Orientierungshilfe: Pseudonymisierung in der medizinischen Forschung

1. Einleitung

Viele Bereiche der medizinischen Forschung benötigen medizinische Patientendaten für ihre Arbeit, z.B. Studien zur klinischen Arzneimittelzulassung, zur Wirksamkeit neuer Behandlungsmethoden, Forschung zu bestimmten Erkrankungen. Neben der Nutzung von Behandlungsdaten der eigenen Patienten in den einzelnen Kliniken entstehen vermehrt Forschungskooperationen zwischen Krankenhäusern, Koordinierungszentren für klinische Studien (KKS), Forschungseinrichtungen etc., teilweise deutschland- und europaweit. Dies ist z.B. bei den diversen medizinischen Kompetenznetzen http://www.kompetenznetze-medizin.de *(externer Link)* der Fall. Dies bringt es mit sich, dass die medizinischen Daten der Patienten die eigentliche Behandlungseinrichtung verlassen. Da in der Regel Informationen des Patienten wie Name, Adresse für die Forschung nicht erforderlich sind und darüber hinaus auch für die Forschung das Arztgeheimnis gewahrt bleiben muss, sind die Daten für die Forschung zu anonymisieren oder zumindest zu pseudonymisieren.

Gleiches gilt auch für Bereiche wie Qualitätssicherung (Bundesgeschäftsstelle Qualitätssicherung, QuasiNiere) oder die Versorgungsforschung, aber auch für den Aufbau von Registern zu einer Krankheit, wie sie z.B. in den Krebsregistern Verbreitung finden.

Deshalb wird an vielen Stellen unabhängig voneinander an Konzepten zur Pseudonymisierung gearbeitet, die die Rechte des Patienten sicherstellen sollen. Um sowohl die Entwicklung als auch die Beurteilung solcher Konzepte zu vereinfachen, sollen in dieser Orientierungshilfe gewisse technisch-organisatorische Grundelemente eines Pseudonymisierungskonzepts aufgezeigt werden.

2. Begriffe

Anonymisierung gemäß § 3 Abs. 6 BDSG (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.

Pseudonymisierung gemäß § 3 Abs. 6a BDSG: Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Reidentifizierungsrisiken können sich aus dem Verfahren der Pseudonymgenerierung und / oder dem Umfang der Datensätze ergeben.

IDAT: Identifizierende Daten des Patienten wie Name, Adresse, KV-Nummer. Häufig wird hierbei der Datensatz der Krankenversichertenkarte verwendet.

MDAT: Medizinische Daten des Patienten. Diese umfassen sämtliche bei der Behandlung anfallenden medizinischen Informationen wie Diagnosen, Anamnesen, Therapien, verordnete Medikamente, Operationen etc. sowie evtl. für die Forschung zusätzlich erhobene Daten.

Behandelnde Stelle: Hier erfolgt die Behandlung des Patienten und somit die Erhebung der für die Forschung interessanten Daten. Sie fungiert dadurch als Datenlieferant für etwaige Forschungsdatenbanken und ist im Besitz der gesamten oder eines Teils der Dokumentation zu dem Patienten, bestehend aus IDAT und MDAT.

Forschende Stelle: Diese Stelle nutzt die pseudonymisierten bzw. anonymisierten Daten der verschiedenen behandelnden Stellen und nimmt wissenschaftliche Auswertungen vor.

Patientenliste: Eine Patientenliste ermöglicht die Zuordnung der IDAT der teilnehmenden Patienten zu einem zugehörigen Pseudonym. Eine zentrale Patientenliste enthält also eine Zusammenstellung von Patienten, die an einer bestimmten Krankheit leiden.

Pseudonymisierende Stelle: Diese Stelle nimmt die Pseudonymisierung der IDAT vor, d.h. sie erzeugt ein Pseudonym, wobei bei mehrstufigen Verfahren mehrere pseudonymisierte Stellen nacheinander durchlaufen werden können. In vielen Fällen führt die pseudonymisierende Stelle gleichzeitig die Patientenliste, soweit eine solche benötigt wird.

