Anforderungen des Datenschutzes an ID-Management in der medizinischen Forschung

Marit Hansen
Stellvertretende Landesbeauftragte für Datenschutz Schleswig-Holstein

TMF-Workshop ID-Management
15.12.2008 in Berlin

Überblick

- Rechtliche Anforderungen
- Technisch-organisatorische Anforderungen
- Beispiel Biobanken
- Fazit

Informationelles Selbstbestimmungsrecht (Art. 2+1 GG)

Forschungsfreiheit (Art. 5 GG)

Erhebung pers. Daten = Eingriff

Konkretes Forschungsvorhaben

Bedarf an pers. Daten

Abwägung

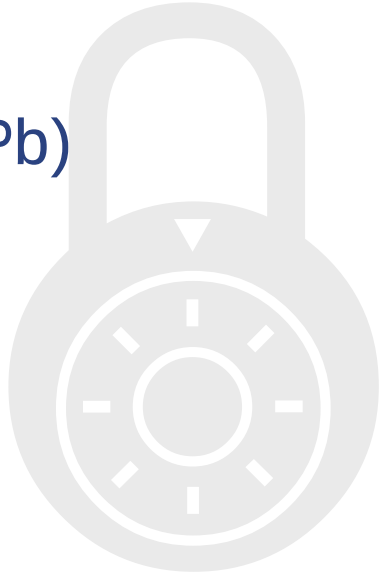
Geeignetheit des Forschungsvorhabens
und Erforderlichkeit des Eingriffs

Anonymisiert/pseudonymisiert
/personenbezogen?

Einwilligung des Betroffenen

{An|Pseud}onymisieren

- Methoden der Datensparsamkeit; Ziele:
  - Entfernen/Erschweren des Personenbezugs (Pb)
  - Kontrolle über Herstellung des Pb
- Ansatz:
  - Entkopplung à la „Need to know“
    - Zwischen Person und Daten (und Proben)
    - Zwischen verschiedenen Prozessen im Workflow
    - Zwischen verschiedenen Rollen im Workflow
  - Zu diesem Zweck:
    - Umkodierung von Identifikatoren
    - Ggf. Einführen von Instanzen zur Entkopplung



(Daten-)
Treuhänder

Anonymisieren

§ 3 Abs. 6 Bundesdatenschutzgesetz

Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Pseudonymisieren

§ 3 Abs. 6a Bundesdatenschutzgesetz

Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(LDSG S-H: Def. wie Anonymisieren, nur „ohne Nutzung der Zuordnungsfunktion“)

Eigentlich gemeint: „Daten verarbeitende Stelle behält Kontrolle über Herstellung des Pb.“

Pseudonymisierungsverfahren

Bei Pseudonymisierung vorab zu klären:

- wo jeweils die Entkopplung greifen soll,
- ob ein „Rückweg“ (z.B. für Feedback-Prozesse) möglich sein soll,
- wer über die Verkettungsregeln verfügen soll,
- wer das Pseudonym generieren soll,
- wer und unter welchen Voraussetzungen Pseudonym und Identifikationsdaten zusammenführen darf,
- welches Reidentifizierungsrisiko hinsichtlich der pseudonymisierten Datensätze besteht.

Qualität der Anonymität (= Nicht-Pb)

- **Bei Anonymisierung:**
  - Größe der Anonymitätsmenge
  - Grad der Anonymisierung
    - Identifizierende Eigenschaften in den Daten selbst
    - (Zusatz-)Wissen der Beteiligten
- **Bei Pseudonymisierung:**
  wie Anonymisierung, aber zusätzlich
  - Qualität der Pseudonyme
    - Zufallsbasierte Generierung?
  - Verarbeitung der Verkettungsregeln
    - Wo Wissen / Nutzungsmöglichkeit?

