Datenschutzkonzepte für Register und Kohorten

TMF-Registertage | Berlin, 22. Mai 2014

Johannes Drepper | TMF-Geschäftsstelle | Berlin

Warum ein Datenschutzkonzept?

Warum ein Datenschutzkonzept?

- Medizinische Forschung ist langfristig auf das Vertrauen von Patienten und Probanden angewiesen
- In Zeiten vermehrter Datenskandale (auch unabhängig vom konkreten Bezug zur Forschung mit Gesundheitsdaten) wird das Gewinnen und Erhalten des Vertrauens immer schwieriger
- Ziel eines Datenschutzkonzepts ist die Balance zwischen der Umsetzung eines angemessenen und realisierbaren Schutzniveaus und möglichst vollständiger Verhinderung von Datenmissbrauch

Warum ein Datenschutzkonzept?

Nach § 4d und § 4e BDSG sind dem Datenschutzbeauftragten zu automatisierten Verarbeitungen u.a. zu melden:

- Verantwortliche Stelle
- Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung
- Betroffene Personengruppen und diesbezügliche Daten oder Datenkategorien
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
- Regelfristen für die Löschung der Daten
- Beschreibung der technischen und organisatorischen Maßnahmen zur Beurteilung der Sicherheit der Verarbeitung

Historie der TMF-Datenschutzkonzepte

2003: Erste generische Datenschutzkonzepte der TMF

- Modelle A + B
- Mit den Arbeitskreisen Wissenschaft und Gesundheit der Datenschutzbeauftragten abgestimmt
- 2006 publiziert als Band 1 der TMF-Schriftenreihe

2006: Generisches Datenschutzkonzept für Biobanken

- Mit dem Arbeitskreis Wissenschaft der Datenschutzbeauftragten abgestimmt
- Auf der Website der TMF verfügbar

2014: Leitfaden zum Datenschutz incl. generischem Konzept

- Skalierbare und modulare Integration von Versorgungs-, Studien-, Forschungs- und BMB-Modul
- Publikation als Band 11 in der TMF-Schriftenreihe geplant

Empfehlung der Datenschutzkonferenz

Die 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg empfiehlt medizinischen Forschungs-einrichtungen und Forschungsverbünden, den von der TMF entwickelten

„Leitfaden zum Datenschutz in medizinischen Forschungsprojekten –
Generische Lösungen der TMF – Version 2“*

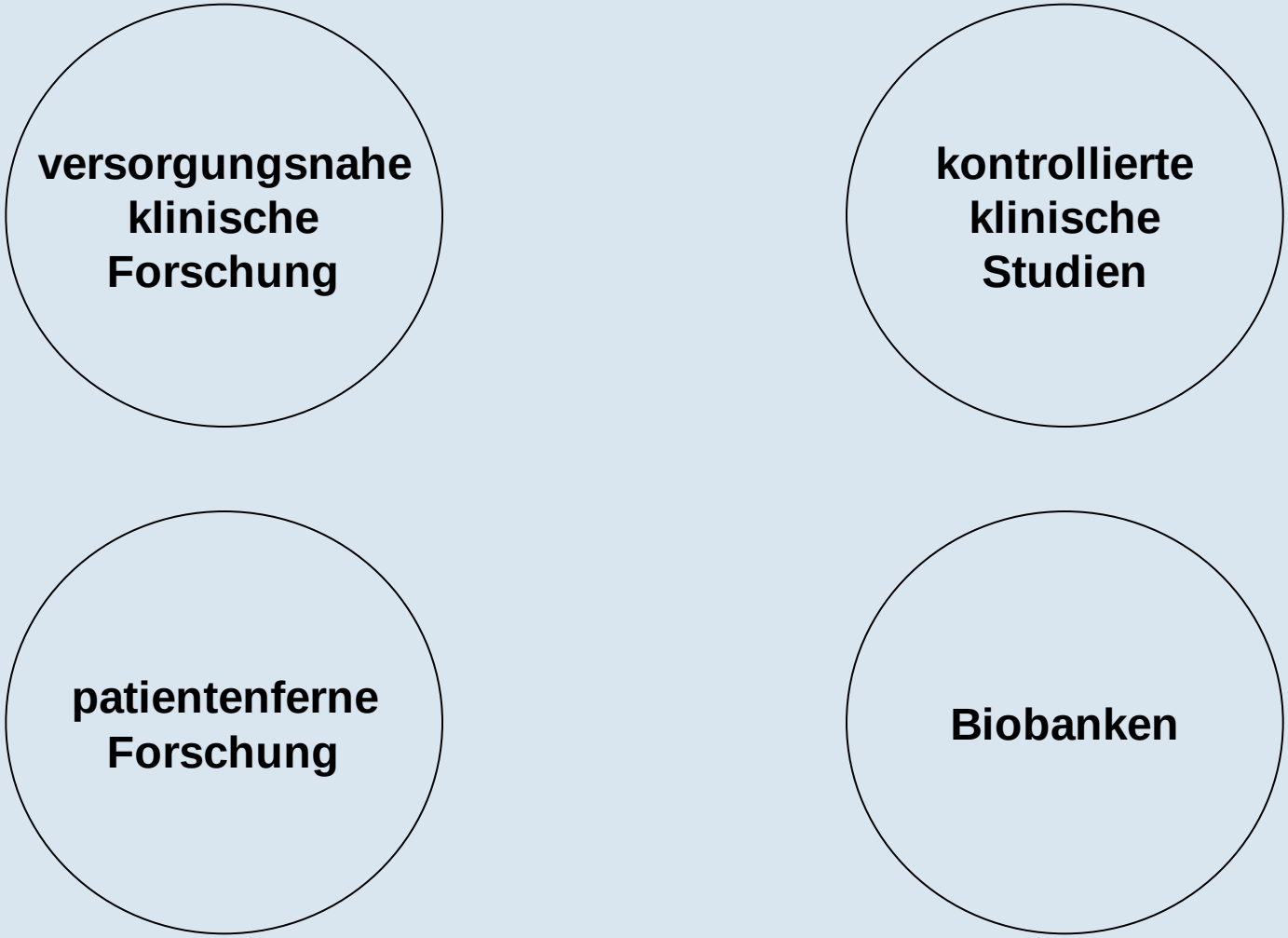
als Basis zu nehmen für die konkrete Ausgestaltung ihrer Datenschutzkonzepte.

