

BMB *Projekt*

Datenschutz in Biomaterialbanken Organisatorische und technische Regelungen

Berlin, 7. April 2006

Prof. Dr. Klaus Pommerening

Universität Mainz, KN Pädiatrische Onkologie und Hämatologie

Coautoren: Dr. Regina Becker, Eva Sellge, Sebastian C. Semler

TMF - Telematikplattform für Medizinische Forschungsnetze e. V.





Gesamtprojektleiter:

PD Dr. Michael Hummel
Charité Berlin



Teilprojektleiter Rechtliche Rahmenbedingungen

Prof. Dr. Michael Krawczak
Universität Kiel, NGFN (PopGen)



Teilprojektleiter Datenschutz

Prof. Dr. Klaus Pommerening
Universität Mainz, KN Pädiatrische Onkologie und Hämatologie



Teilprojektleiter Patienteneinwilligungserklärung / Ethik

Peter Ihle
Universität Köln, PMV



Teilprojektleiter Organisation und Qualitätssicherung

Dr. Dr. Michael Kiehntopf
Universitätsklinikum Jena, Kompetenznetz Sepsis (SEPNET)



Externe Gutachter:

Dr. Debold (Hamburg), Prof. Dr. Goebel (Bad Homburg),
Prof. Dr. Simon (Lüneburg)

Projektkoordination:

Dr. Regina Becker
TMF e.V. Berlin,
(seit 01.07. Helmholtz GF)

Sebastian C. Semler

Eva Sellge

TMF e.V. Berlin

Prof. Dr. Goebel

Kanzlei Goebel & Scheller

- ↳ Sammlung von Biomaterialien
 - Organe, Gewebeproben, Blut/Plasma/Serum/Zellen, Extrakte (DNA, RNA)
 - für vernetzte Forschungsprojekte für *unbestimmte Zeit* und *nicht immer vorher bestimmten Zweck* und *Anwenderkreis*:
 - ↳ drei datenschutzrechtliche Hindernisse! (sogar bei Einwilligung)
 - ↳ Dazu noch: Genetische Informationen in Materialien.
 - ↳ Verknüpfung der Proben mit krankheitsbezogenen u. a. Daten

- ↳ BMB sind wesentliche Komponenten medizinischer Forschungsnetze;
 - ↳ aber auch: eigenständige BMB und Probensammlungen in Klinik.

⇒ *Rechtssicherheit dringend erforderlich!*

- ↪ Biomaterial: Träger genetischer Informationen
 - ↪ „Genetischer Fingerabdruck“ charakterisiert Person eindeutig.
 - ↪ Darüber medizinische Daten evtl. auf Person beziehbar,
 - ↪ Informationsdichte nicht verringerbar („Datensparsamkeit“).
- ↪ Ausbalancieren der Grundrechte „Forschungsfreiheit“ und „informationelle Selbstbestimmung“
 - ↪ Ausgestaltung nach Verhältnismäßigkeit
- ↪ Festlegung und Gewährleistung von Verantwortlichkeit:
 - ↪ Träger der BMB, Verantwortliche für Probenlagerung und Datenspeicherung/ -verarbeitung
 - ↪ Prüfung und Genehmigung von Projekten, Datenschutz
- ↪ Datenschutzrelevante Angriffsszenarien auf BMB:
 - ↪ unbefugter Zugriff auf Daten
 - ↪ unbefugte Rückidentifizierung
 - ↪ Zugriff auf Proben (weniger interessant)

- ↪ Offene Konzeption (Dauer, Zweck, Anwender) durch festgelegte Rahmenbedingungen und zusätzliche Sicherheitsmaßnahmen kompensieren.
- ↪ Verbindliche und nachprüfbare Regel- und Vertragswerke.
- ↪ Übergang in Forschungskontext nur anonymisiert oder pseudonymisiert.
- ↪ Minimierung und Kontrolle der Zugriffe.
- ↪ Möglichst vollständige Aufklärung und Einwilligung; Erhalt des Widerspruchsrechts.

↪ Minimierung des Angriffspotenzials durch

↪ technische Maßnahmen:

- ↪ Verschlüsselung, Firewalls, Zugangs- und Zugriffskontrolle, Überwachung, ...