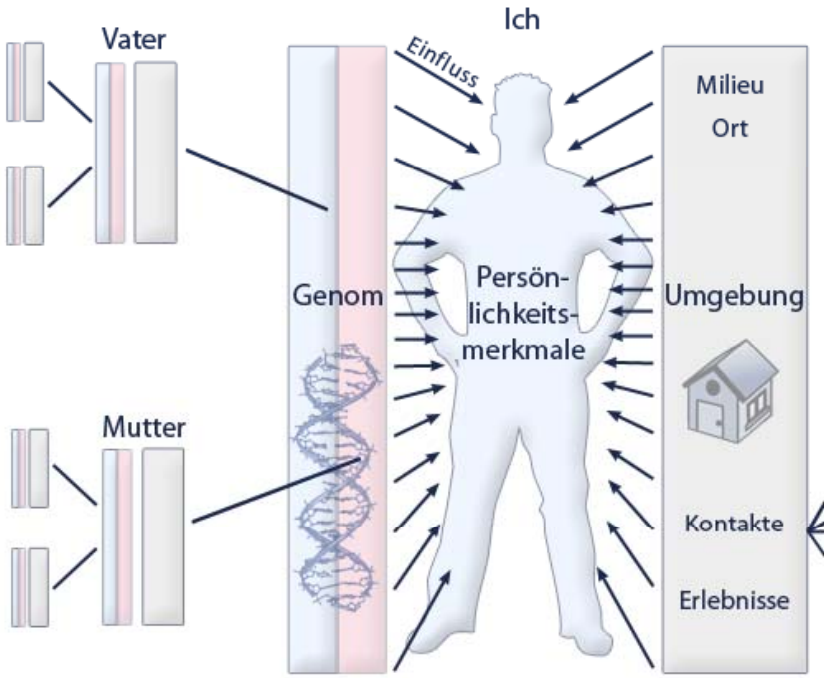
Aufbau- und Ablauforganisation

Gestaltungsbereiche:

- Prozesse
- Rollenkonzept (inkl. potenzieller Rollenkonflikte, Stellvertretung, Weisungsverhältnisse, Treuhänder(kontrolle))
- Verbindung von Prozessen mit Rollen
- Kommunikationen (authentisch, integer, vertraulich, ...)
- Systeme & Subsysteme (Datenbanksystem, Probenlager, ...)
- Protokollierung der Daten- und Probenverwendung
- Schutzgegenstände und –maßnahmen (inkl. Notfallkonzept)
- Risikoanalyse (Robustheit, mögliche Angreifermodelle)