Treuhänder: Ein Treuhänder ist eine neutrale Vertrauensstelle, die gewisse zentrale Aufgaben wahrnimmt und hierfür personenbezogene Daten erhält. Häufig übernimmt er die Aufgaben der pseudonymisierenden Stelle und / oder der Patientenliste. Dabei ist in der Regel die Sicherstellung des Beschlagnahmeschutzes erforderlich, weswegen häufig Notare zum Einsatz kommen.

Hash-Verfahren / Hash-Wert: Hash-Verfahren sind mathematische Verfahren, die Eingangsdaten (hier IDAT) auf eine Prüfsumme (Hash-Wert) abbilden. Hash-Verfahren haben einige typische Eigenschaften:

- Keine Rückrechnung der Originaldaten aus dem Hash-Wert (Einwegfunktionen)
- Eindeutigkeit/Kollisionsfreiheit des Hash-Werts, d.h. verschiedene Eingangsdaten erzeugen unterschiedliche Hash-Werte (wobei gleiche Eingangsdaten immer den gleichen Hash-Wert erzeugen)

3. Grundprobleme der Pseudonymisierung

Bei der Erstellung eines geeigneten technisch-organisatorischen Pseudonymisierungskonzepts müssen zunächst verschiedene Fragen betrachtet werden:

- Beteiligte Stellen: Die Komplexität der Pseudonymisierung hängt stark ab von der Anzahl der beteiligten Stellen. In der kleinsten Form gibt ein Krankenhaus pseudonymisierte Daten an eine externe Forschungseinrichtung weiter. Das hierfür benötigte Konzept unterscheidet sich in der Regel deutlich von dem Fall, dass eine Vielzahl deutschlandweit verteilter Kliniken Daten in eine zentrale Datenbank liefert, die von unterschiedlichen Forschungsgruppen ausgewertet wird.
- Erhebungszeitraum: Je nach Krankheitsart können über einen unterschiedlich langen Zeitraum Behandlungsdaten anfallen. Bei akuten Erkrankungen betrifft dies in der Regel nur wenige Wochen oder Monate, bei chronischen Erkrankungen können über das ganze Leben des Patienten hinweg Daten erfasst werden. Gerade bei derartigen Erkrankungen sind Langzeituntersuchungen von großem Interesse, so dass sichergestellt werden muss, dass Meldungen zu einem Patienten für den gesamten Zeitraum richtig in der Forschungsdatenbank zugeordnet werden können.

- Mobilität des Patienten: Gerade bei längerfristigen Studien ist es wünschenswert, dass Patienten auch nach einem Umzug, Arzt oder Namenswechsel noch richtig in der Forschungsdatenbank ermittelt werden können, d.h. das Pseudonym muss über die ganze Studiendauer richtig zuordenbar sein.
- Erforderlichkeit der Depseudonymisierung: Eine Pseudonymisierung der Daten anstelle einer Anonymisierung ist erforderlich, wenn die Daten nicht in einem Schritt erhoben werden können, sondern über einen gewissen Zeitraum hinweg "Nachlieferungen" erfolgen, oder wenn die Möglichkeit einer Depseudonymisierung im Einzelfall im Interesse des Betroffenen liegt. Grundsätzlich ist somit zu klären, ob bzw. wann eine Reidentifizierung der pseudonymisierten Daten erforderlich ist, wofür im Konzept Mechanismen integriert werden müssen. Dies kann z.B. der Fall sein, wenn Ergebnisse der Forschung direkt in die Behandlung einfließen sollen.
- Zugriffsart: Ein weiteres Gestaltungsmerkmal ist die Frage, ob Forscher online auf Daten zugreifen sollen und diese daher jederzeit zugreifbar sein müssen, oder ob nur ein Offline-Zugriff gewährt werden soll. In beiden Fällen muss dem Zugriff ein Antrag auf Genehmigung vorausgehen. Die für die Genehmigung zuständige Stelle muss u.a. prüfen, ob di ein Frage stehenden Daten hinreichend anonymisiert bzw. pseudonymisiert sind oder ob sich Reidentifizierungsrisiken z.B. augrund des Umfangs der Datensätze ergeben.
- Universalität des Pseudonyms: Bei der Auswahl und Gestaltung des Pseudonymisierungsverfahrens für eine Studie ist darauf zu achten, dass die erzeugten Pseudonyme sich von denen anderen Studien unterscheiden, d.h. nimmt ein Patient an mehreren Studien teil, muss er dort jeweils unterschiedliche Pseudonyme erhalten. Dies soll die Entstehung eines lebenslang gültigen Personenkennzeichens für die medizinische Forschung verhindern.