* in der Dokumentversion 1.01 vom 5.3.2014

Rechtliche Trennlinien

- Versorgung vs. Forschung
  - Behandlungskontext: identifizierender Zugriff
  - Forschungskontext: pseudonymer Zugriff
- Eng zweckgebundene Forschung vs. „zweckoffene" Forschung
  - Dauer der Speicherung konkret befristet oder nicht
  - nutzender Personenkreis klein oder groß
  - Informiertheit der Betroffenen konkret oder allgemein
  - höheres Risiko bei weniger eng zweckgebundener Forschung muss technisch und organisatorisch ausbalanciert werden
- Daten vs. Proben
  - Reidentifizierungspotential von Proben zu beachten
  - Sachenrecht und Eigentumsverhältnisse bei Proben zu beachten

Bereiche der medizinischen Forschung



Versorgungsnahe Forschung

typisch:
Forschung eng mit
Behandlung verzahnt,
Langzeitaspekt,
offener Forschungsansatz

Beispiele:
Beobachtungsstudien,
klinische Register,
seltene Erkrankungen.

Klinische Studien

typisch:
Regulierung durch Spezialgesetze und -vorschriften, Verzahnung mit Behandlung, Hypothesenprüfung

Beispiele:
AMG-Studien,
MPG-Studien

Patientenferne Forschung

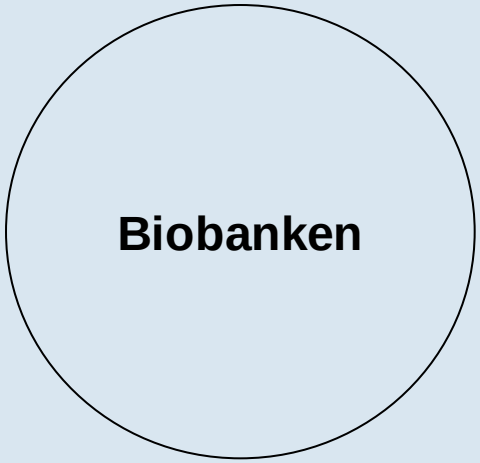
typisch:
keine Verzahnung
mit Behandlung,
Langzeitaspekt,
offener
Forschungsansatz