↪ organisatorische Maßnahmen:

- ↪ getrennte Speicherung / Lagerung
- ↪ Trennung der Verantwortlichkeiten („Mehraugenprinzip“)
- ↪ Verpflichtungen, Selbstverpflichtungen, vertragliche Regelungen, verbindliche SOPs, Einwilligungserklärung

↪ Werkzeuge:

- ↪ Informationsteilung
- ↪ Zugriffskontrolle
- ↪ Pseudonymisierung

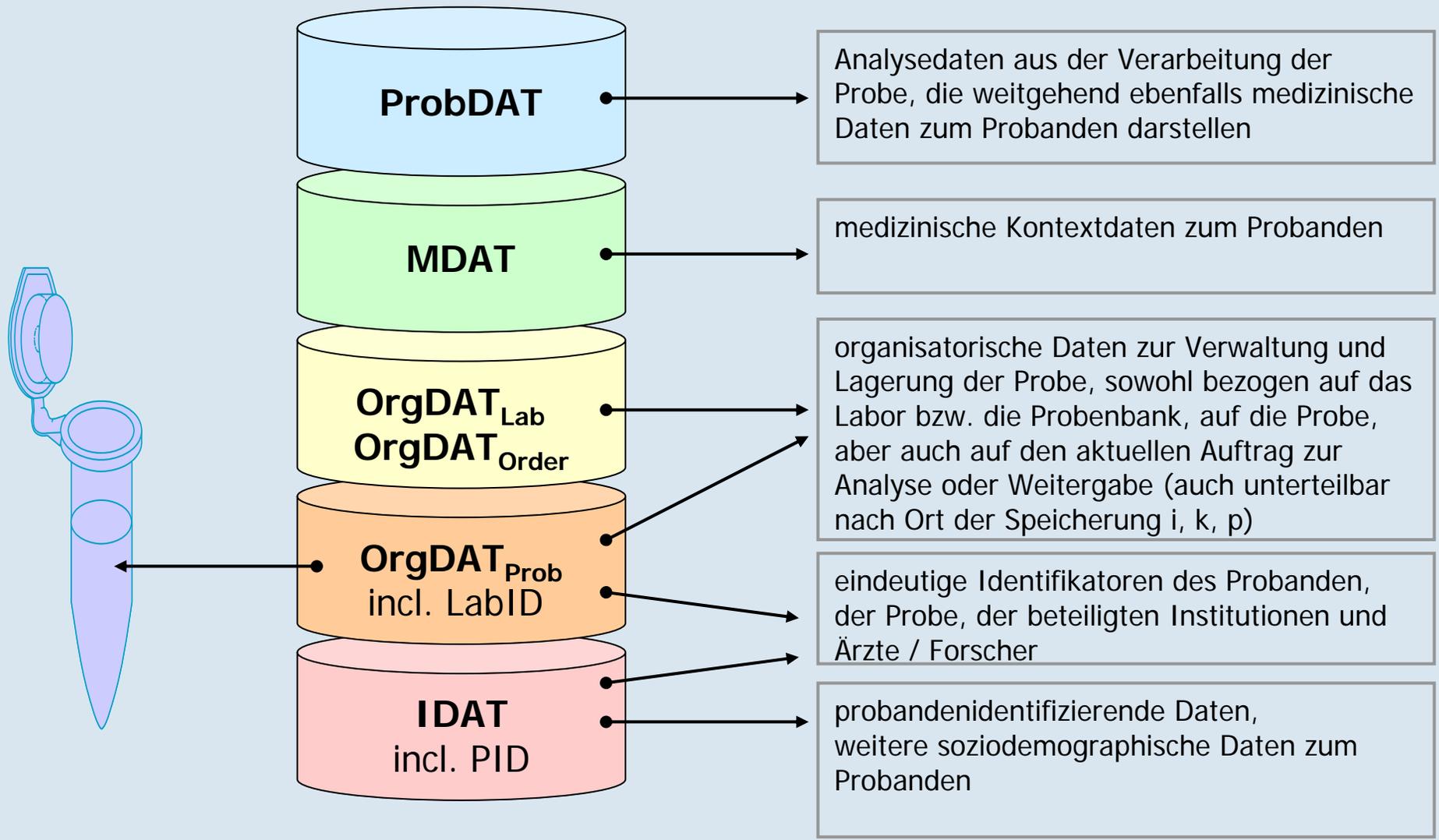
Anlehnung an das „generische Datenschutzkonzept“ der TMF, aber auch Berücksichtigung „kleiner“ BMB

Varianten:

- ↪ BMB als Teil einer Klinik o. ä.
- ↪ eigenständige BMB
- ↪ BMB in Forschungsnetz (nach Modell B des generischen TMF-Datenschutzkonzepts – Forschungs-DB)
- ↪ BMB in Forschungsnetz (nach Modell A des generischen TMF-Datenschutzkonzepts – zentrale klinische DB)

Kategorien:

- ↪ Modell 1 („zentral“)
- ↪ Modell 2 („dezentral“)
- ↪ Modell 3 („kooperativ“)
- ↪ Modell 4 („Vermittler“)



Prinzipieller Ansatz:

1. getrennte Speicherung / getrennte Verantwortung

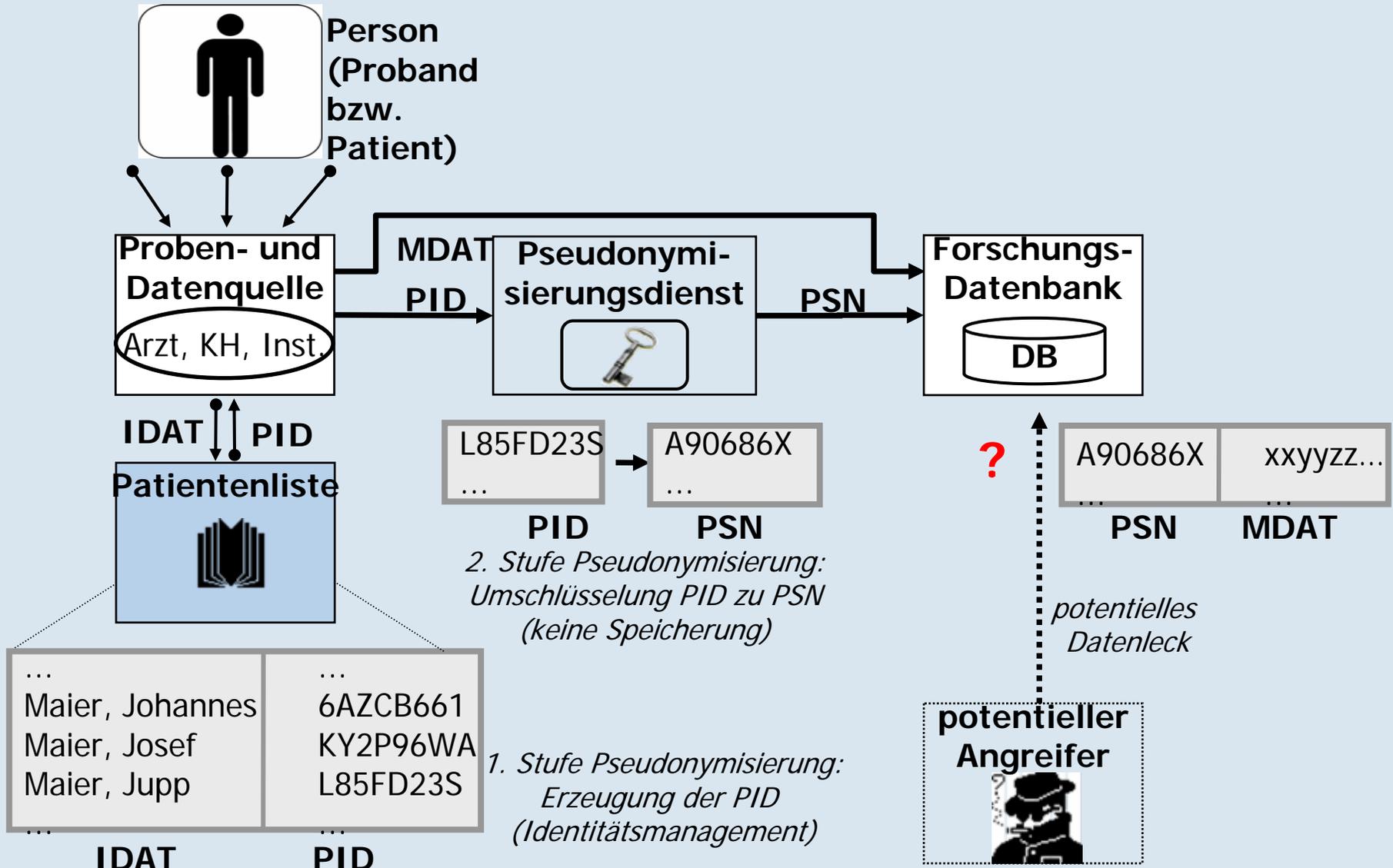
IDAT – MDAT – Probe/OrgDAT – ProbDAT

