Biomaterialbanken
Datenschutz und Pseudonymisierung

Informationsveranstaltung Biomaterialbanken, Berlin, 14. September 2009

Prof. Dr. Klaus Pommerening

Universität Mainz + KN Pädiatrische Onkologie und Hämatologie
+ TMF-AG Datenschutz

gefördert vom
Bundesministerium für Bildung und Forschung

Spezifika von Biomaterialbanken

- Sammlung von Biomaterialien für Forschungsprojekte
  - für unbestimmte *Zeit*,
  - nicht immer vorher bestimmten *Zweck,*
  - nicht immer vorher bekannten *Anwenderkreis*.
- Drei datenschutzrechtliche Hindernisse (sogar bei Einwilligung)
  - besondere Schutzmaßnahmen nötig.
- Genetische Informationen in Materialien stets personenbeziehbar.
  - Informationsdichte nicht verringerbar (im Sinne der „Datensparsamkeit“).
- Verknüpfung der Proben mit krankheitsbezogenen, soziodemographischen und anderen Daten –
  - über Referenzproben **unbefugte Rückidentifizierung** möglich.

TMF-Datenschutzkonzept

- **Datenschutzkonzept der TMF für Biomaterialbanken** liegt vor.
  - Buchpublikation in Vorbereitung (TMF-Schriftenreihe)
  - Wichtigste Grundlagen:
    - Generisches DS-Konzept der TMF,
    - Stellungnahme des Nationalen Ethikrates zu Biobanken,
    - Konsens der Datenschutzbeauftragten (AK Wissenschaft).

- Bereits publiziert in TMF-Schriftenreihe:
  - **Rechtliche Rahmenbedingungen,**
  - **Leitfaden zur Einwilligung**.

- **Rechtliche Rahmenbedingungen**
  - Das Ausbalancieren der Grundrechte „Forschungsfreiheit“ und „informationelle Selbstbestimmung“/ Persönlichkeitsrechte erfordert die Ausgestaltung von Regelungen nach dem Prinzip der Verhältnismäßigkeit.

- **Organisatorisches und technisches Umfeld**
  - z. B. datenschutzrelevante Angriffsszenarien auf BMB:
    - unbefugter Zugriff auf Daten,
    - unbefugte Rückidentifizierung,
    - Zugriff auf Proben.

- Wesentliches **Ziel eines Datenschutzkonzepts**:
  Das Rückidentifizierungsrisiko muss minimiert und kontrolliert werden.

- **Persönlichkeitsrecht**
  - ... verhindert beliebige Nutzung von Proben und ist *unveräußerbar*. [BGH]
  - Proband muss Kontrolle über seine „abgetrennten Körperteile“ behalten.
- **Datenschutzrecht**
  - ... sichert die informationelle Selbstbestimmung über personenbeziehbare Informationen.
  - Strenge Regeln des Arztrechts (Schweigepflicht).
- **Eigentumsrecht** (folgt)
- Umgang mit „Altproben“ in rechtlicher Grauzone.

Eigentumsrecht

- Eine Probe befindet sich, vorbehaltlich anderer Übereinkünfte, im **Eigentum des Probanden**.
  - *Das Eigentumsrecht kann abgetreten werden*.
  - Aber: Der Eigentumsübertrag einer Probe an eine BMB bedarf einer **ausdrücklichen Vereinbarung** zwischen BMB und Proband.

- Eine BMB kann eine Probe an einen Dritten übergeben, sofern sie Eigentümer der Probe ist,
  - aber nur, soweit das Persönlichkeitsrecht des Probanden nicht verletzt wird.
  - *Das Persönlichkeitsrecht kann nicht abgetreten werden*.

Einwilligungserklärung
Grundsätze

- Die verbindliche a-priori-Festlegung von Zweck, Zeitraum, Nutzerkreis
  - gehört zu einer wirksamen Einwilliguungserklärung,
  - Widerspricht aber dem Nutzen einer BMB.

Daher **Abschwächung**:

- Als Standardvorgabe sind Zweck und Nutzungsdauer der Probe *so konkret wie möglich* benennen.
- Der Forschungszweck kann aber *offen formuliert* werden. Der Patient behält dabei durch sein Widerrufsrecht angemessene Kontrolle über seine Proben und Daten.
- Adäquate Aufklärung und *abgestufte* Vorlage zur *Einwilligung* – soweit im Kontext sinnvoll machbar – erlauben dem Patienten individuelle Festlegung der Reichweite
  - als Ausdruck des Rechts auf informationelle Selbstbestimmung.