Beispiele:
epidemiologische
Register,
Kohorten

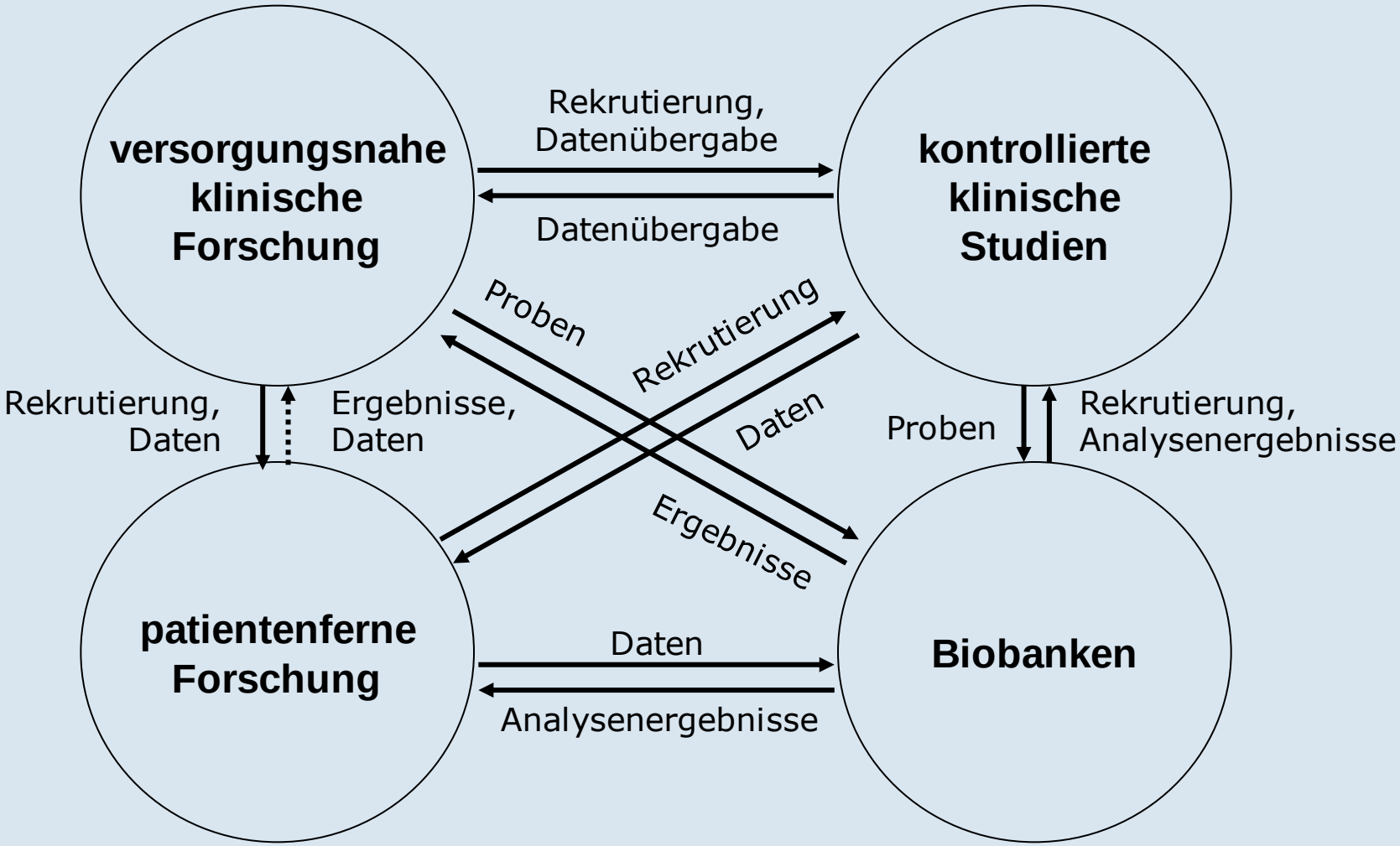
Biobanken

typisch:
Proben u. Annotationen,
Langzeitaspekt,
offener Forschungsansatz,
Betrieb und Nutzung oft getrennt

Beispiele:
krankheits- und bevölkerungsbezogene Biobanken



Beziehungen medizinischer Forschungsbereiche



Was enthält ein Datenschutzkonzept?

Inhalte für ein Verfahrensverzeichnis nach BDSG (§ 4e) oder LDSG:

- Verantwortliche Stelle
- Zweckbestimmung und Rechtsgrundlage
- Betroffene Personengruppen und diesbezügliche Daten oder Datenkategorien
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
- Regelfristen für die Löschung der Daten
- Beschreibung der technischen und organisatorischen Schutzmaßnahmen

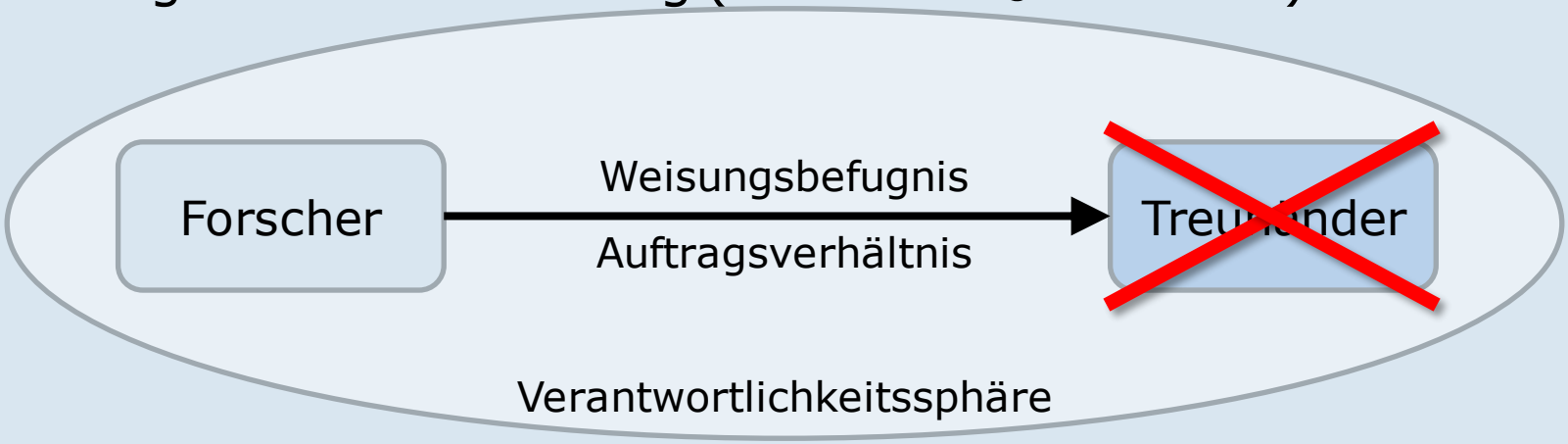
Verantwortliche Stelle(n)