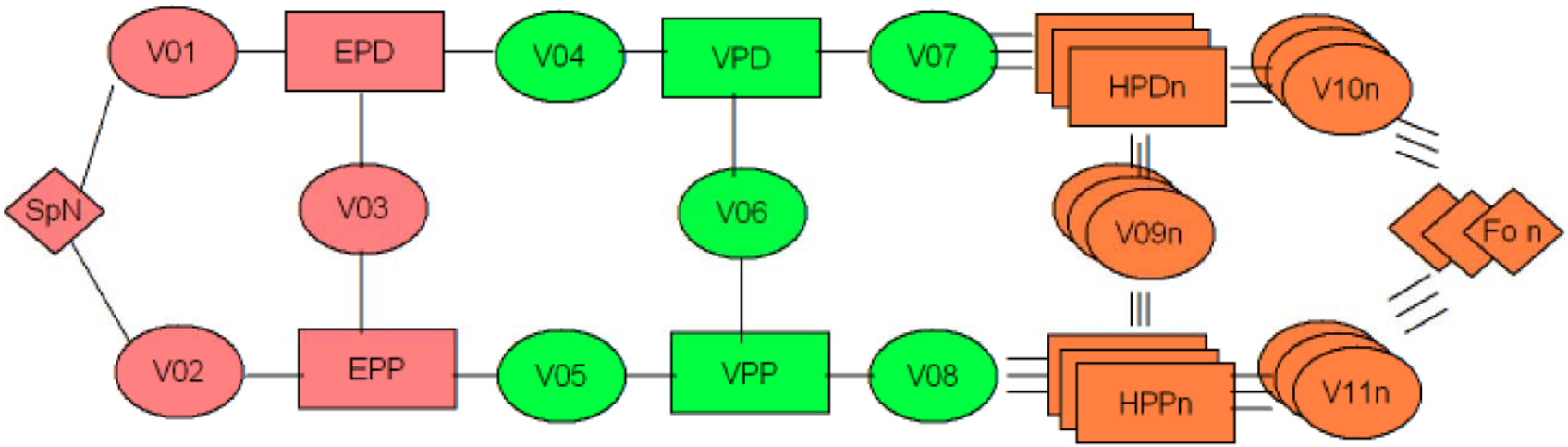
Beispiel Biobanken

- Nicht nur Daten, sondern auch Proben
- Gendaten: besonders sensibel
- Breite Beforschbarkeit:
  - Mehrfache Herausgabe
  - Pb-kritische Ausreißer in Daten können relevant sein
- Rückholbarkeit der Einwilligung mit der Folge der Probenvernichtung
- Möglichkeit für Feedback
- Geschäftsmodelle relevant



„Gestreckte Pseudonymisierung“
(Quelle: bdc|AUDIT)

Pseudonymisierung in Biobanken als gestreckter Vorgang mit drei Risikosphären unterschiedlicher Beherrschbarkeit



Erhebung Vorhaltung Herausgabe

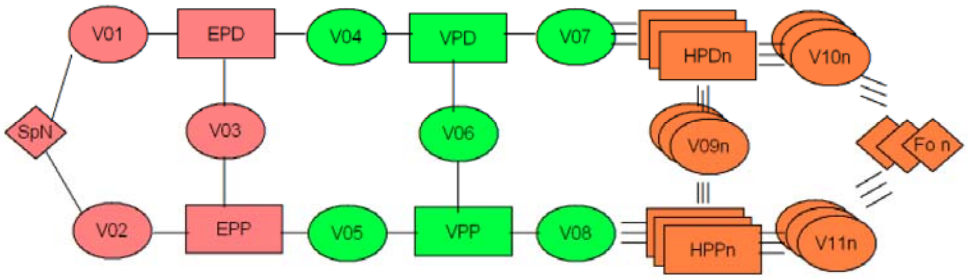
Referenz auf TMF-Begriffe:
EPD=PID, EPP=LabID,
VPD=PSN, VPP=LabIDtrans,
HPDn=HPPn=PSNi

bdcAUDIT

Bezeichnerwechsel
(Quelle: bdc|AUDIT)