Aus der Betrachtung dieser Fragen können grundsätzliche Gestaltungselemente abgeleitet und kombiniert werden, die im nächsten Kapitel näher beschrieben werden:

- Zentrale oder dezentrale Datenhaltung
- Zentrale oder dezentrale Pseudonymisierung
- Pseudonymgenerierung über zufällige Werte (plus Zuordnungstabelle) oder Hash-Verfahren
- Aufbewahrung von Zuordnungsinformationen (Patientenliste)
- Anzahl Pseuonymisierungsschritte

4. Sicherheitselemente für Pseudonymisierungsverfahren

4.1. Datenhaltung

Bei einer zentralen Datenhaltung übermitteln die behandelnden Stellen die pseudonymisierten MDAT an eine zentrale Forschungsdatenbank, auf die die Forscher meist online zugreifen können. Einrichtungsübergreifende Auswertungen können dann, nach entsprechender Genehmigung, schnell und unkompliziert vorgenommen werden. Bei einer dezentralen Datenhaltung dagegen verbleiben die Forschungsdaten beispielsweise in der behandelnden Einrichtung (in einer gesonderten Forschungsdatenbank, getrennt von den eigentlichen Behandlungsdaten) oder in einer Projektdatenbank und können bei Bedarf abgerufen und kombiniert werden.

4.2. Ort der Pseudonymisierung

Die Pseudonymisierung sollte möglichst früh durchgeführt werden, d.h. wenn möglich bereits in der behandelnden Stelle. In diesem Fall verlassen die IDAT nie die Stelle, die die vollständigen Daten im Rahmen der Behandlung besitzt, weswegen es sich um ein durchgängig pseudonymisiertes Verfahren handelt, das aus Datenschutzsicht deutliche Vorteile bietet.

Eine Pseudonymisierung außerhalb der behandelnden Stelle beinhaltet in der Regel, dass die IDAT des Patienten weitergegeben werden und eine andere Stelle somit erfährt, welche Patienten an einer bestimmten Krankheit leiden. Dies ist bereits ein Durchbrechen der ärztlichen Schweigepflicht, für das die Einwilligung des Patienten oder eine gesetzliche Grundlage benötigt wird. Zudem sollte sichergestellt werden, dass die Pseudonymisierung bei einer vertrauenswürdigen Stelle, die nicht selbst inhaltlich an der Studie beteiligt ist, stattfindet. Besonders geeignet für solche Aufgaben ist in der Regel ein externer Treuhänder, bei dem der Beschlagnahmeschutz gewährleistet ist, also beispielsweise ein Notar. Dies ist insbesondere nötig bei Krankheiten, die eine gesellschaftliche Stigmatisierung mit sich bringen könnten, wie z.B. psychische Erkrankungen oder AIDS. Für weniger problematische Krankheiten könnte in Einzelfällen auch die Verwaltung der Patientenliste in einem teilnehmenden Krankenhaus dort, in einer nicht an der Studie inhaltlich beteiligten Abteilung, in Betracht gezogen werden.