Verantwortlichkeiten festlegen

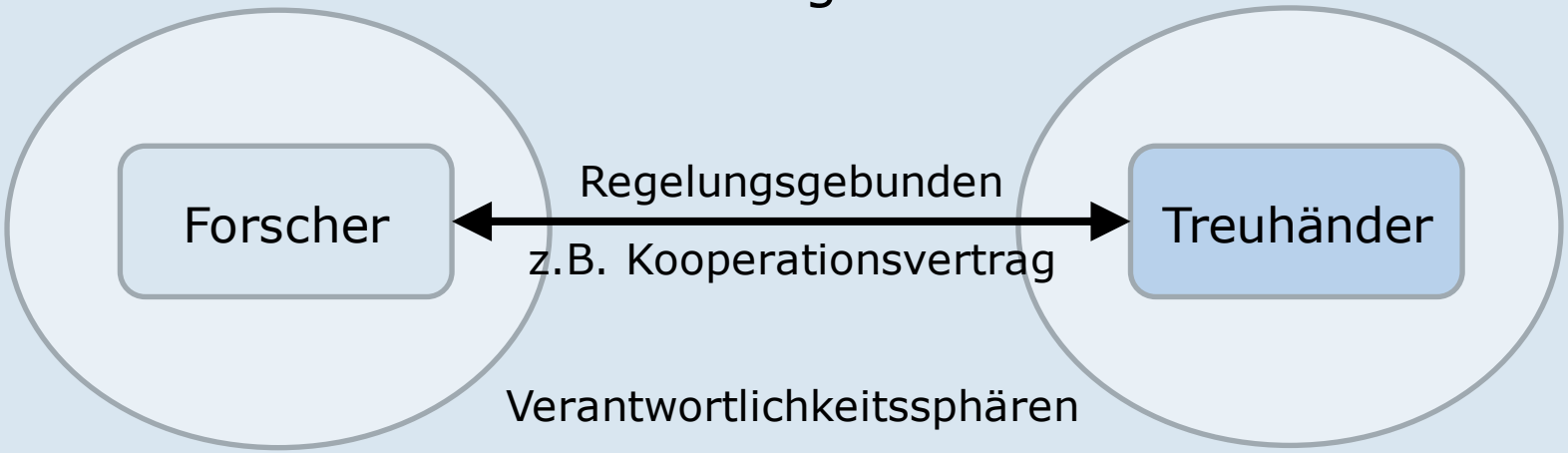
- juristische Person als verantwortliche Stelle festzulegen
- bei Verbund bzw. einrichtungsübergreifender Speicherung und Nutzung ggf. juristische Person zu gründen
- Verantwortungsbereiche zentraler und dezentraler Stellen klären
- bei Förderprojekt auch an Rechtsnachfolge denken (auch relevant für Einwilligungserklärungen)
- Informationelle Gewaltenteilung beachten, je nach Verhältnismäßigkeit
  - Gering: Technische Trennung
  - Mittel: Unterschiedliche Fachabteilungen in einer Klinik
  - Groß: Rechtlich unabhängige Stellen (Treuhänder)

Verantwortliche Stelle(n)

- Auftragsdatenverarbeitung (z.B. nach § 11 BDSG)



- Informationelle Gewaltenteilung



Was enthält ein Datenschutzkonzept?

Inhalte für ein Verfahrensverzeichnis nach BDSG (§ 4e) oder LDSG:

- Verantwortliche Stelle
- Zweckbestimmung und Rechtsgrundlage
- Betroffene Personengruppen und diesbezügliche Daten oder Datenkategorien
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
- Regelfristen für die Löschung der Daten
- Beschreibung der technischen und organisatorischen Schutzmaßnahmen

Zweckbestimmung und Rechtsgrundlage

- Zweckbestimmung immer anzugeben, definiert Erforderlichkeit und Rechtsgrundlage der Datenverarbeitung
- Mögliche Rechtsgrundlagen:
  - Informierte Einwilligung
  - spezialgesetzliche Regelungen (z.B. Krebsregister)
  - Forschungsklauseln der Datenschutzgesetze

- Forschungsklauseln
  - sind in den Landesdatenschutzgesetzen sehr unterschiedlich
  - Kriterien für Wissenschaft u. Forschung beachten
    - ergebnisoffen
    - Publikation der Ergebnisse