Einwilligungserklärung
Wissen / Nichtwissen

- Das Auskunftsrecht (nach BDSG) muss der Patient **aktiv** wahrnehmen.
- Es besteht von Seiten der Forscher **keine datenschutz-rechtliche** Mitteilungs**pflicht** über die in der Einwilligungserklärung vereinbarte Vorgehensweise hinaus.
- Das in einer Einwilligung vereinbarte **Recht auf Nichtwissen** bedarf im Einzelfall einer (ethischen) Prüfung.
- Auch das Vorgehen bei „Zufallsbefunden“ bedarf einer eingehenden ethischen Erörterung.

Aufklärung und Einwilligungserklärung
Umfang

- Eigentums- und Nutzungsübertragung
- Träger und Rechtsnachfolge der BMB
- Verantwortliche, Ansprechpartner
- Reichweite der Einwilligung (Zweck, Nutzungsdauer)
- vorgesehene oder mögliche Weitergabe an Dritte
- geplante Anonymisierung oder Pseudonymisierung
- Mitteilungspflichten, Auskunftsrecht, Wissen versus Nichtwissen
- Widerruf und Löschung
- Regelung für den Todesfall
- Materialgewinnung und -handhabung
- mögliche Zusatzerhebungen, „Rekrutierung“ für künftige Studien

Anonymisierung

- Absolute Anonymisierung von Proben ist nicht möglich.
  - Die Rückidentifizierung ist noch sehr aufwendig.
  - Anonymisierbarkeit (de facto) z. Z. noch angenommen.
  - „*Der Erhalt des Persönlichkeitsrechts auf Verfügung über eigenes Körpermaterial kann einen Verzicht auf sonst mögliche Anonymisierung nicht rechtfertigen.*“ [AK Wissenschaft]
- Wirksamkeit der Anonymisierung muss **immer wieder neu** nach dem aktuellen Stand **bewertet** werden (z. B. bei Weitergabe).
- Für eine langfristige Nutzung von Biomaterialien sollte die Einwilligung eine *pseudonymisierte* Verarbeitung vereinbart werden.
- Eine geplanten Anonymisierung der Materialien bzw. Daten ist mitzuteilen.
  - Der Patient ist darauf hinzuweisen, dass er bestimmte Rechte nach Anonymisierung nicht mehr wahrnehmen kann:
    - das Recht auf Mitteilung individueller Ergebnisse,
    - das Recht auf Berichtigung/Löschung/Vernichtung,
    - das Recht auf Widerruf der Verarbeitung.

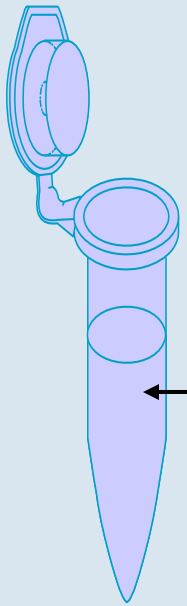
Datenschutzkonzept BMB
einige Grundsätze

- Offene Konzeption (Dauer, Zweck, Anwender) **muss** durch strengen organisatorischen Rahmen und besondere Sicherheitsmaßnahmen kompensiert werden.
  - Einwilligung allein reicht nicht.
- Verbindliche und nachprüfbare Regel- und Vertragswerke.
  - Satzung der BMB, Policies
  - Nennung der Verantwortlichen für Probenlagerung und Datenspeicherung/ -verarbeitung
  - Prüfung und Genehmigung von Projekten,
  - Durch öffentliche Bekanntmachung Vereinfachung der Aufklärung.
- Übergang in Forschungskontext nur anonymisiert oder pseudonymisiert.
- Minimierung und Kontrolle der Zugriffe.