4.3. Zentrale vs. dezentrale Pseudonymisierung

Bei einer dezentralen Pseudonymisierung werden die Pseudonyme in der Regel direkt in der behandelnden Einrichtung vorgeben. Dies kann jedoch je nach Struktur des Forschungsnetzes gewisse Schwierigkeiten mit sich bringen: Für einrichtungsübergreifende Studien muss sichergestellt werden, dass die Pseudonyme im ganzen Verfahren eindeutig sind, d.h. die behandelnden Stellen dürfen nicht für verschiedene Personen das gleiche Pseudonym vergeben. Genauso dürfen für eine Person nicht mehrere Pseudonyme genutzt werden, auch wenn sich beispielsweise der Name oder die Adresse ändert bzw. der Patient den Arzt wechselt. Häufig ist die dezentrale Pseudonymisierung deshalb besonders für Studien geeignet, bei denen nur wenige Stellen beteiligt sind, die Mobilität der Patienten gering ist, oder wo Daten nur über einen kurzen Zeitraum hinweg erhoben werden müssen.

Ein Hilfsmittel zur dezentralen Pseudonymisierung ist die Nutzung unveränderlicher Kennzeichen wie Vorname, Geburtsort, Geburtsdatum, oder zukünftig evtl. die Versichertennummer der neuen Gesundheitskarte zur Generierung der Pseudonyme. Zudem kann eine Normalisierung der IDAT vorgenommen werden, die unterschiedliche Schreibweisen, Tippfehler etc. ausgleicht. Mit diesen Methoden sollte an einem beliebigen Ort und zu einem beliebigen Zeitpunkt immer das gleiche Pseudonym generiert werden können.

Werden derartige Verfahren als nicht praktikabel angesehen, kann eine zentrale Pseudonymisierung gewählt werden, bei der die IDAT an eine zentrale Stelle versandt werden, die dann ein entsprechendes Pseudonym zurückliefert. Diese zentrale Stelle hat die Möglichkeit, die eingehenden Meldungen / IDAT abzugleichen und Duplikate etc. aufzudecken. Dies hat jedoch wie unter 4.2 bereits dargestellt den Nachteil, dass die IDAT hierbei die behandelnde Stelle verlassen und häufig eine zentrale, externe Patientenliste entsteht.

4.4. Versand IDAT und MDAT

Nach Möglichkeit sollten die IDAT und die MDAT im Falle einer zentralen Pseudonymisierung nicht gemeinsam versandt werden, sondern ein zweigeteiltes Verfahren gewählt werden. Im ersten Schritt werden die IDAT zur Pseudonymisierung an die pseudonymisierende Stelle versandt, die das Pseudonym zurückliefert, und im zweiten Schritt werden die MDAT mit dem Pseudonym an den Empfänger verschickt.

Ist nur ein gemeinsamer Versandt der IDAT und MDAT, zunächst an die pseudonymisierende Stelle und anschließend an die forschende Stelle möglich, müssen die Daten entsprechend verschlüsselt werden. Die IDAT dürfen nur für die pseudonymisierende Stelle entschlüsselbar sein und müssen dort durch das Pseudonym ersetzt werden. Evtl. werden diese Informationen anschließend in der Patientenliste abgelegt. Die MDAT dagegen müssen für die forschende Stelle verschlüsselt werden, d.h. sie dürfen für die pseudonymisierende Stelle nicht lesbar sein, obwohl sie sie erhält. Insgesamt darf nur die behandelnde Einrichtung IDAT und MDAT im Klartext für die von ihr behandelten Patienten besitzen.

4.5. Pseudonymgenerierung

Für die eigentliche Pseudonymgenerierung können zwei grundsätzliche Verfahren unterschieden werden, zum einen die Generierung eines Hash-Werts aus den IDAT, zum anderen die Erzeugung von Zufallswerten und deren zufällige Zuordnung zum Patienten über eine Zuordnungsliste.