Erweiterte Einwilligung

Problem:

- Einerseits gilt das datenschutzrechtliche Schutzprinzip der engen, bestimmten Zweckbindung der Datenerhebung und Verarbeitung
- Andererseits sollen umfangreiche Daten- und Probensammlungen möglichst lange und für möglichst wenig eingrenzbare Zwecke aufbewahrt werden (Langfristigkeit impliziert häufig geringere Zweckbindung)

Kompromisslösung:

- Abgestufte Einwilligungserklärung,
- rechtlich klar geregelte Verantwortlichkeit und
- erhöhter technischer und organisatorischer Schutz gemäß TMF-Datenschutzkonzept

Was enthält ein Datenschutzkonzept?

Inhalte für ein Verfahrensverzeichnis nach BDSG (§ 4e) oder LDSG:

- Verantwortliche Stelle
- Zweckbestimmung und Rechtsgrundlage
- Betroffene Personengruppen und diesbezügliche Daten oder Datenkategorien
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
- Regelfristen für die Löschung der Daten
- Beschreibung der technischen und organisatorischen Schutzmaßnahmen

Personengruppen / Daten (-kategorien)

- Beschreibung der betroffenen Patienten / Probanden
  - Ein- und Ausschlusskriterien etc.
- Beschreibung der Daten und Datenkategorien
  - Hinweis auf besonders schützenswerte Gesundheitsdaten
  - Datensparsamkeit beachten,
    nur erforderliche Daten erheben und nutzen
  - Beschreibung auch für die Einwilligungs-
    erklärung notwendig

Was enthält ein Datenschutzkonzept?

Inhalte für ein Verfahrensverzeichnis nach BDSG (§ 4e) oder LDSG:

- Verantwortliche Stelle
- Zweckbestimmung und Rechtsgrundlage
- Betroffene Personengruppen und diesbezügliche Daten oder Datenkategorien
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
- Regelfristen für die Löschung der Daten
- Beschreibung der technischen und organisatorischen Schutzmaßnahmen

Empfänger / Datenweitergabe

- Projektprüfung und ggf. -zulassung durch „Ausschuss Datenschutz" des Forschungsverbunds
- Kategorien von Empfängern und Freigabeverfahren in Einwilligung aufnehmen
- Datensparsamkeit beachten:
  - Nur die benötigten Daten herausgeben
  - Keine Herausgabe interner, langfristig genutzter Pseudonyme
  - exportspezifische Pseudonymisierung oder Anonymisierung
- verbindliche Vereinbarung mit Empfänger nötig
  - keine weitere Weitergabe
  - keine Dauerspeicherung (kein Restmaterial aufheben)
  - keine Reidentifizierungsversuche.

Was enthält ein Datenschutzkonzept?

Inhalte für ein Verfahrensverzeichnis nach BDSG (§ 4e) oder LDSG:

- Verantwortliche Stelle
- Zweckbestimmung und Rechtsgrundlage
- Betroffene Personengruppen und diesbezügliche Daten oder Datenkategorien
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
- Regelfristen für die Löschung der Daten
- Beschreibung der technischen und organisatorischen Schutzmaßnahmen