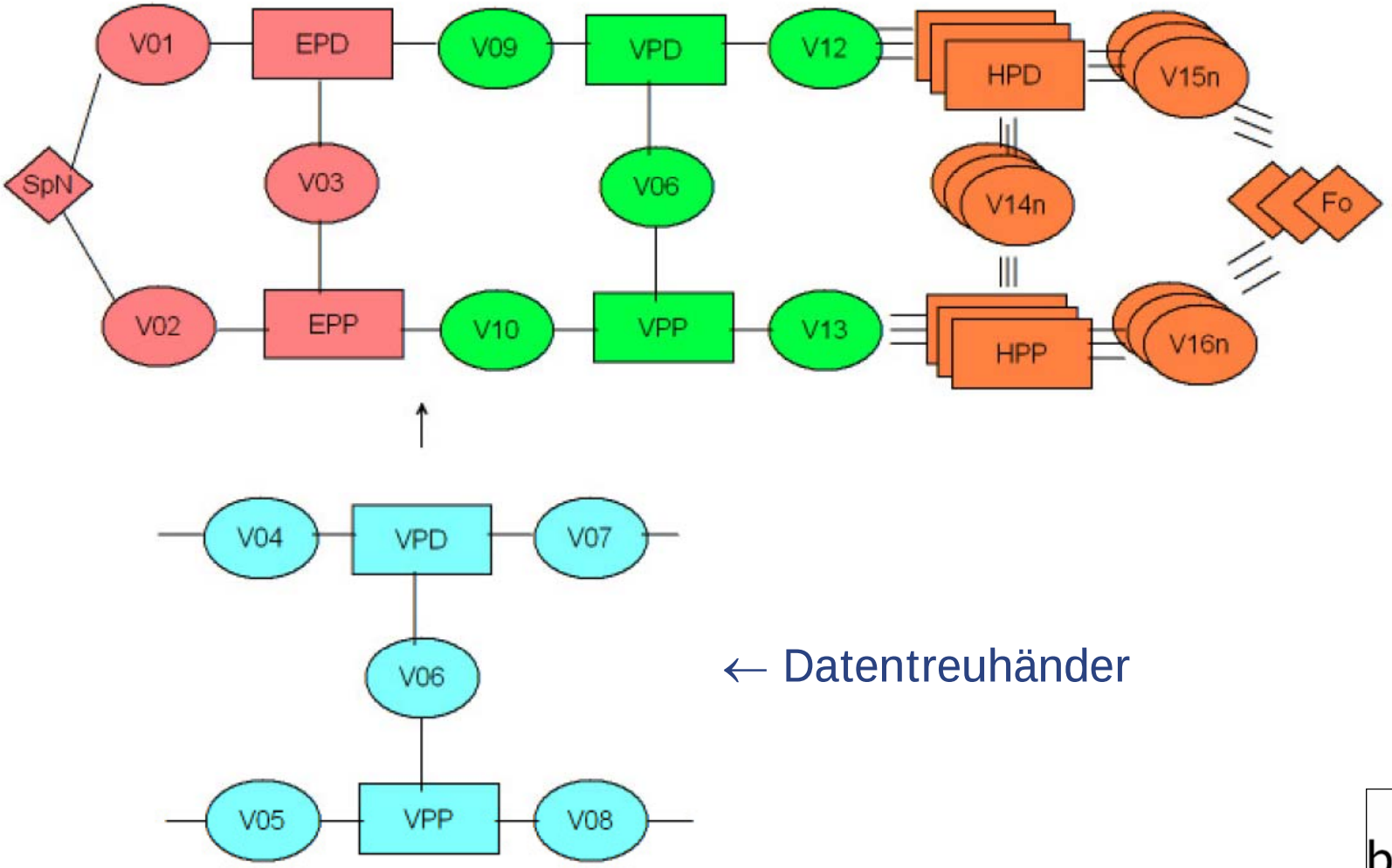
Pseudonym-wechsel		EP	Risikoschwelle	VP	Risikoschwelle	HP	HP*
		Unsicherer Außenbereich Erhebung		Sicherer Innenbereich Vorhaltung		Unsicherer Außenbereich Herausgabe	
						Forscher 1	Forscher 2
Ideal-zustand	**Daten**	EPD		VPD		HPD	HPD*
	Proben	EPP		VPP		HPP	HPP*

D: Daten
P: Proben
EP: Erhebungspseudonym
VP: Vorhaltungspseudonym
HP: Herausgabepseudonym



bdcAUDIT

Integration eines Datentreuhänders in das Modell (Quelle: bdc|AUDIT)



← Datentreuhänder

bdc AUDIT

Fazit

- ID-Management zur Entkopplung des Personenbezugs
- Ziel: Kontrolle über Herstellung des Personenbezugs
- Notwendig:
  - Maßgeschneiderte, standardisierte, überprüfbare Lösungen für unterschiedliche Risikosphären
  - Berücksichtigung der Interessen aller Beteiligten (auch für Angreifermodell!)
  - Angemessener Umgang mit Langzeitrisiken

Literatur

- Rainer Metschke, Rita Wellbrock (LfD Berlin und Hessen): Datenschutz in Wissenschaft und Forschung, 2000/2002
- Rita Wellbrock: Datenschutzrechtliche Aspekte des Aufbaus von Biobanken, MedR 2003, Heft 2, 77-82
- European Medicines Agency, Evaluation of Medicines for Human Use: Understanding the terminology used in pharmacogenetics, 29 July 2004, EMEA/3842/04/Final
- Recommendation Rec(2006)4 of the Committee of Ministers to member states on research on biological materials of human origin
- Beiträge auf dem GI-Workshop zu Datentreuhändern, 2006
- bdc\AUDIT-Workshop, 2008
- Generisches TMF-Datenschutzkonzept

Vielen Dank für Ihre Aufmerksamkeit!