Bei der Pseudonymisierung per Zuordnungsliste gibt es keinen inneren Zusammenhang zwischen IDAT und Pseudonym, daher muss die Zuordnung aufbewahrt werden, um nachfolgende Meldungen korrekt pseudonymisieren zu können. Ein wichtiger Aspekt hierbei ist die gesicherte Aufbewahrung dieser Zuordnungsliste (= Patientenliste) beispielsweise bei einem Treuhänder. Dieses Verfahren der Zuordnungsliste hat den Vorteil, dass die Pseudonyme nach dem Zufallsprinzip vergeben werden, was eine Ausforschung schwierig macht, solange die Zuordnungsliste gut geschützt ist. Gleichzeitig ist dieses Verfahren wohl nur mit einer zentralen Pseudonymisierungsstelle handhabbar. Bei dezentralen Verfahren müssten z.B. an jede behandelnde Einrichtung Teillisten vergeben werden. Es ergeben sich jedoch Schwierigkeiten der Listenpflege, wenn ein Patient den Arzt wechselt. Es muss z .B. geklärt werden, ob er sein Pseudonym mitnehmen kann, welches dann nicht mehr in den "Nummernbereich" des neuen Arztes passt, oder ob das Pseudonym geändert werden muss, was einen erheblichen Aufwand mit sich bringen würde.

Die Erzeugung von Pseudonymen durch ein Hashverfahren hat den Vorteil, dass hier auch eine dezentrale Generierung denkbar ist und keine Zuordnungstabellen aufbewahrt werden müssen, wobei grundsätzlich die Gefahr besteht, dass ein Angreifer bei Kenntnis der IDAT und des Hash-Verfahrens durch Ausprobieren die Pseudonyme ermitteln kann. Deshalb ist auf eine sichere Gestaltung des Hash-Verfahrens zu achten, in dem z.B. ein Geheimnis zur Erzeugung des Hashes notwendig ist. Beispielsweise kann der erzeugte Hash-Wert noch zusätzlich (symmetrisch) verschlüsselt werden (oder auch umgekehrt), wobei der Schlüssel sicher verwahrt werden muss.

4.6. Anzahl Pseudonymisierungsschritte

Häufig werden einstufige Pseudonymisierungsverfahren verwendet, bei denen (zentral oder dezentral) die IDAT direkt durch das Pseudonym ersetzt werden, das für den Forscher sichtbar ist. Dies hat jedoch den Nachteil, dass die pseudonymisierende Stelle in alleiniger Hoheit eine Depseudonymisierung der Patienten vornehmen kann. Für eine

Kompromittierung des Systems muss also nur die pseudonymisierende Stelle angegriffen werden. Dies ist insbesondere kritisch, wenn eine zentrale Pseudonymisierung stattfindet.

Deshalb kann es sinnvoll sein, eine weitere Pseudonymisierungsstufe einzuführen. Im ersten Schritt werden die IDAT durch ein Zwischenpseudonym ersetzt, (wie oben beschrieben per Hash-Verfahren oder Zuordnungsliste), das im zweiten Schritt beispielsweise durch eine kryptographische Transformation in das eigentliche Pseudonym übersetzt wird, mit dem die MDAT dann gespeichert werden. Der behandelnden Stelle muss das endgültige Pseudonym nicht bekannt sein. Eine Depseudonymisierung benötigt somit die Kooperation aller Stellen, was die Sicherheit deutlich erhöht. Im Idealfall sollten beide Dienste von unterschiedlichen Treuhändern realisiert werden, denkbar ist grundsätzlich jedoch auch die Nutzung getrennter Funktionseinheiten eines Treuhänders oder die Verwaltung der Patientenliste durch eine Klinik (siehe Kapitel 4.2) und die Abwicklung der zweiten Stufe durch einen Treuhänder.

Um die Sicherheit weiter zu erhöhen ist es auch möglich, das Pseudonym aufzusplitten. Z.B. könnte das aus den IDAT erzeugte Zwischenpseudonym in zwei Teile zerlegt und an zwei verschiedene Transformationsdienste weitergegeben werden, die jeweils mit unterschiedlichen Schlüsseln Teilpseudonyme erzeugen, die beim Empfänger für die Datenspeicherung zum Pseudonym zusammengesetzt werden.