2. Zuordnung über verschiedene Pseudonyme

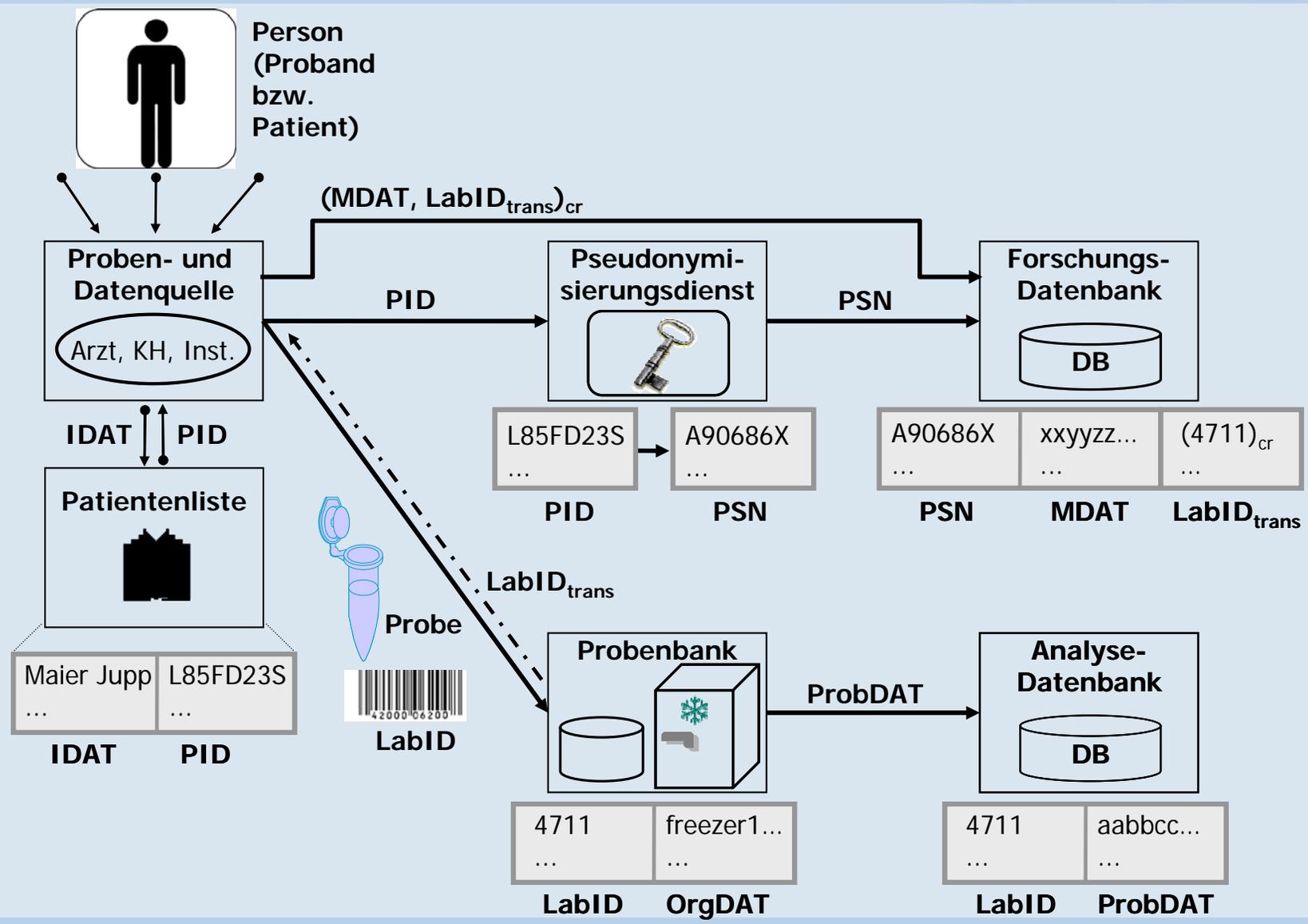
PID – PSN – LabID – LabID_{trans}

3. Anonymisierung oder zusätzliche Pseudonymisierung beim Übergang
zentrale Datenbank/ Probenbank → Forschung

4. Evtl. Vereinfachungen nach Verhältnismäßigkeit (s. u.).

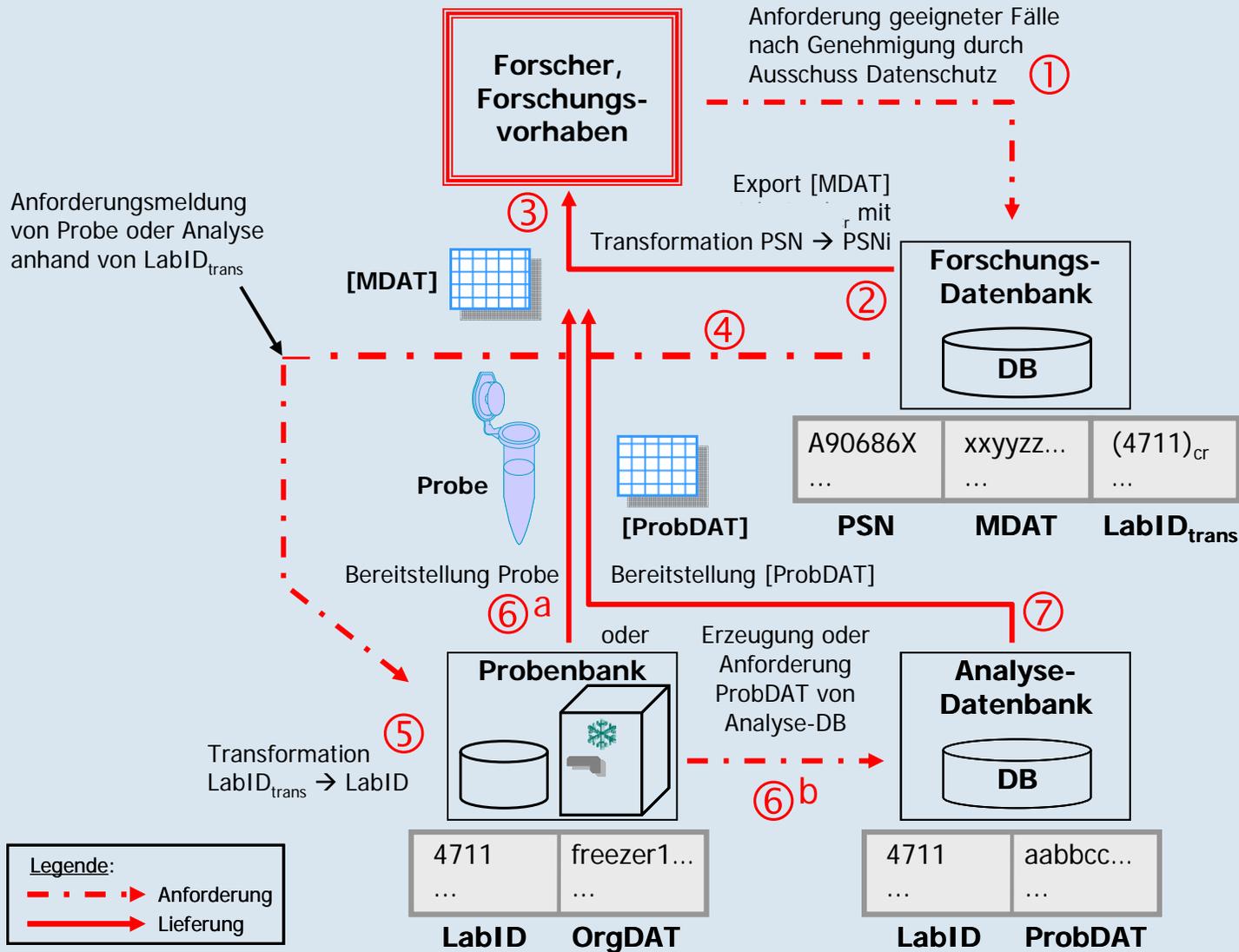


- ↪ Patientenliste erlaubt Rückbezug auf Identität.
- ↪ Führung der Patientenliste verlangt:
 - ↪ Ansiedlung an vertrauenswürdiger Einrichtung
 - ↪ Ausstattung mit umfangreichen Schutzmaßnahmen gegen unbefugte Zugriffe
- ↪ Beschlagnahmefestigkeit nur gegeben:
 - ↪ im Behandlungskontext
 - ↪ bei notarieller Verwahrung
- ↪ **Verhältnismäßigkeit:**
 - Notarielle Führung der Patientenliste nur erforderlich,
 - ↪ bei sehr großem Patientenbestand
 - ↪ wenn Daten oder Proben attraktiv für Rückidentifizierungsversuche
 - ↪ Sonst wenigstens organisatorische Unabhängigkeit empfohlen.
 - ↪ Unter Umständen reicht auch dezentrale Patientenliste („an der Quelle“) bei getrennter Datenbank-Administration.