Datenschutzkonzept BMB
Methoden

- Minimierung des Angriffspotenzials durch
  - technische Maßnahmen/ Sicherheitsdienste:
    - Verschlüsselung, Firewalls, Zugangs- und Zugriffskontrolle, Überwachung, ...
  - organisatorische Maßnahmen:
    - getrennte Speicherung / Lagerung
    - Trennung der Verantwortlichkeiten („Mehraugenprinzip“)
    - Verpflichtungen, Selbstverpflichtungen, vertragliche Regelungen, verbindliche SOPs, Einwilligungserklärung
- Werkzeuge:
  - Informationsteilung mit Kommunikationskontrolle
  - Zugriffskontrolle
  - Identitätsmanagement mit Pseudonymisierung (und Anonymisierung) für Personen und Proben/ Material

Informationsarten



ProbDAT → Analysedaten aus der Verarbeitung der Probe

MDAT → medizinische Kontextdaten zum Probanden

$OrgDAT_{Lab}$ $OrgDAT_{Order}$ → organisatorische Daten zur Verwaltung und Lagerung der Probe, auch zum aktuellen Auftrag zur Analyse oder Weitergabe

$OrgDAT_{Prob}$ → eindeutige Identifikatoren des Probanden, der Probe, der beteiligten Institutionen und Ärzte / Forscher

IDAT → probandenidentifizierende Daten, weitere soziodemographische Daten zum Probanden

Informationstrennung

Prinzipieller Ansatz: Verteilte Architektur, Kommunikation über Treuhänderdienste (TTP = Trusted Third Party)
– Evtl. Vereinfachungen nach Verhältnismäßigkeit