Grundsätzlich sind beliebig viele Stufen und Aufsplittungen denkbar, die durch ihre zunehmende Verteilung der Pseudonymgenerierung das Risiko einer unbefugten Despeudonymisierung reduzieren. Es muss jedoch geprüft werden, ob der Aufwand den Gewinn an Sicherheit rechtfertigt.

4.7. Despeudonymisierung

Die Gestaltung des Pseudonymisierungsverfahrens hängt nicht zuletzt davon ab, ob eine Depseudonymisierung in bestimmten Fällen gewünscht ist, da z.B. im Fall von Hash-Verfahren hierfür gewisse Zusatzinformationen vorgehalten werden müssen. Ein Bedarf für die Reidentifizierung kann z.B. entstehen, wenn Forschungsergebnisse dem Patienten mitgeteilt werden sollen bzw. wenn sich hieraus Folgen für seine Behandlung ergeben.

Zunächst müssen organisatorische Abläufe festgelegt werden, in welchen Fällen eine Depseudonymisierung stattfinden darf, durch welche Stellen dies genehmigt werden kann und wie hierfür der Ablauf ist, dessen technische Ausgestaltung seinerseits von gewählten Pseudonymisierungsverfahren abhängt.

Wird eine Patientenliste geführt, besteht immer die Möglichkeit zur Depseudonymisierung, da diese in der Regel dauerhaft vorhanden ist. Dagegen ist die Pseudonymisierung über Hash-Verfahren möglich, ohne dass Zuordnungsinformationen aufbewahrt werden müssen. Eine Depseudonymisierung wäre dann nur noch in der behandelnden Stelle möglich, soweit hier das Pseudonym bekannt ist. Ist dagegen eine Depseudonymisierung gewünscht, muss eine Möglichkeit zur Rückrechnung oder Zuordnung des Pseudonyms gegeben sein, so dass die Pseudonymisierungsschritte rückwärts durchlaufen werden können. Häufig wird für diesen Zweck zusätzlich zum Hash-Verfahren eine Patientenliste angelegt, über die die Reidentifizierung erfolgt.

4.8. Pseudonymisierung der Angaben zur behandelnden Stelle

In bestimmten Fällen kann es wünschenswert sein, die Angaben zur behandelnden Stelle zu pseudonymisieren (und nur im Bedarfsfall eine Depseudonymisierung zur ermöglichen). Es ist beispielsweise für die wissenschaftliche medizinische Forschung nicht immer nötig zu wissen, welcher Arzt den Patienten behandelt hat. Diese Informationen können die Interessen des Arztes berühren und/oder das Reidentifizierungsrisiko für den Patienten erhöhen. Anders kann es für die medizinische Qualitätssicherung sein, bei der für die Durchsetzung einheitlicher Behandlungsstandards gesorgt werden soll. Aber auch hier sollte eine Depseudonymisierung nur nach einem bestimmten Verfahren und nicht für alle Auswerter möglich sein. Die gewählten technischen Verfahren können analog zu denen für die Pseudonymisierung der Patienten gestaltet werden.

5. Technisch-organisatorische Sicherheitsmaßnahmen

Bei der Realisierung eines Pseudonymisierungskonzepts und der zugehörigen Forschungsdatenbanken sind die technisch-organisatorischen Sicherheitsmaßnahmen, wie sie z.B. in Art. 7 BayDSG (Bayerisches Datenschutzgesetz) oder analog in §9 BDSG (Bundesdatenschutzgesetz) und Anlage definiert sind, zu berücksichtigen. Näheres hierzu findet sich beispielsweise unter http://www.datenschutz-bayern.de/technik/orient/10geb.htm Grundsätzliche technische Sicherheitsanforderungen im medizinischen Bereich können auch in der Orientierungshilfe Telemedizin der Datenschutzbeauftragten http://www.datenschutz-bayern.de/verwaltung/DatenschutzTelemedizin.pdf eingesehen werden.