- ↪ Eindeutige Kennzeichnung der Probe
 - ↪ als Aufkleber (Barcode)
 - ↪ und Teil der OrgDAT
- ↪ Erzeugung bei probengewinnender Stelle
 - ↪ Zuordnung zum Patienten nur dort möglich
- ↪ Erzeugung dezentral oder durch zentrales online-Verfahren
 - ↪ analog zur PID-Erzeugung
- ↪ Probenbank erzeugt LabID_{trans}:
 - ↪ kryptographisch oder über Zuordnungstabelle,
 - ↪ Zuordnung zu LabID nur in Probenbank möglich
- ↪ Forschungsdatenbank erhält nur LabID_{trans}
- ↪ Bei Anforderung von ProbDAT (oder Proben) Mitarbeit der Probenbank nötig

Übermittlung von Daten und Proben an Forschungsprojekte



Datensparsamkeit beachten:

- ↪ Nur die benötigten Daten herausgeben
- ↪ Keine Herausgabe der Ordnungsparameter PSN, LabID_{trans}
 - ↪ Export anonymisiert oder mit jeweils eigenem Pseudonym PSN_i
- ↪ Kein direkter Zugriff für Forscher auf Forschungsdatenbank
- ↪ Als Regelfall: Herausgabe nur von Analysedaten statt ganzer Proben

Z. B. Verhältnismäßigkeit Aufbewahrung:

- ↪ ProbDAT zu MDAT? Möglich, wenn:
 - ↪ ProbDAT enthält keine probenidentifizierenden Informationen
 - ↪ ProbDAT enthält keine personenidentifizierenden Informationen
- ↪ ProbDAT zu Proben? Möglich, wenn:
 - ↪ ProbDAT sind leicht aus der Probe gewinnbar
 - ↪ ProbDAT erlauben keine Zuordnung zu MDAT
- ↪ MDAT, Probe, ProbDAT in der gleichen Institution? Wenn:
 - ↪ Verschiedene Fachaufsicht gegeben, kein gegenseitiger Zugriff
 - ↪ Daten dürfen keinen unmittelbaren Rückschluss auf Identität zulassen

⇒ vereinfachte Modellvarianten

Anmerkung:

Verschiedene Einrichtungen/Fachabteilungen eines Klinikums haben verschiedene Fachaufsicht/ Verantwortlichkeit.

Grundsätzlich:

- ↪ Biomaterialproben gelten noch als anonymisierbar.
→ Anonymisierte Proben fallen nicht unter Datenschutzgesetze.
- ↪ Saubere Lösung für Eigentumsverhältnisse notwendig.
- ↪ Für eine langfristige Nutzung von Biomaterialien sollte die Einwilligung
in eine *pseudonymisierte* Verarbeitung vereinbart werden.

Altproben:

- ↪ anonymisiert für die Forschung verwenden.

Neuproben:

- ↪ Klausel im Behandlungsvertrag vorsehen.
 - ↪ Beispiel: „Ich willige ein, dass meine Proben nach Löschung der identifizierenden Daten (bzw. Pseudonymisierung) zu Forschungszwecken genutzt werden, und übertrage das Eigentum an ihnen dem QQQ-Klinikum.“

- ↪ Rechtlich einwandfreier Umgang mit Biomaterialien und Aufbau von Biomaterialbanken ist möglich.
- ↪ Wichtige Grundlagen dafür:
 - ↪ Ordnungsgemäßer Betrieb der BMB mit klaren Verantwortlichkeiten
 - ↪ Sorgfältig formulierte Einwilligungserklärung
 - ↪ Hoher Sicherheitsstandard
 - ↪ Informationstrennung mit Pseudonymen
- ↪ Das Konzept hat den Konsens des AK Wissenschaft der Datenschutzbeauftragten.
- ↪ Publikation in TMF-Buchreihe (bei MMV) in Vorbereitung.