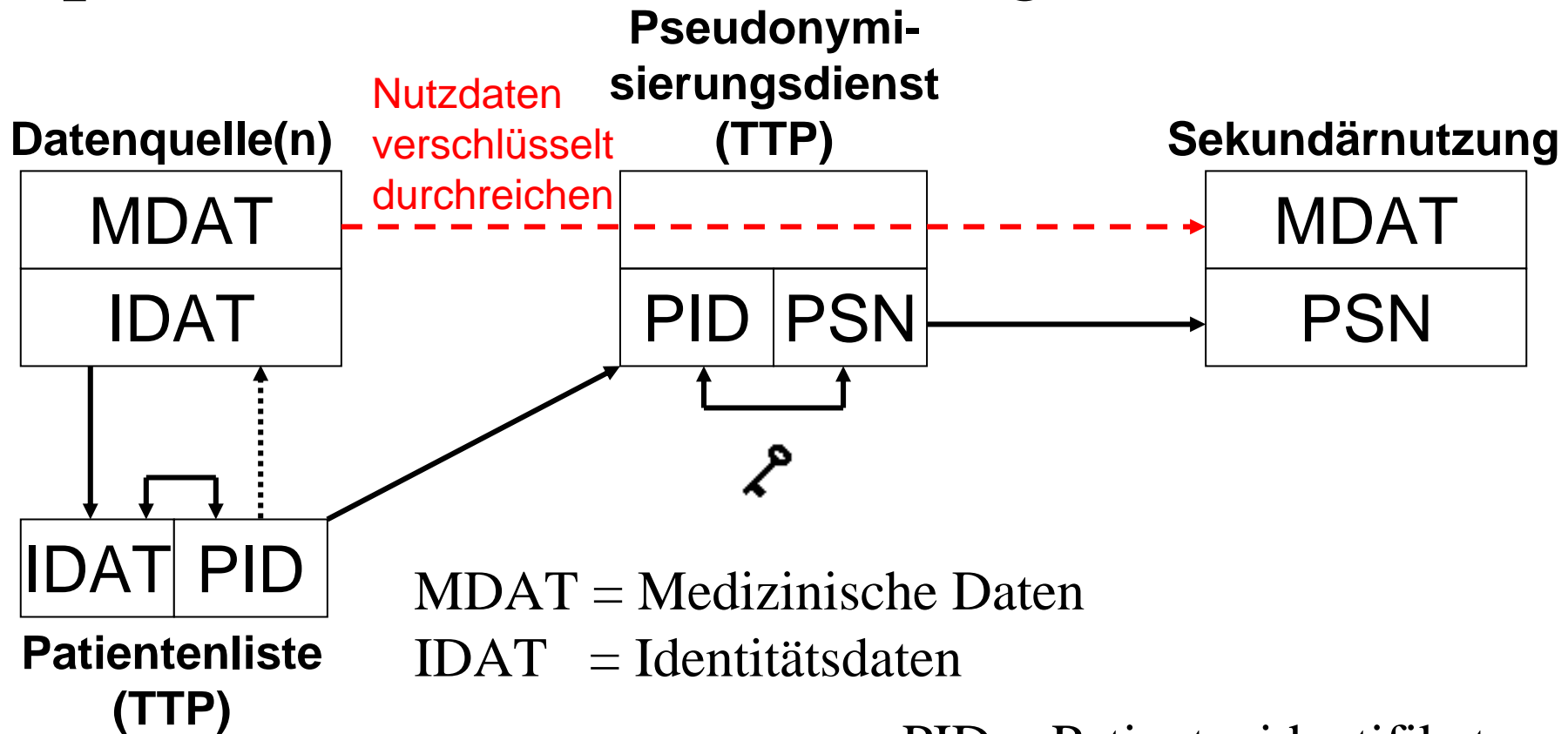
Ansätze:

- 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 Treuhänderregelung (z. B. Krebsregister).
- In der medizinischen Forschung in der Regel nur die Treuhänderlösung sinnvoll.
 - Pseudonymisierung rechtlich *nicht* äquivalent zur Anonymisierung (da prinzipiell rückidentifizierbar).
 - Verschiedene Pseudonyme in verschiedenen Kontexten nötig.

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



MDAT = Medizinische Daten

IDAT = Identitätsdaten

PID = Patientenidentifikator

PSN = Pseudonym

Funktion der Patientenliste

... ist das eigentliche Identitätsmanagement:

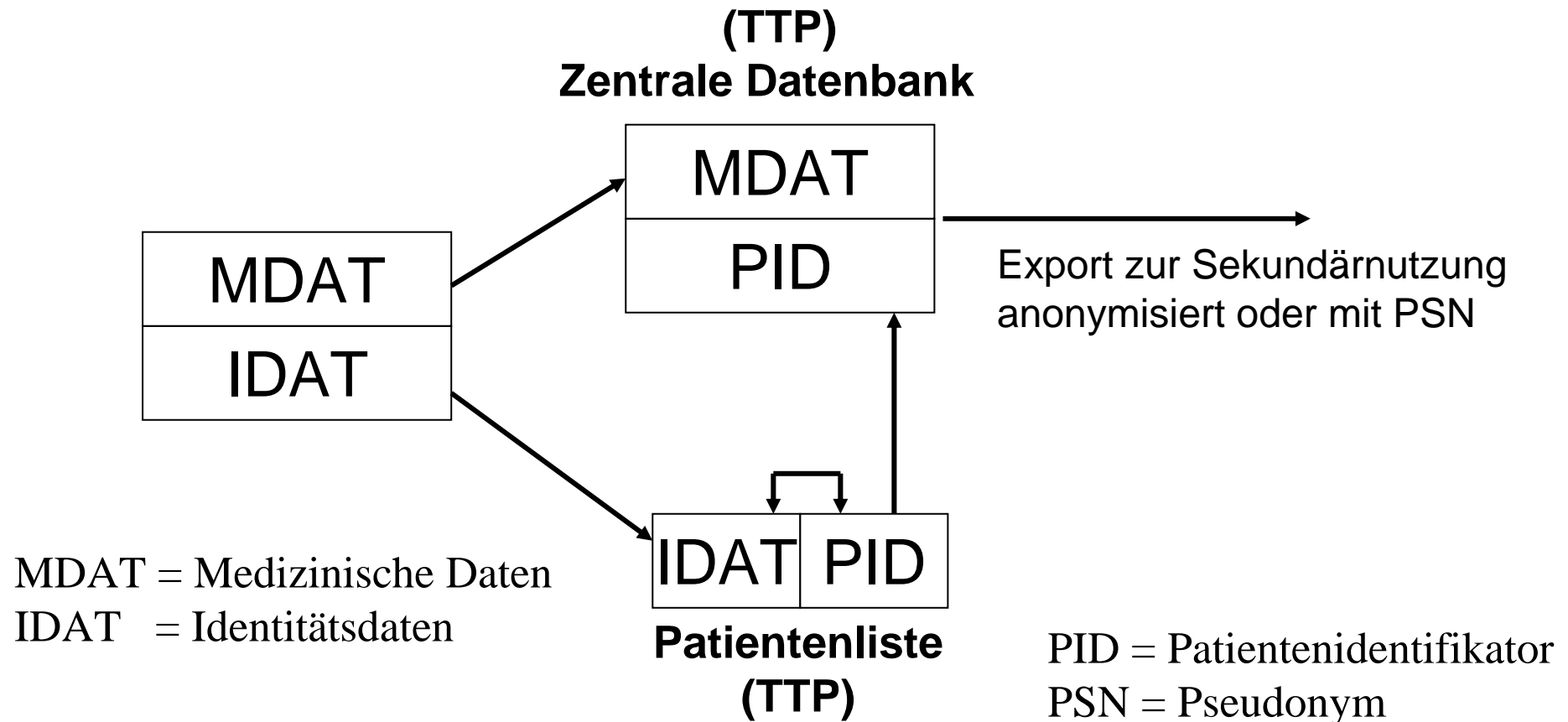
- Eindeutige fehlertolerante Zuordnung von Daten aus verschiedenen Quellen (Matchen, Record Linkage)
 - deterministische, stochastische oder „KI“ Methoden
 - Klassifikationsproblem
- Vergabe eines eindeutigen (nichtsprechenden) Identifikators PID
 - 1. Stufe der Pseudonymisierung
- Mithilfe im Falle 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 von Forschungsdaten wird also im Modell B technisch durch zwei unabhängige vertrauenswürdige Stellen (TTPs) 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 hier 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 52 000 PIDs)
 - einigen anderen Netzen in Einführungsphase
- Kompetenznetz Parkinson und CAPnet mit externem Datentreuhänderdienst für Identitätsmanagement
- Verschiedene Netze nach Modell A oder B im Aufbau
 - Kosten, Aufwand, Verhältnismäßigkeit
 - zentraler Service durch TMF geplant

Ausblick und Diskussion I

- 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 Patientennummer nehmen.
 - Das Problem des Record Linkage bleibt trotzdem.
 - Einheitliches Identitätsmanagement für verschiedene Sekundärkontexte weiterhin nicht erlaubt.

Ausblick und Diskussion II

- Revision des generischen TMF-Datenschutzkonzepts in Arbeit – u. a.
 - Modelle für komplexe Netze mit vielen Datenbanken,
 - Verzahnung Versorgung/Forschung besser berücksichtigen,
 - Übertragbarkeit auf Gesundheitstelematik (lokale Patientenakte, ePA/eGA, Sekundärverwertung von Versorgungsdaten).
- Rechtsgutachten in Arbeit – u. a.
 - Abgrenzung Behandlungskontext/ Forschungskontext, insb. bei patientennaher Forschung,
 - Möglichkeiten zur eGK-Nutzung.

Probleme des Identitätsmanagements für Patienten

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.

Zusammenfassung: Stufen des ID-Managements für Patienten

1. Behandlungskontext

- Speicherung und Zugriff personenbezogen.

2. Patientennahe Forschung – Modell A

- Speicherung pseudonym, Zugriff für *Berechtigte* personenbezogen.

3. Patientenferne Sekundärverwertung – Modell B

- Speicherung und Zugriff pseudonym,
- falls möglich sogar anonym.