Löschen / Anonymisieren

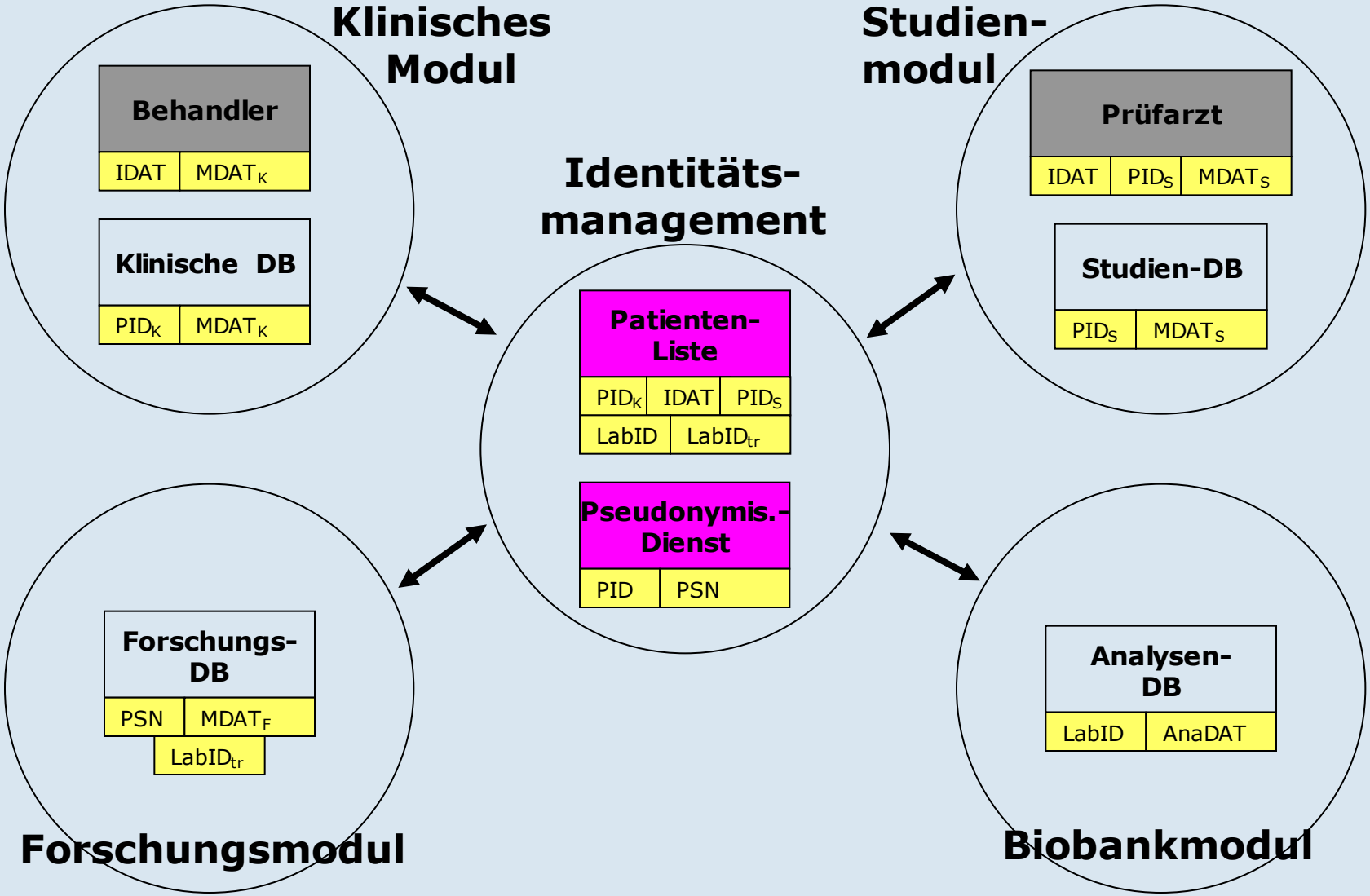
- Prinzip der Erforderlichkeit beachten
  - nur so lange pseudonymisiert speichern, wie z.B. Follow-up zu erwarten oder Rückmeldung an Probanden
  - Dauer der pseudonymen Speicherung ist zu begründen
- begründete Festlegung zu Löschung oder Anonymisierung
- Verfahren ist ggf. auch in der Einwilligungserklärung zu dokumentieren

Was enthält ein Datenschutzkonzept?

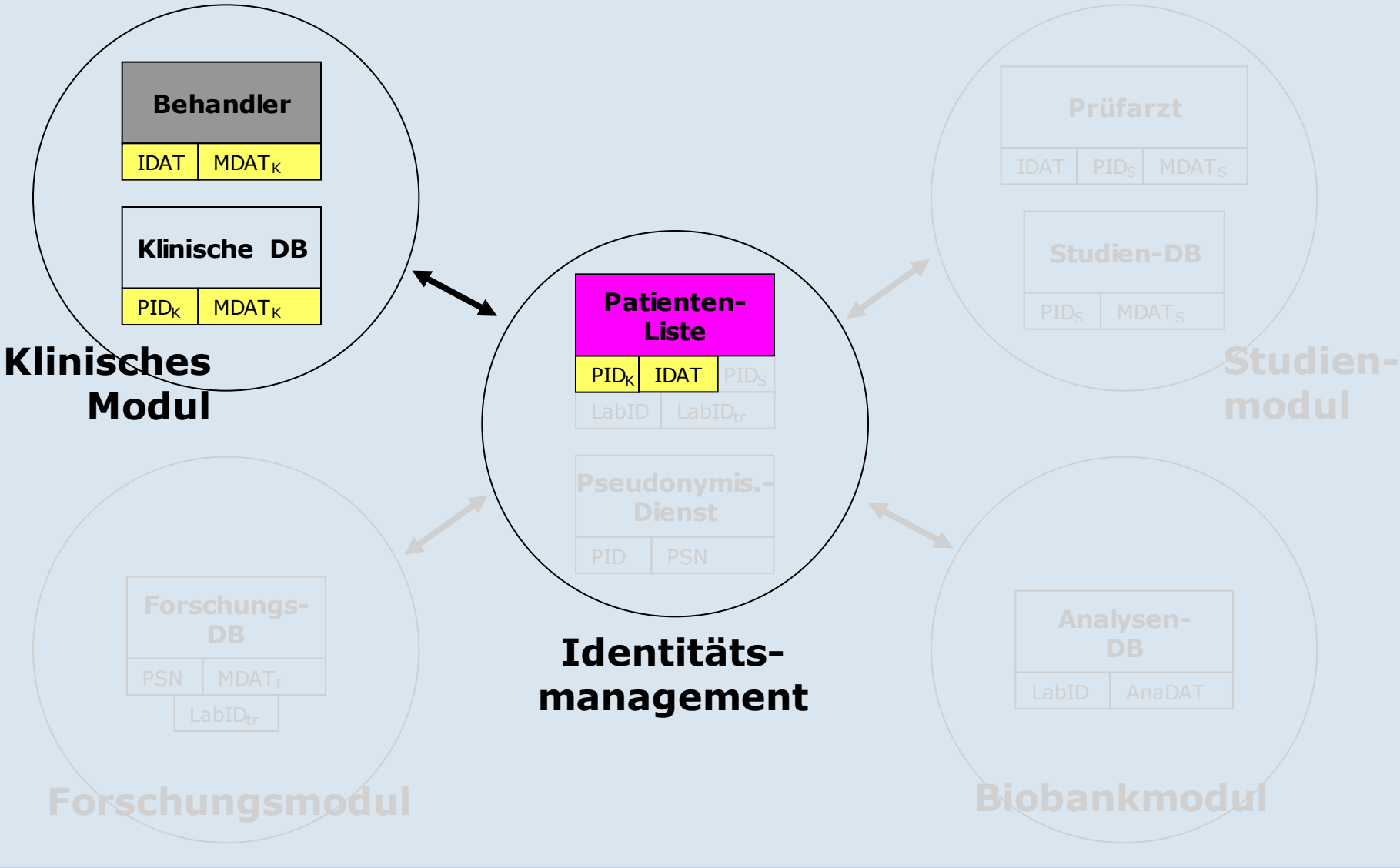
Inhalte für ein Verfahrensverzeichnis nach BDSG (§ 4e) oder LDSG:

- Verantwortliche Stelle
- Zweckbestimmung und Rechtsgrundlage
- Betroffene Personengruppen und diesbezügliche Daten oder Datenkategorien
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
- Regelfristen für die Löschung der Daten
- Beschreibung der technischen und organisatorischen Schutzmaßnahmen

Datenschutzkonzept 2.0



Klinisches Register



Klinisches Register

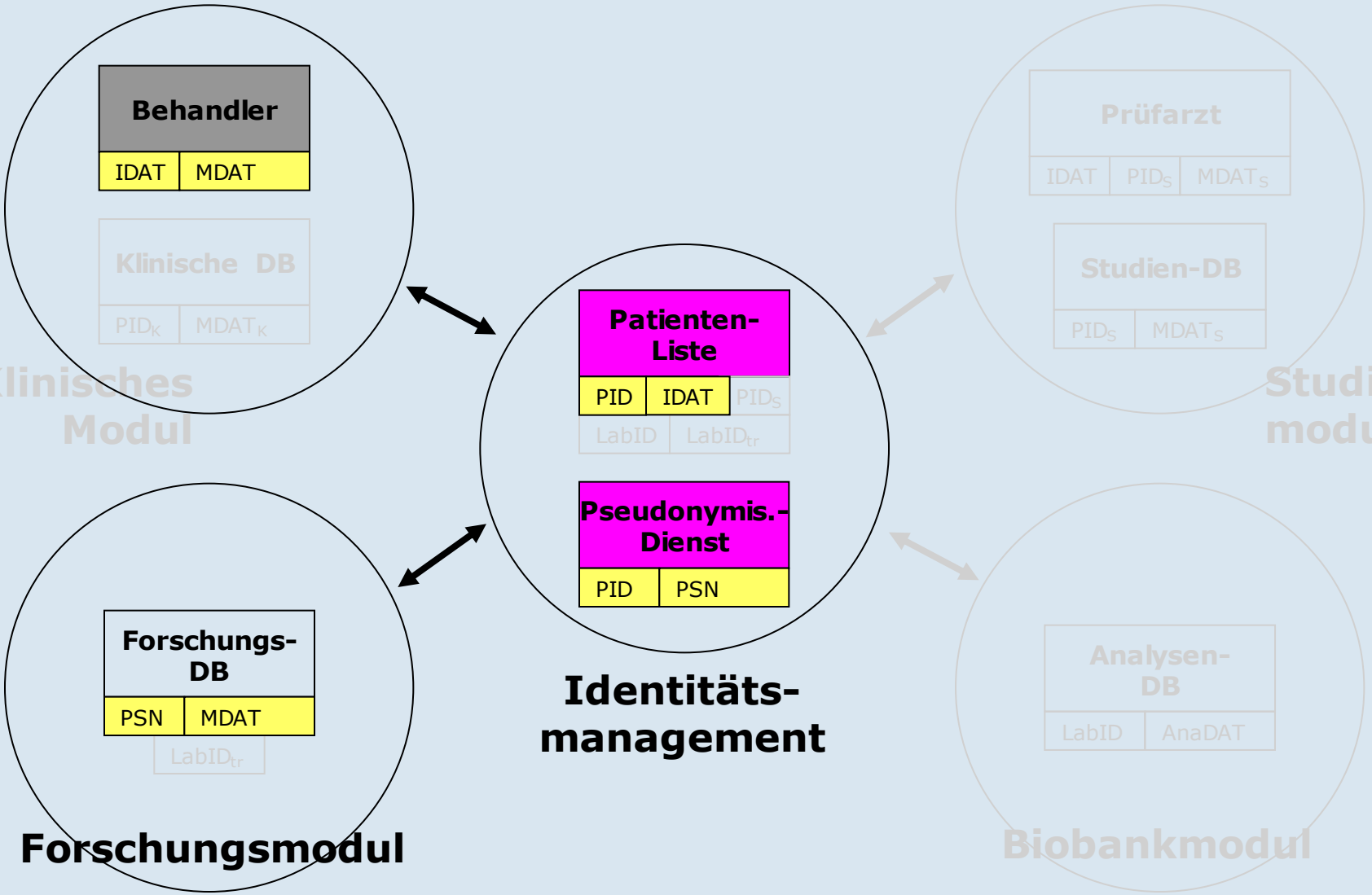
- Versorgungsnahe Datenbank („klinische Datenbank“)
  - Zweck: Forschung im direkten Patientenbezug,
  - Möglicherweise, aber nicht notwendig direkte Rückwirkung auf die Behandlung,
    insbesondere *kein Ersatz für Patientenakte*.
  - Datenqualitätssicherung „an der Quelle“.
  - Ansatz: pseudonyme Speicherung,
    personenbezogener Zugriff für behandelnde Ärzte.
  - Kein Direktzugriff für Forschungsprojekte,
    - statt dessen Datenexport.
- Pseudonym (hier PID genannt) ist nur in DB und TTP bekannt.
- Zugriff über (temporäres) Zugriffsticket geregelt