1. getrennte Speicherung / getrennte Verantwortung

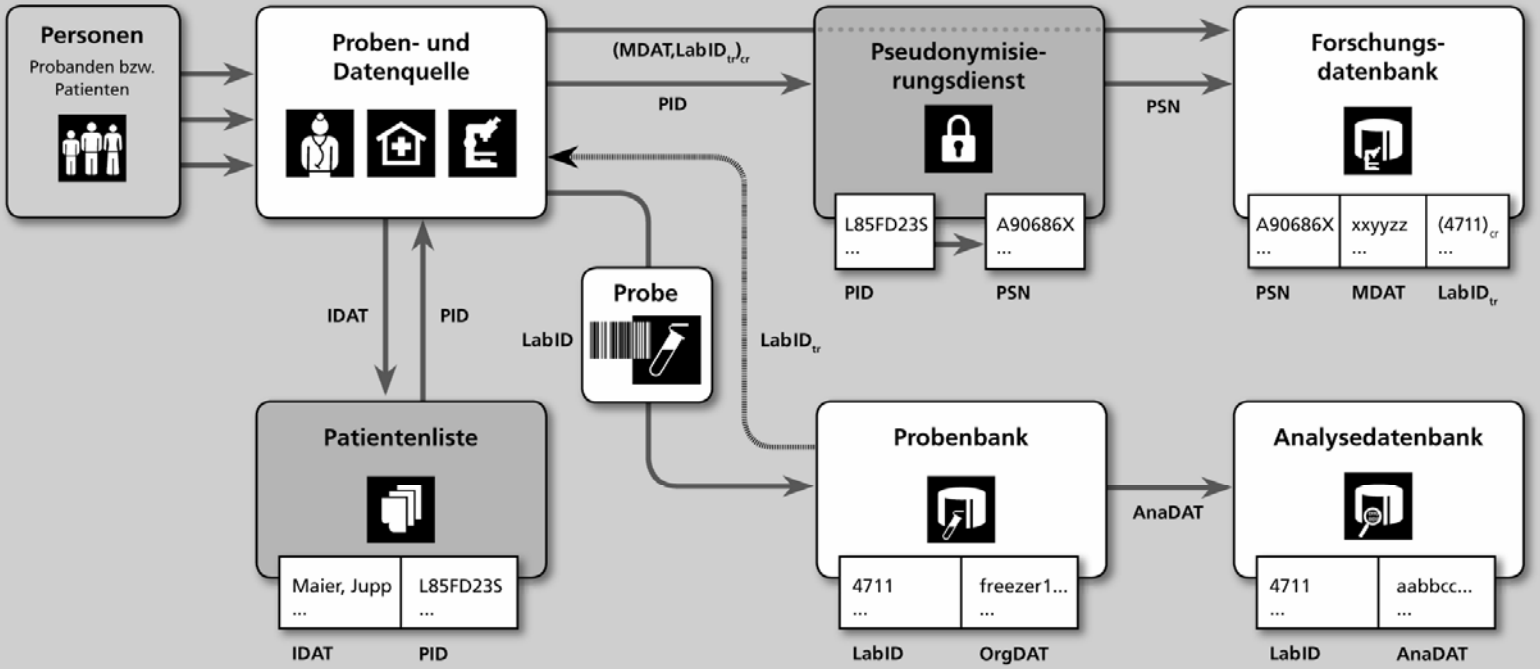
   IDAT – MDAT – Probe/OrgDAT – ProbDAT

2. Zuordnung über verschiedene Pseudonyme („Identitätsmanagement“)

   PID – PSN – LabID – $LabID_{tr}$

3. Anonymisierung oder zusätzliche Pseudonymisierung beim Übergang BMB → Forschungsprojekt
   - Nur benötigte Daten herausgeben („Datensparsamkeit“).
   - Angestrebter Regelfall: Statt Proben Analysedaten herausgeben.

Informationsfluss und -verteilung in BMB („Maximalmodell“)



(entspricht „TMF-Modell B“: MDAT in patientenferner „Forschungsdatenbank“)

Die LabID

- Eindeutige Kennzeichnung der Probe
  - als Aufkleber (Barcode)
  - und Teil der OrgDAT
  - nicht-sprechend (pseudonym)
- Erzeugung bei probengewinnender Stelle
  - Zuordnung zum Patienten nur dort möglich.
- Erzeugung dezentral oder durch zentrales Online-Verfahren
  - analog zur PID-Erzeugung
- Probenbank (oder ID-Management-TTP) erzeugt $LabID_{tr}$:
  - kryptographisch oder über Zuordnungstabelle,
  - Zuordnung zu LabID nur in Probenbank möglich.
- Forschungsdatenbank erhält nur $LabID_{tr}$.
- Bei Anforderung von ProbDAT Mitarbeit der Probenbank nötig (bei Proben sowieso).

Redundanzen der Sicherheitsmaßnahmen

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.

Beispiele für Verhältnismäßigkeit
abhängig von Kriterien und Einzelfall-Bewertung

- Verhältnismäßigkeit Aufbewahrung
  - ProbDAT zu MDAT? Möglich, wenn:
    - ProbDAT enthält keine probenidentifizierenden Informationen.
    - ProbDAT enthält keine personenidentifizierenden Informationen.
  - MDAT, Probe, ProbDAT in der gleichen Institution? Wenn:
    - Verschiedene Fachaufsicht gegeben, kein gegenseitiger Zugriff.
    - Daten dürfen keinen unmittelbaren Rückschluss auf Identität zulassen.

- Ansiedlung von TTP-Diensten
  - Pseudonymisierung „an der Quelle“,
    - wenn Behandlungskontext und einmalige Probenentnahme.
  - Im „großen“ Forschungsverbund TTP-Dienste bei verschiedenen Kliniks-Rechenzentren
    - wenn diese ansonsten am Forschungsprojekt unbeteiligt sind.

⇒ vereinfachte Modellvarianten

Proben aus dem Behandlungszusammenhang

- Für eine langfristige Nutzung von Biomaterialien sollte die Einwilligung in eine *pseudonymisierte* Aufbewahrung vereinbart werden.
- Saubere Lösung für Eigentumsverhältnisse notwendig.

Altproben:

- anonymisiert für die Forschung verwenden.
  - (Rechtlich problematisch wegen Persönlichkeitsrecht und Eigentumsrecht.)

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.“
- Getrennte Lagerung für Forschungszwecke rechtlich nicht notwendig,
  - aber entsprechende Kennzeichnung in OrgDAT und adäquate Umgangsregeln.

Zusammenfassung

- Rechtlich einwandfreier Umgang mit Biomaterialien und Aufbau von Biomaterialbanken ist möglich.

- Wichtige Grundlagen dafür:
  - ordnungsgemäßer Betrieb der BMB mit klaren Verantwortlichkeiten,
  - sorgfältige Aufklärung und Einwilligungserklärung,
  - hoher Sicherheitsstandard,
  - Informationstrennung und Identitätsmanagement mit Pseudonymen,
  - Einsatz von Treuhänderdiensten.