Zusammenfassend betrachtet sind u.a. folgende Maßnahmen nötig:

- Übliche Maßnahmen zum Schutz der Patientendaten in der behandelnden Einrichtung (siehe z.B: http://www.datenschutz-bayern.de/technik/orient/patdatkh.html
- Verschlüsselte Datenübertragung zwischen allen beteiligten Stellen (z.B. SSL), Sicherstellung, dass jede Stelle beim Datentransport nur jeweils die Daten einsehen kann, für die sie berechtigt ist
- Verbindungsaufbau nur durch befugte Personen und nur zwischen beteiligten Komponenten
- Verschlüsselte Speicherung bzw. gesicherte Aufbewahrung der Patientenliste (IDAT und Pseudonym) sowie der Forschungsdatenbank
- Gesicherte Aufbewahrung der zur Pseudonymisierung verwendeten kryptographischen Schlüssel
- Sichere Authentifizierung der Nutzer (Forscher, Behandler, Treuhänder etc.)
- Differenzierte Zugriffsrechte gemäß der Aufgaben
- Revisionsfähige Protokollierung
- Einsatz von Firewalls, Virenschutz
- Räumliche Absicherung der Komponenten

6. Ausblick: Einbeziehung von Biomaterialien

In zunehmendem Maße werden für wissenschaftliche Studien Blut- oder Gewebeproben der Patienten benötigt. Hierbei ist grundsätzlich zu unterscheiden, ob diese Proben ursprünglich im Behandlungszusammenhang erhoben wurden und nun für die Forschung verwendet werden sollen, oder ob die Erhebung direkt für die Forschung erfolgt. Zudem sollte unterschieden werden, ob die Proben für eine bestimmte Studie, d.h. für die Untersuchung eines bestimmten Krankheitsbildes erhoben und danach vernichtet werden, oder ob eine

Biomaterialdatenbank aufgebaut werden soll, die grundsätzlich für die Nutzung durch verschiedene Studien offen sein soll.

Dies alles beinhaltet einerseits rechtliche Unterschiede, andererseits aber auch technisch-organisatorische Unterschiede insbesondere im Bereich der Pseudonymisierung. Erfolgt die Nutzung im Rahmen einer bestimmten Studie, wird für diese in der Regel ein Pseudonymisierungskonzept aufgestellt, in dem die Pseudonymisierung der Proben integraler Bestandteil ist. Für eine Biomaterialdatenbank dagegen muss ein eigenes Konzept aufgestellt werden, das unabhängig von den geplanten Auswertungen und Studien funktioniert.

Datenschutzkonzepte zur Verwendung von Biomaterialien sind gerade erst im Entstehen, so dass zum jetzigen Zeitpunkt noch keine abschließenden Empfehlungen hierzu gegeben werden können. In allen Fällen muss jedoch sichergestellt werden, dass die Forscher, die mit den Proben arbeiten, keine identifizierenden Daten zu den Patienten erhalten. Auch hier gilt somit der Grundsatz, dass Daten möglichst früh pseudonymisiert oder, wenn möglich, anonymisiert werden sollten, als z.B. bereits bei der Lagerung. Auch sollte die informationelle Gewaltenteilung innerhalb der Biomaterialbank berücksichtigt werden.

7. Weiterführende Literatur, Beispiele

[1] ATG-Managementpapier Pseudonymisierung / Anonymisierung, http://ehealth.gvg-koeln.de/xpage/objects/pseudonymisierung/docs/5/files/MP040316.pdf *(externer Link)*

[2] Generische Datenschutzkonzepte der Telematikplattform für medizinische Forschungsnetze (TMF), http://www.tmf-ev.de *(externer Link)*

[3] Pseudonymisierungskonzept Qualitätssicherung in der Nierenersatztherapie (Quasi-Niere), http://www.quasi-niere.de/ *(externer Link)*

[4] Deutsches Hämophilieregister, http://www.pei.de/professionals/dhr.htm *(externer Link)*

[5] Arbeitspapier Datenschutzfreundliche Technologien, http://www.datenschutz-bayern.de/technik/grundsatz/apdsft.htm