Klinisches Register

Zusammenführung der identifizierenden (IDAT) und medizinischen Daten (MDAT) nur beim behandelnden Arzt

- technische Anforderungen
  - Zusammenführung im Webbrowser oder
  - Zusammenführung auf Proxy in der behandelnden Einrichtung oder
  - Zusammenführung auf geschütztem Applikationsserver bei TTP

Epidemiologische Register und Kohorten



Epidemiologische Register und Kohorten

- Versorgungsferne Datenbank („Forschungs-Datenbank"),
  - Zweck: Forschung ohne direkten Patientenbezug,
  - Ansatz: Speicherung und Zugriff pseudonym.
  - Vom Client nur Datenübermittlung, sonst kein Zugriff.
- TTP „Patientenliste" sorgt für eindeutige Zuordnung von Daten aus verschiedenen Quellen durch Vergabe eines PID,
- TTP „Pseudonymisierungsdienst" verschlüsselt PID zu PSN.
  - Schlanke TTP, speichert nur Schlüssel.
- MDAT werden (asymmetrisch) verschlüsselt durchgereicht
  - oder über Einmal-Ticket zugeordnet.
- Datenqualitätssicherung erfordert gesonderten Prozess (Rückfragen von Datenbank an Datenquelle),
  - evtl. mit temporärer Depseudonymisierung.

Generische Konzepte – individuelle Beratung

- Generische Datenschutzkonzepte sind mit den Arbeitskreisen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder abgestimmt und werden von der Konferenz als Grundlage empfohlen
- Die AG Datenschutz berät bei der Anpassung der generischen Konzepte an die individuellen Aufgabenstellung von Forschungsverbünden
- Die AG kann bei Bedarf ein Votum für die Abstimmung eines Konzepts mit den lokalen Datenschutzbeauftragten und in besonderen Einzelfällen auch für die Vorabstimmung mit den Aufsichtsbehörden erstellen

Teilnehmer der Sitzung der AG Datenschutz vom 29. Januar 2014

Arbeitsgruppe Datenschutz

Beratung zu Datenschutzkonzepten durch AG DS :

- Seit 2003 über 70 Konzepte diskutiert und beraten, darunter z.B.
  - Kompetenznetze (Rheuma, Parkinson, Hepatitis, ...)
  - Grid- und Cloud-Projekte (PneumoGrid, cloud4health, ...)
  - Register (Deutsches Lipidapherese-Register, Endoprothesenregister Deutschland, ...)
  - Bundesinstitute (PEI, RKI)
  - Biobanken (cBMB der RWTH Aachen, GEPARD, ...)
  - Netze Seltene Erkrankungen (Skelnet, CureNet, ...)
  - Deutsche Zentren der Gesundheitsforschung (DKTK, DZNE, …)
- steigende Nachfrage: in 2014 bereits 10 Beratungen

Weitere Informationen & Kontakt

Geschäftsstelle TMF e.V.
Tel: 030 – 31 01 19 50 | Fax: 030 – 31 01 19 99
info@tmf-ev.de | www.tmf-ev.de

Dr. Johannes Drepper
Tel: 030 – 31 01 19 53
E-Mail: johannes.drepper@tmf-ev.de